บริษัท บางกอก แอสเซท

อินเตอร์กรุ๊ป จำกัด (มหาชน)

ส่วนงานเทคโนโลยีสารสนเทศ

ผู้จัดทำ	ผู้ตรวจสอบ	ผู้อนุมัติ
.....	.....	.....
วันที่ 27 ธ.ค. 2567	วันที่ 27 ธ.ค. 2567	วันที่ 27 ธ.ค. 2567

BANGKOK ASSET INTERGROUP	บริษัท บางกอก แอสเซท อินเตอร์กรุ๊ป จำกัด (มหาชน)	
	ส่วนงานเทคโนโลยีสารสนเทศ	วันที่บังคับใช้ 27 ธันวาคม 2567 แก้ไขครั้งที่ 1

บันทึกการแก้ไขเอกสาร

วันที่	แก้ไขครั้งที่	รายการแก้ไข	ผู้ขอแก้ไข
15 มกราคม 2567	0	-	-
27 ธันวาคม 2567	1	PC-IT-001 กำกับดูแลและรักษาความมั่นคง IT	ชาญยุทธ วัฒนาศักดิกุล
		PC-ORG-008 บริหารความต่อเนื่องทางธุรกิจ	ชาญยุทธ วัฒนาศักดิกุล
		PC-ORG-013 บริหารความต่อเนื่องทางธุรกิจ	ชาญยุทธ วัฒนาศักดิกุล
		IT-Procedure-002 (File Sharing&ClassificationV2.0	ชาญยุทธ วัฒนาศักดิกุล
		IT-Procedure-008(SW installation) V1.1	ชาญยุทธ วัฒนาศักดิกุล
		IT-Procedure-010 (OS Admin)V1.1	ชาญยุทธ วัฒนาศักดิกุล
		IT-Procedure-015 (NAS Backup Recovery)V1.1	ชาญยุทธ วัฒนาศักดิกุล
		IT-Procedure-018 (System Config)V2.0	ชาญยุทธ วัฒนาศักดิกุล
		IT-Procedure-021ขั้นตอนการตรวจสอบความเรียบร้อยห้อง Server V2.0	ชาญยุทธ วัฒนาศักดิกุล
		IT-Procedure-028 (Log NAS)V2.1	ชาญยุทธ วัฒนาศักดิกุล
		IT-Procedure-029 (AD log) V2.1	ชาญยุทธ วัฒนาศักดิกุล
		IT-Procedure-034ขั้นตอนการตั้งค่าโปรแกรม Anti-Virus V2.0	ชาญยุทธ วัฒนาศักดิกุล

วันที่	แก้ไขครั้งที่	รายการแก้ไข	ผู้ขอแก้ไข
		IT-Procedure-036 (Firewall Configuration)V3.0	ชาญยุทธ วัฒนาศักดิกุล
		IT-Procedure-037 (OS Manual) 1.1	ชาญยุทธ วัฒนาศักดิกุล
		IT-Procedure-038 (DBC Manual) V1.1	ชาญยุทธ วัฒนาศักดิกุล
		IT-Procedure-039 V2.4 Software and Applications List	ชาญยุทธ วัฒนาศักดิกุล
		IT-Procedure-045 (Firewall Log) V1.1	ชาญยุทธ วัฒนาศักดิกุล
		IT-Procedure-050 (IT Disaster)v2.1	ชาญยุทธ วัฒนาศักดิกุล
		IT-Procedure-054 ขั้นตอนการเก็บ Log Anti-Virus 2.0	ชาญยุทธ วัฒนาศักดิกุล
		IT-Procedure-056 เปลี่ยน Harddisk V1.1	ชาญยุทธ วัฒนาศักดิกุล
		IT-Procedure-058 ขั้นตอนการบริหารจัดการ WiFi V2.0	ชาญยุทธ วัฒนาศักดิกุล
		IT-Procedure-060 ขั้นตอนการทำแผนกลยุทธ์ IT	ชาญยุทธ วัฒนาศักดิกุล

ตารางคู่มือปฏิบัติการ

IT-Procedure	ชื่อ Procedure	วันที่ประกาศใช้	เวอร์ชั่นล่าสุด
PG-IT-001	นโยบายเทคโนโลยีสารสนเทศ	14-12-2024	1.0
PC-ORG-008	แผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan)	14-12-2024	1.0
SISP-IT-002	แผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ	14-12-2024	1.0
IT-Procedure-001	ขั้นตอนการเข้าใช้งานห้อง Server (Sever Room Access Control)	01-07-2022	1.1
IT-Procedure-002	ขั้นตอนการบริหารจัดการ Files Sharing (Files Sharing Management Procedure)	01-03-2024	2.0
IT-Procedure-003	ขั้นตอนการพัฒนาระบบสารสนเทศ (System Development Procedure)	05-01-2023	2.0
IT-Procedure-004	การเข้าใช้สิทธิ์ระบบงาน System Access Control Procedure	15-03-2022	1.0
IT-Procedure-005	ขั้นตอนการป้องกันไวรัสคอมพิวเตอร์ /มัลแวร์ Virus Computer/Malware Protection Procedure	15-03-2022	1.0
IT-Procedure-006	ขั้นตอนการทำลายสื่อบันทึกข้อมูลอิเล็กทรอนิกส Records Disposition Procedure	15-03-2022	1.0
IT-Procedure-007	ขั้นตอนการสำรองข้อมูลและการกู้คืน OS (OS Backup and Recovery Procedure)	15-11-2022	2.0
IT-Procedure-008	ขั้นตอนการติดตั้งซอฟต์แวร์คอมพิวเตอร์ Software Installation Procedure	04-03-2024	1.1
IT-Procedure-009	ขั้นตอนการใช้งานและการใช้ Admin ระบบDBC (DBC Administrator Procedure)	15-03-2022	1.0
IT-Procedure-010	ขั้นตอนการใช้ Admin ระบบOS (OS Administrator Procedure)	04-03-2024	1.1
IT-Procedure-011	ขั้นตอนการใช้ Admin ระบบKintone Kintone Administrator Procedure	30-03-2022	1.0
IT-Procedure-012	ขั้นตอนการแจ้งปัญหาด้านระบบ Service Desk Procedure	30-03-2022	1.0
IT-Procedure-013	ขั้นตอนการคัดเลือกผู้ให้บริการภายนอก Outsourcing Management Procedure	30-03-2022	1.0
IT-Procedure-014	ขั้นตอนการสำรองข้อมูลและการกู้คืน DBC (DBC Backup and Recovery Procedure)	30-03-2022	1.0
IT-Procedure-015	ขั้นตอนการสำรองข้อมูลและการกู้คืนจาก NAS (NAS Backup and Recovery Procedure)	01-03-2024	1.1
IT-Procedure-016	ขั้นตอนการติดตั้งค่าระบบการสำรองข้อมูล NAS (NAS Backup Configuration Procedure)	30-03-2022	1.0
IT-Procedure-017	ขั้นตอนการติดตั้ง Domain Controller (Domain Controller Setup Procedure)	30-03-2022	1.0
IT-Procedure-018	ขั้นตอนการตั้งค่าระบบเทคโนโลยีสารสนเทศ IT System Configuration Procedure	20-01-2024	2.0
IT-Procedure-019	คู่มือสำหรับการใช้งาน Admin ของ Kintone (Kintone Administrator Procedure)	30-03-2022	1.0
IT-Procedure-020	ขั้นตอนการสำรวจความพึงพอใจผู้ใช้งาน Customer Satisfaction Survey Procedure	30-03-2022	1.0
IT-Procedure-021	ขั้นตอนการตรวจสอบความเรียบร้อยห้อง Server (Server Room Environment Checking Procedure)	15-01-2024	2.0
IT-Procedure-022	ขั้นตอนการพัฒนาและฝึกอบรมพนักงาน IT Development & Training Procedure	19-04-2022	1.0
IT-Procedure-023	การจำแนกข้อมูล Information Classification Procedure	05-01-2023	1.1
IT-Procedure-024	การบริหารจัดการ Log (Log Management Procedure)	19-04-2022	1.0
IT-Procedure-025	ขั้นตอนการเก็บ Log ของ DBC (DBC Log Setup Procedure)	19-04-2022	1.0
IT-Procedure-026	ขั้นตอนการเก็บ Log ของ DBC (DBC Log Setup Procedure)	19-04-2022	1.0
IT-Procedure-027	ขั้นตอนการเก็บ Log ของ Kintone (Kintone Log Setup Procedure)	19-04-2022	1.0
IT-Procedure-028	ขั้นตอนการเก็บ log NAS (NAS log Setup Procedure)	15-02-2024	2.1
IT-Procedure-029	ขั้นตอนการเก็บ Log ของ AD (AD Log Setup Procedure)	15-02-2027	2.1

ตารางคู่มือปฏิบัติการ

IT-Procedure	ชื่อ Procedure	วันที่ประกาศใช้	เวอร์ชั่นล่าสุด
IT-Procedure-030	ขั้นตอนการเก็บ Log ของ VPN (VPN Log Setup Procedure)	01-09-2022	2.0
IT-Procedure-031	ขั้นตอนการจัดการ NDA (Non-Disclosure Agreement Process Procedure)	03-05-2022	1.0
IT-Procedure-032	ขั้นตอนการจัดการความเสี่ยงเทคโนโลยีสารสนเทศ IT Risk Management Procedure	01-08-2022	2.0
IT-Procedure-033	คู่มือสำหรับการใช้งาน Admin ของ AD (Active Directory Administrator Procedure)	03-05-2022	1.0
IT-Procedure-034	ขั้นตอนการตั้งค่าโปรแกรม Anti-Virus (Anti-Virus Configuration Procedure)	03-05-2022	1.0
IT-Procedure-035	ขั้นตอนการใช้งานจากหน่วยงานภายนอก 3rd Party Access Control Procedure	01-07-2022	1.0
IT-Procedure-036	ขั้นตอนการตั้งค่า Firewall / HA (Firewall / HA Configuration Procedure)	01-02-2024	3.0
IT-Procedure-037	คู่มือ และเอกสารประกอบการพัฒนาโปรแกรม OS (OS Manual Procedure)	01-02-2024	1.1
IT-Procedure-038	คู่มือการใช้งาน DBC (DBC Manual Procedure)	01-02-2024	1.1
IT-Procedure-039	ทะเบียนโปรแกรมและระบบ Software and Applications List	11-11-2024	2.4
IT-Procedure-040	การสำรองข้อมูลระบบ DBC ไว้ที่ Local (DBC Backup to Local System)	01-08-2022	1.0
IT-Procedure-041	ขั้นตอนการติดตั้ง IIS (IIS Configuration Procedure)	01-08-2022	1.0
IT-Procedure-042	การแจ้งซ่อมอุปกรณ์คอมพิวเตอร์ประเภทไม่ใช่ทรัพย์สิน (Non-Asset)	01-08-2022	1.0
IT-Procedure-043	การจัดการอุปกรณ์คอมพิวเตอร์ประเภททรัพย์สิน IT Asset Management	01-02-2023	1.2
IT-Procedure-044	การแจ้งปัญหา IT (Incident/Problem Management)	01-09-2022	1.0
IT-Procedure-045	ขั้นตอนการเก็บ Log ของ Firewall (Firewall Log Configuration Procedure)	15-02-2024	1.1
IT-Procedure-046	การ Upgrade โปรแกรม หรือ Software (Program or Software Upgrade)	01-09-2022	1.0
IT-Procedure-047	การตรวจสอบ Software และบำรุงรักษาอุปกรณ์ SW Checking and HW Maintenance	01-09-2022	1.0
IT-Procedure-048	การแก้ไขระบบ/โปรแกรม (System Change Requisition)	20-01-2023	2.1
IT-Procedure-049	ขั้นตอนการควบคุมการลง Software (Software Control Procedure)	01-11-2022	1.0
IT-Procedure-050	คู่มือการปฏิบัติงานรองรับสถานการณ์ฉุกเฉิน IT Disaster Backup/Recovery	15-01-2024	2.1
IT-Procedure-051	ขั้นตอนการจัดการพนักงานลาออก Employee Exit Clearance Procedure	01-12-2022	1.0
IT-Procedure-052	ขั้นตอนการทดสอบความปลอดภัยของระบบ Vulnerability Assessment	01-03-2023	1.0
IT-Procedure-053	ขั้นตอนการกู้ข้อมูลจากไฟล์ที่ลบไปจาก SERVER (Data recovery from deleted files on server)	01-02-2024	1.1
IT-Procedure-054	ขั้นตอนการเก็บLog Anti-Virus	11-11-2024	2.0
IT-Procedure-055	ขั้นตอนการ backup ข้อมูลของ SERVER บัญชี และการ Revert ไฟล์ 192.168.100.74	01-07-2023	1.0
IT-Procedure-056	ขั้นตอนการ เปลี่ยน Hard Disk Server 192.168.1.224	01-02-2024	1.1
IT-Procedure-057	ขั้นตอนการบริหารจัดการ eMail (eMail Management Procedure)	05-07-2023	1.0
IT-Procedure-058	ขั้นตอนการบริหารจัดการ WiFi (Wifi Management Procedure)	01-02-2024	2.0
IT-Procedure-059	การตรวจสอบ Traffic ของ User และ Application ภายใน องค์กร	01-08-2023	1.0
IT-Procedure-060	ขั้นตอนการจัดทำแผนกลยุทธ์เทคโนโลยีสารสนเทศ	25-01-2024	1.0



นโยบายกำกับดูแลและรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

บริษัท บางกอก แอสเซท อินเตอร์กรุ๊ป จำกัด (มหาชน)

ประวัติการจัดทำ และทบทวนเอกสาร

ครั้งที่	วันที่แก้ไข	รายละเอียด
00	11 พฤศจิกายน 2566	เผยแพร่เพื่อใช้งานครั้งที่ 1 ภายหลังการแปรสภาพบริษัทจากบริษัทจำกัดเป็นบริษัทมหาชนจำกัด
01	14 ธันวาคม 2567	ทบทวนประจำปี 2567

นโยบายกำกับดูแลและรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

ของ

บริษัท บางกอก แอสเซท อินเตอร์กรุ๊ป จำกัด (มหาชน)

1. บทนำ

บริษัท บางกอก แอสเซท อินเตอร์กรุ๊ป จำกัด (มหาชน) ("**บริษัทฯ**") ได้จัดให้มีการกำหนดนโยบายกำกับดูแลและรักษาความมั่งคงปลอดภัยเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และ/หรือ การถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่บริษัทฯ บริษัทฯ จึงได้จัดทำนโยบายกำกับดูแลและรักษาความมั่งคงปลอดภัยเทคโนโลยีสารสนเทศขึ้นใช้ในบริษัทเพื่อใช้เป็นแนวปฏิบัติเพื่อการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ

นโยบายกำกับดูแลและรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศฉบับนี้ ประกอบด้วยหมวดใหญ่ทั้งสิ้น 8 หมวด และ 6 มาตรฐาน ดังต่อไปนี้

หมวดที่ 1 นโยบายการใช้งานคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง (Computer Usage Policy)

1.1 มาตรฐานของ User และ Password (User Account Standard)

1.2 มาตรฐานของควบคุมระบบหรือ Administrator (System Access Control Standard)

หมวดที่ 2 นโยบายการใช้ Hardware และ Software (Hardware and Software Policy)

2.1 มาตรฐานบริหารการจัดการ Software (Software Management Standard)

2.2 มาตรฐานการซ่อมและการตัดออกจากระบบบัญชีทรัพย์สิน (Repairing and Disposal Standard)

2.3 มาตรฐานการพัฒนาระบบสารสนเทศ (System Development Life Cycle Standard)

หมวดที่ 3 นโยบายความมั่นคงปลอดภัยทางข้อมูลข่าวสาร เว็บไซต์ เมล แชท (Information, Website, E-mail and Instant Messaging Security (Chat) Policy)

หมวดที่ 4 นโยบายความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Policy)

หมวดที่ 5 นโยบายการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Policy)

5.1 มาตรฐานการสำรองและกู้กลับข้อมูล (Backup and Recovery Standard)

หมวดที่ 6 นโยบายการกำกับดูแลการใช้งาน Cloud (Cloud Computing Policy)

หมวดที่ 7 นโยบายการบริหารการจัดการความเสี่ยงทางเทคโนโลยีสารสนเทศ (IT Risk Management Policy)

หมวดที่ 8 นโยบายความมั่นคงปลอดภัยทางกายภาพ และสิ่งแวดล้อม (Physical and Environmental Security Policy)

2. วัตถุประสงค์

2.1 เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศหรือ เครือข่ายคอมพิวเตอร์ของบริษัท ทำให้สามารถดำเนินงานได้อย่างมีประสิทธิภาพ

2.2 เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในบริษัทฯ ได้รับทราบ และเจ้าหน้าที่บริษัททุกคนต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

2.3 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่บริษัทฯ เจ้าหน้าที่สารสนเทศ และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทฯ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศสำหรับการดำเนินงาน

2.4 บริษัทฯ ต้องกำหนดให้มี "เจ้าหน้าที่เทคโนโลยีสารสนเทศ" หรือตัวแทน หรือพนักงานที่ได้รับมอบหมายที่สามารถดูแลรับผิดชอบ แก้ไขปัญหา ติดต่อประสานงานกับหน่วยงานภายนอก เพื่อบริหารจัดการระบบเครือข่ายและคอมพิวเตอร์ที่บริษัทใช้งานอยู่ได้

2.5 นโยบายกำกับดูแลและรักษาความปลอดภัยสารสนเทศนี้ต้องมีการดำเนินการตรวจสอบ ประเมิน รวมทั้งทบทวนเพื่อปรับปรุงนโยบายอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงใดๆ ที่กระทบต่อนโยบายฉบับนี้

3. ขอบเขต

ขอบเขตของนโยบายกำกับดูแลและรักษาความปลอดภัยสารสนเทศครอบคลุมการป้องกันและรักษาความมั่นคงปลอดภัยของสารสนเทศของบริษัทฯ ทั้งที่อยู่ในสถานที่ปฏิบัติงานของบริษัทฯ หรือภายนอกบริษัทฯ โดยครอบคลุมถึงเจ้าหน้าที่บุคคล และหน่วยงานภายนอกที่ได้รับสิทธิในการเข้าถึงทรัพย์สินที่เกี่ยวข้องกับสารสนเทศของบริษัทฯ

4. คำนิยาม

"บริษัทฯ"	หมายถึง	บางกอก แอสเซท อินเตอร์กรุ๊ป จำกัด (มหาชน)
"ระบบเทคโนโลยีสารสนเทศ"	หมายถึง	อุปกรณ์ (Hardware) หรือโปรแกรม (Software) หรือระบบคอมพิวเตอร์ ตลอดจนระบบเครือข่ายที่ใช้งานในบริษัทฯ
"ฝ่ายเทคโนโลยีสารสนเทศ"	หมายถึง	หน่วยงานที่รับผิดชอบดูแลระบบเทคโนโลยีสารสนเทศของบริษัทฯ และให้หมายความรวมถึงสถานที่ปฏิบัติงานของเจ้าหน้าที่เทคโนโลยีสารสนเทศ
"เจ้าหน้าที่บริษัท"	หมายถึง	เจ้าหน้าที่ของบริษัท บางกอก แอสเซท อินเตอร์กรุ๊ป จำกัด (มหาชน) รวมถึงบุคคลอื่นที่บริษัทฯ มอบหมายให้ปฏิบัติงานตามสัญญาหรือข้อตกลง
"เจ้าหน้าที่เทคโนโลยีสารสนเทศ" (System Administrator)	หมายถึง	เจ้าหน้าที่ที่ได้รับมอบหมายจากหัวหน้าสายงานให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

“หน่วยงานภายนอก”	หมายถึง	บุคคลที่ไม่ใช่พนักงานของบริษัทฯ เช่น ผู้ให้บริการ ลูกค้า ผู้ขายสินค้า เป็นต้น หน่วยงานภายนอก ที่บริษัทอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของบริษัท โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล
“ผู้ให้บริการ”	หมายถึง	บุคคลภายนอกที่ให้บริการพัฒนาระบบงาน หรือให้บริการบำรุงรักษาระบบคอมพิวเตอร์ และอุปกรณ์อื่น หรือผู้ให้บริการด้านเทคโนโลยีซึ่งบริษัท เป็นผู้ใช้บริการ
“ทรัพย์สินสารสนเทศ”	หมายถึง	ทรัพย์สินซึ่งทางบริษัทฯ เป็นเจ้าของ เช่า ว่าจ้างให้พัฒนา พัฒนาขึ้นเอง หรือซื้อ ได้แก่ ข้อมูลสารสนเทศ เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่างๆ โปรแกรมคอมพิวเตอร์ อุปกรณ์เชื่อมโยงเครือข่าย ระบบอินทราเน็ต ของบริษัท รวมทั้งการเรียกใช้ ส่งข้อมูล และการค้นหาข้อมูลผ่านทางอินเทอร์เน็ต
“หน่วยงานธุรกิจเจ้าของข้อมูล”	หมายถึง	หน่วยงานที่ก่อให้เกิดข้อมูลขึ้นในบริษัทฯ มีความรับผิดชอบในความถูกต้องของข้อมูล และจัดทำข้อมูลให้เป็นปัจจุบันอยู่เสมอ จัดหมวดหมู่ดูแล และควบคุมให้มีการรักษาความปลอดภัยที่เหมาะสม รวมถึงเป็นผู้พิจารณาอนุมัติการการเข้าถึงข้อมูล การจัดเก็บ และการทำลายข้อมูลที่ตนเป็นเจ้าของ
“ผู้ดูแลระบบเทคโนโลยีสารสนเทศ”	หมายถึง	พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบเครือข่ายคอมพิวเตอร์และระบบฐานข้อมูลของบริษัทฯ
“ผู้ดูแลระบบงาน”	หมายถึง	พนักงานของบริษัทฯ ที่ปฏิบัติงานในฝ่ายเทคโนโลยีสารสนเทศ และได้รับมอบหมายให้ดูแลระบบงาน หรือโปรแกรมต่างๆ ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของบริษัทฯ
“ศูนย์คอมพิวเตอร์”	หมายถึง	ห้องหรือพื้นที่ที่มีการจัดวางอุปกรณ์คอมพิวเตอร์ หรือเครื่องเครือข่ายต่างๆที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของบริษัทฯ ซึ่งต้องได้รับการควบคุมความปลอดภัยในทุกด้าน
“ข้อมูลคอมพิวเตอร์”	หมายถึง	คำสั่ง ชุดคำสั่ง ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

"ระบบคอมพิวเตอร์"	หมายถึง	อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
"ระบบเครือข่าย (Network System)"	หมายถึง	ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆของบริษัทฯ ได้ เช่น ระบบ LAN ระบบ Intranet ระบบ Internet เป็นต้น <u>ระบบ LAN และระบบ Intranet</u> หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อ สื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในบริษัทฯ <u>ระบบ Internet</u> หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก
"ซอฟต์แวร์ (Software)"	หมายถึง	ซอฟต์แวร์แอพพลิเคชั่น (Application Software) ซอฟต์แวร์ระบบปฏิบัติการคอมพิวเตอร์ (Operating System Software) เครื่องมือในการพัฒนาระบบงาน (Development Tool) และโปรแกรมอรรถประโยชน์ (Utility)
"ฮาร์ดแวร์ (Hardware)"	หมายถึง	เครื่องคอมพิวเตอร์และอุปกรณ์รอบข้าง ที่สามารถสัมผัสได้ โดยจะประกอบด้วยอุปกรณ์ทางด้านอิเล็กทรอนิกส์ที่ควบคุมการประมวลผลข้อมูล การรับข้อมูล การแสดงผลข้อมูลของเครื่องคอมพิวเตอร์ มีทั้งที่ติดตั้งภายในเครื่องคอมพิวเตอร์และเชื่อมต่อภายนอกเครื่องคอมพิวเตอร์
"จดหมายอิเล็กทรอนิกส์ (E-mail)"	หมายถึง	ระบบที่เจ้าหน้าที่บริษัท ใช้ในการรับ-ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน
"รหัสผ่าน (Password)"	หมายถึง	ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

"ผู้ใช้งาน"	หมายถึง	เจ้าหน้าที่บริษัทฯ ผู้บริหาร เจ้าหน้าที่เทคโนโลยีสารสนเทศ หรือเจ้าหน้าที่จากหน่วยงานภายนอกที่ได้รับอนุญาต ในการเข้าถึงข้อมูลและ/หรือ ระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ
"ชุดคำสั่งไม่พึงประสงค์"	หมายถึง	ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
"เหตุการณ์ด้านความมั่นคงปลอดภัย"	หมายถึง	กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลวหรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
"เจ้าของข้อมูล"	หมายถึง	ผู้ได้รับมอบอำนาจจากผู้บริหารให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
"สินทรัพย์"	หมายถึง	ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น
"ฝ่ายบริหาร"	หมายถึง	ผู้มีหน้าที่ในการบริหารงานต่างๆ ในบริษัทฯ ประกอบด้วยประธานกรรมการบริหาร และประธานเจ้าหน้าที่ฝ่ายต่างๆ

5. การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties) บริษัทฯ ต้องจัดให้มีการแบ่งแยกหน้าที่การปฏิบัติงานระหว่างบุคลากรภายในฝ่ายเทคโนโลยีสารสนเทศอย่างเพียงพอ เพื่อช่วยให้มีการสอบยันการปฏิบัติงานและมีการอนุมัติการปฏิบัติงานอย่างเพียงพอและเหมาะสม รวมทั้งการมีขอบเขตการปฏิบัติงานของพนักงานที่ชัดเจนและมีบุคลากรที่เพียงพอต่อการปฏิบัติงานของฝ่ายเทคโนโลยีสารสนเทศ

6. นโยบาย

<u>หมวดที่ 1</u> นโยบายการใช้คอมพิวเตอร์ และอุปกรณ์ต่อพ่วง (Computer Usage Policy)

นโยบายการใช้คอมพิวเตอร์ และอุปกรณ์ต่อพ่วง หมายถึงแนวทางปฏิบัติการใช้งานคอมพิวเตอร์ และอุปกรณ์ต่อพ่วงระบบคอมพิวเตอร์ (Applications/Systems ต่างๆ) รวมถึงสิ่งที่ต่อเชื่อมเข้ากับเครือข่ายของบริษัทฯ และเครือข่ายอินเทอร์เน็ต ให้เหมาะสม เป็นไปอย่างประสิทธิภาพ ภายใต้ระเบียบข้อบังคับ และกฎหมาย

<u>วัตถุประสงค์</u>

1. เพื่อให้มีการใช้งานคอมพิวเตอร์ และ ระบบคอมพิวเตอร์ ได้อย่างต่อเนื่อง และมีประสิทธิภาพ

2. ปกป้องบริษัทฯ จากความเสี่ยงต่างๆ เช่นการสูญหายของทรัพย์สิน และข้อมูลที่สำคัญ รวมถึงการจู่โจมจากผู้ไม่หวังดีทั้งภายใน และภายนอกรวมทั้งการแพร่ระบาดของไวรัสคอมพิวเตอร์
3. เพื่อให้ไปตามกฎระเบียบข้อบังคับของบริษัทฯ และเป็นตามข้อกำหนดกฎหมาย

<u>ขอบเขต</u>

คอมพิวเตอร์ มือถือ, Tablet, EDI, Wi-Fi, Internet, Network และอุปกรณ์ต่อพวงเข้ากับระบบเครือข่ายคอมพิวเตอร์ Systems, Applications

<u>แนวทางปฏิบัติ</u>

1. ปฏิบัติตามข้อปฏิบัติการใช้งานต่างๆ ของบริษัทฯ และปฏิบัติภายใต้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
2. จำกัดการใช้งานคอมพิวเตอร์และอุปกรณ์ต่อพวง อินเทอร์เน็ต สำหรับงานส่วนตัว
3. รหัสประจำตัว (User ID) และรหัสผ่าน (Password) เป็นข้อมูลที่สำคัญ จะต้องเก็บเป็นความลับและไม่เปิดเผยให้ผู้อื่นนำไปใช้เด็ดขาด
4. ห้ามใช้เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพวง อินเทอร์เน็ตกับงานเหล่านี้เด็ดขาด
   - 4.1 การ Hacking หรือกระทำผิดต่อพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562
   - 4.2 การกระทำที่ผิดต่อลิขสิทธิ์ และกฎหมาย
   - 4.3 การใช้งานในการขุด Cryptocurrency
   - 4.4 การลับลอบขโมย/โจรกรรมข้อมูลทางการเงินหรือข้อมูลที่สำคัญของบริษัทฯ
   - 4.5 การยุ่งเกี่ยวกับสถาบันพระมหากษัตริย์ และการเมือง
   - 4.6 Download ข้อมูลที่ไม่เกี่ยวข้องกับงาน หรือสิ่งที่มีผลกระทบต่อเครือข่ายโดยรวมกับบริษัทฯ.

1.1 มาตรฐานของ User และ Password (User Account Standard)

<u>วัตถุประสงค์</u>

1. เพื่อเป็นการยืนยันตัวตนของผู้ใช้งาน และการเข้าถึงข้อมูลในระบบของบริษัทฯ
2. เพื่อความมั่นคง และปลอดภัยจากบุคคลที่ไม่ได้รับอนุญาตเข้ามาในใช้งานในระบบ หรือเครือข่ายของบริษัทฯ

<u>ขั้นตอนการทำงานผู้ใช้งาน</u>

1. จะต้องมี ชื่อ (User ID) และรหัสผ่าน (Password) เป็นของตนเองโดยเฉพาะ เพื่อเป็นการยืนยันสิทธิ์ และหน้าที่รับผิดชอบของผู้ใช้งานในแต่ละระบบ ซึ่งไม่สามารถเปิดเผยให้ผู้อื่นรู้เด็ดขาด
2. ชื่อและรหัสผ่านที่ใช้งานในแต่ระบบ ให้กำหนดเป็นมาตรฐานเดียวกัน โดยมีรูปแบบดังนี้
   - 2.1 ชื่อภาษาอังกฤษของพนักงานตามด้วย . (จุด) นามสกุลตัวแรก หากสกุลตัวแรกซ้ำก็จะเพิ่มตัวถัดไป ยกเว้นมีระบบที่ไม่สามารถใช้รูปแบบนี้ได้ ก็ให้ใช้ตามมาตรฐานของระบบนั้น

2.2 รหัสผ่านจะเป็นลักษณะ Strong Password ตั้งแต่ 8 ตัวขึ้นไป โดยประกอบด้วยเงื่อนไขดังต่อไปนี้

(1) ตัวหนังสือตัวใหญ่อย่างน้อย 1 ตัว (A-Z)

(2) ตัวหนังสือตัวเล็กอย่างน้อย 1 ตัว (a-z)

(3) ตัวเลขอย่างน้อย 1 ตัว (0-9)

(4) อักขระพิเศษอย่างน้อย 1 ตัว (!,@,#,$,%,&)

2.3 รหัสผ่านชั่วคราวที่กำหนดจากระบบหรือฝ่ายเทคโนโลยีสารสนเทศ จะต้องถูกเปลี่ยนภายใน 24 ชั่วโมง

2.4 การตั้งรหัสผ่านไม่ควรกำหนดให้มีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคล เช่น ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่ เป็นต้น

2.5 การตั้งรหัส ไม่ควรกำหนดเป็นคำศัพท์ที่อยู่ในพจนานุกรมภาษาอังกฤษ

2.6 การเปลี่ยนรหัสผ่านจะถูกกำหนดให้เปลี่ยนภายใน 90 วัน

2.7 กำหนดให้ทุกเครื่องมี Time out Facilities 15 นาที

3. การยกเลิกการใช้สิทธิ์ หรือ ลาออกจากบริษัทฯ จะต้องมีใบคำขอผ่านระบบ หากไม่มีการระบุว่าให้เก็บผู้ใช้ไว้ ทางเจ้าหน้าที่จะพิจารณาว่าผู้ใช้นั้น มีความสำคัญหรือมีผลกระทบต่อการใช้งานที่เกี่ยวข้องหรือไม่ หากไม่มีเจ้าหน้าที่ จะทำการลบชื่อนั้นออกจากระบบทันทีที่มีการแจ้งผ่านระบบ

1.2 มาตรฐานของควบคุมระบบหรือ Administrator (System Access Control Standard

<u>วัตถุประสงค์</u>

1. เพื่อเป็นมาตรฐานในปฏิบัติในการควบคุมใช้งาน User Admin ของทุกระบบภายในบริษัทฯ
2. เพื่อความมั่นคงและปลอดภัยจากความเสี่ยงต่างๆ ที่จะเกิดจากการโจรกรรม การคุกคามทางไซเบอร์

<u>ขั้นตอนการควบคุม</u>

1. ผู้ดูแล User Administrator ทุกระบบจะเป็นทาง IT Infrastructure หรือผู้ที่ได้รับมอบหมายเท่านั้นในการทำหน้าที่เข้าระบบ ส่วนรหัสสำรองมีการจะเก็บไว้ในตู้เซฟซึ่งจะนำมาใช้ในกรณีฉุกเฉินเท่านั้น
2. การใช้งาน Administrator จะต้องบันทึกทุกครั้งที่ใช้งาน
3. การตั้ง Password ให้เป็นไปตาม Strong Password Standard มีความยาวอย่างน้อย 8 ตัวอักขระประกอบไปด้วย ตัวอักษรตัวใหญ่ ตัวอักษรตัวเล็ก ตัวเลข และอักขระพิเศษ อย่างน้อย 1 ตัวประกอบกัน
4. การตั้งค่าหรือกำหนดให้เปลี่ยน Password ทุก 90 วันหรือน้อยกว่า
5. ให้ออกจากระบบ หรือ Log out ทันทีที่เลิกปฏิบัติการ
6. มีการตรวจสอบการใช้งานโดยผู้บริหารฝ่าย

7. มีการสอบทานสิทธิทุกปี
8. กรณีที่มีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญ มีการให้สิทธิผู้ใช้งานรายอื่นให้สามารถเข้าถึง หรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การ Share file จะต้องได้รับอนุญาตจากประธานกรรมการบริหาร และจะต้องเป็นการให้สิทธิเฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิดังกล่าวในกรณีที่ไม่มีความจำเป็นแล้ว โดยมีกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
9. ในกรณีที่มีความจำเป็นต้องให้สิทธิบุคคลอื่น ให้มีสิทธิใช้งานระบบคอมพิวเตอร์ในลักษณะฉุกเฉินหรือชั่วคราว ต้องมีขั้นตอนหรือวิธีปฏิบัติและต้องมีการขออนุมัติจากผู้มีอำนาจหน้าที่รวมทั้งประธานกรรมการบริหารทุกครั้ง ลงบันทึกเหตุผล และความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

<u>หมวดที่ 2</u> นโยบายการใช้ Hardware และ Software (Hardware and Software Policy)

<u>วัตถุประสงค์</u>

1. เพื่อที่จะสร้างความมั่นใจให้พนักงานทุกคนได้รับรู้ถึงแนวทางปฏิบัติการใช้งานของคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง ระบบคอมพิวเตอร์ (Applications/Systems ต่างๆ) รวมถึงสิ่งที่ต่อเชื่อมเข้ากับเครือข่ายของบริษัทและเครือข่ายอินเทอร์เน็ต อย่างเพียงพอ และปฏิบัติตามการใช้งานให้เหมาะสม และเป็นไปอย่างประสิทธิภาพ
2. เพื่อให้ปฏิบัติตามการใช้งานภายใต้ระเบียบข้อบังคับ และข้อกำหนดกฎหมาย

<u>แนวทางปฏิบัติ</u>

1. ปฏิบัติตามข้อปฏิบัติการใช้งานต่างๆ ของบริษัทฯ และปฏิบัติภายใต้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฉบับล่าสุด
2. ไม่อนุญาตนำเครื่องคอมพิวเตอร์ หรือ Software ส่วนตัวมาใช้ในบริษัทโดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษร
3. ไม่อนุญาตลงโปรแกรมหรือ Software ที่ไม่ถูกต้องตามกฎหมาย หรือ ไม่ได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ ไปลงในเครื่องเด็ดขาด
4. ไม่อนุญาตให้ถอดถอนระบบของบริษัทฯ ออกโดยไม่ได้รับอนุญาต โดยเฉพาะระบบรักษาความปลอดภัยต่างๆ เช่น ระบบป้องกันไวรัส
5. ไม่อนุญาตให้นำ Software ที่ซื้อมา ไปทำซ้ำ หรือ โอนย้าย หรือ นำไปจำหน่าย โดยไม่ได้รับอนุญาตจากผู้มีอำนาจหรือเจ้าของลิขสิทธิ์ และให้ปฏิบัติเป็นไปตาม Licenses Agreement

2.1 มาตรฐานการบริหารการจัดการ Software (Software Management Standard)

<u>วัตถุประสงค์</u>

1. เพื่อเป็นมาตรฐานในปฏิบัติในการควบคุมใช้งาน Software ภายในบริษัทฯ ให้ใช้งานได้ประสิทธิภาพสูงสุด
2. เพื่อควบคุมความปลอดภัยจากความเสี่ยงต่างๆ ที่จะเกิดจากการโจรกรรม การคุกคามทางไซเบอร์จากการใช้ Software ที่ไม่ถูกต้อง
3. เพื่อเป็นไปตามกฎหมายลิขสิทธิ์ Software ภายใต้ พรบ.คอมพิวเตอร์ฉบับล่าสุด

<u>ขั้นตอนการควบคุม</u>

1. ผู้ดูแลทั้ง IT Infrastructure และ IT Development เป็นผู้รวบรวม และดูแลในการปรับปรุงรายการ Software ให้เป็นปัจจุบันอย่างสม่ำเสมอ
2. บริษัทฯ ไม่อนุญาตให้นำ Software ที่ไม่ถูกกฎหมาย หรือ Software ที่ไม่มีลิขสิทธิ์มาใช้งานเด็ดขาด
3. การนำ Application หรือ โปรแกรมต่างๆ ที่ถูกกฎหมายมาลงจะต้องได้รับอนุญาตจากผู้บริหารสารสนเทศเป็นอย่างน้อย
4. ผู้ดูแล IT infrastructure จะมีการสุ่มตรวจ Software อย่างสม่ำเสมอ อย่างน้อยปีล่ะ 1 ครั้ง
5. หากเจอว่ามีการลง Software ไม่ได้รับอนุญาต จะมีการเตือนเจ้าของเครื่อง พร้อมรายงาน ให้ผู้บริหาร IT ทราบ
6. หากพบว่ามีการทำผิดเรื่องเดิมอีกครั้ง นอกจากเตือนเจ้าของเครื่องนั้นแล้ว จะต้องมีการรายงานไปยังผู้บังคับบัญชาโดยตรง พร้อมทั้งรายงานไปยังผู้บริหาร IT ทราบ
7. หากพบว่ามีการทำผิดเรื่องเดิมเป็นครั้งที่ 3 จะต้องมีการรายงานไปยังผู้บังคับบัญชาโดยตรง พร้อมทั้งรายงานไปยังประธานเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศทราบ และให้ประธานเจ้าหน้าที่บริหารพิจารณาตามนโยบายบริษัทฯ

2.2 มาตรฐานการซ่อมและการตัดออกจากระบบบัญชีทรัพย์สิน (Repairing and Disposal Standard)

<u>วัตถุประสงค์</u>

1. เพื่อที่จัดการทรัพย์สินทางคอมพิวเตอร์และอุปกรณ์ ให้ถูกต้องเป็นไปตามกฎระเบียบของบริษัท ฯ และภายใต้กฎหมาย
2. เพื่อที่เป็นขั้นตอนในการปฏิบัติงานการการยกเลิกใช้งานหรือการตัดทรัพย์สินสารสนเทศประเภทอุปกรณ์เทคโนโลยีสารสนเทศออกจากระบบ ให้ถูกต้องตามมาตรฐานการทำงานของบริษัทฯ

ขั้นตอนการทำงาน

1. กระบวนการนำทรัพย์สิน IT ออกจากระบบ
   1.1 ทำคำขอตัดทรัพย์สินออกจากทะเบียนทรัพย์สินไปยังแผนกบัญชี
      1.1.1 กรณีบริจาค
      1.1.2 กรณีขาย
      1.1.3 กรณีทำลาย
   1.2 IT Infrastructure จัดการทำการทำลายข้อมูลโดยมีเงื่อนไข
      1.2.1 กรณีที่เป็นคอมพิวเตอร์ หรือ Server ให้ Format หรือ Low Level Format 3 ครั้ง
      1.2.2 กรณีทีเป็น แท็บเล็ต ให้ Reset all Settings หรือ Erase all Settings
      1.2.3 กรณีที่เป็น Memory ในเครื่องพิมพ์ หรือ อุปกรณ์เครือข่าย ให้ทำการลบหรือ Reset
      1.2.4 หากไม่สามารถ Reset หรือ Format ได้ ให้ทำการทุบทิ้ง
   1.3 ทางแผนกบัญชีจะทำการตัดทรัพย์สินออกจากทะเบียนทรัพย์สิน
   1.4 IT Infrastructure ทำการบันทึกในระบบการจัดการทรัพย์สินของ IT
2. การส่งซ่อม
   2.1 ส่งซ่อม
      2.1.1 ค่าซ่อมจะต้องน้อยกว่า 40% ของราคาสินค้าที่ซื้อ และมีค่าน้อยกว่ามูลค่าทรัพย์สิน (Book Value) ณ ปัจจุบัน

3.3 มาตรฐานการพัฒนาระบบสารสนเทศ (System Development Life Cycle Standard)

วัตถุประสงค์

1. เพื่อให้บริษัทฯ มีมาตรฐานในการพัฒนาระบบสารสนเทศ การกำหนดคุณสมบัติของระบบคอมพิวเตอร์ (Configuration)
2. เพื่อให้การพัฒนาระบบสารสนเทศ เป็นไปตามวงจรการพัฒนาระบบสารสนเทศ (System Development Life Cycle-SDLC) จากจุดเริ่มต้น จนกระทั่งยกเลิกการใช้ระบบ ด้วยการควบคุม รวมทั้งการบำรุงรักษา และการปรับปรุงระบบ
3. เพื่อให้มีแนวปฏิบัติตามการเปลี่ยนแปลงด้านเทคโนโลยี และสอดคล้องกับกลยุทธ์ขององค์กรในการสร้างความได้เปรียบในการแข่งขันทางธุรกิจ

ขั้นตอนการจัดทำโครงการสารสนเทศ

1. Idea Phase เป็นขั้นตอนเริ่มต้นโครงการ/การวางแผน/การสำรวจความต้องการผู้ใช้งาน (User Requirements Specification) ผู้ขอจัดทำโครงการ จะต้องกรอกเอกสารรายละเอียดต่างๆ ตามแบบฟอร์ม การขอจัดทำโครงการให้ครบถ้วน ความจำเป็นที่ต้องใช้ และกรอกรายละเอียดหัวข้อโครงการ ระยะเวลาในการดำเนินการ รวมถึงค่าใช้จ่ายในการดำเนินโครงการและรายละเอียดอื่นๆ

2. Feasibility Phase จะเป็นขั้นตอนเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศนำข้อมูลที่ได้จากผู้ขอมาวิเคราะห์ความเป็นไปได้ ภายใต้ข้อบังคับ กฎหมายต่างๆ ความจำเป็นทางธุรกิจ ความเสี่ยง รวมทั้งความคุ้มทุนที่จะลงทุน (ROI) ส่งให้ผู้บริหารพิจารณาอนุมัติ
3. Design Phase เป็นขั้นตอนที่ทาง Developer มาวิเคราะห์ (Analysis) และออกแบบ (Design) ส่วนต่อประสานผู้ใช้งาน (User Interface) การภาษาที่พัฒนา ฐานข้อมูลที่ใช้ (Database) ความปลอดภัย (Security) และ Network เป็นต้น พร้อมวางแผนกำหนดการต่างๆ มาให้ผู้ขอใช้มาพิจารณารับรอง กำหนดเป็น System Design Specification ในการตอนนี้จะต้องมีแผนการทดสอบระบบ
4. System Development เป็นขั้นตอนการพัฒนาระบบจาก User Requirement และ System Design Specification ตามแผนงานที่กำหนดไว้ ด้วยเครื่องมือที่ Developer นำมาใช้ภายใต้เอกสารที่เข้าใจได้ง่าย
5. System Testing/Verification การทดสอบระบบเป็นการประกันคุณภาพของการพัฒนาระบบให้เป็นไปตาม User Requirements Specification ค้นหาข้อผิดพลาด ป้องกันการเกิดข้อผิดพลาด (Error/Bug) โดยที่การทดสอบประกอบด้วย การทดสอบแบบ Function (Functional Testing) โดย Developer เพื่อทดสอบโดยองค์รวมของระบบ แล้วสร้าง Test
6. System Installation การติดตั้งระบบ/ (Data Conversion/Migration) การนำข้อมูลเข้าระบบทางฝ่ายเทคโนโลยีสารสนเทศทำการติดตั้งระบบที่เครื่องคอมพิวเตอร์แม่ข่าย รวมถึงการกำหนดค่าเริ่มต้นต่างๆ ของระบบเพื่อให้พร้อมในการใช้งานจริง ซึ่งอาจจะมีการนำข้อมูลจากระบบเดิมที่ต้องการนำเข้าระบบ นำส่งให้ฝ่ายเทคโนโลยีสารสนเทศทำการจัดเตรียมข้อมูลด้วย Format ต่างๆ สำหรับนำเข้าสู่ระบบงานใหม่ เมื่อมีการนำเข้าสู่ระบบงานใหม่ เจ้าของข้อมูลต้องทำการตรวจสอบข้อมูลเปรียบเทียบกับระบบงานเดิมว่าถูกต้อง ครบถ้วน
7. Operations and Maintenance เป็นขั้นตอนหลังจากที่ระบบได้ใช้งานจริงไปแล้ว โดยปกติจะมีการติดตามอย่างใกล้ชิดในระยะเวลา 1-3 เดือน ว่าระบบมีข้อผิดพลาด Error/Bug เล็กๆ หรือ ความล่าช้าในการประเมินผล แต่หากประเมินแล้ว เป็นปัญหาใหญ่เกิน และไม่สามารถแก้ไขได้ อาจจะพิจารณาไปเริ่มขั้นตอน ที่ 1-6 ใหม่ (New Development Cycle)
8. Change Management เป็นขั้นตอนหลังจากที่ระบบได้ใช้งานไปแล้ว เกิดปัญหาไม่ว่าจะมีข้อผิดพลาดไม่ว่าจะเล็กหรือใหญ่ก็ตาม หากจำเป็นต้องแก้ไขระบบ หรือ เขียนโปรแกรมเพิ่มเติม จะต้องส่งคำขอเพื่อเปลี่ยนแปลง หรือ แก้ไขระบบ ซึ่งจำเป็นต้องพิจารณาตามการพัฒนาระบบข้อ 1-6 ใหม่

9. Manual & Training การจัดทำคู่มือและฝึกอบรม ดำเนินการโดยฝ่ายเทคโนโลยีสารสนเทศเป็นฝ่ายจัดทำคู่มือสำหรับผู้ดูแลระบบ (System/Programmer Manual) และคู่มือการใช้งานระบบ (User Manual) พร้อมอบรมการใช้งานระบบงานใหม่
10. Harvest การยกเลิกระบบ จะต้องผ่านการตัดสินใจของคณะกรรมการบริหาร และวางแผนการยกเลิกระบบต่อไป และทุกฝ่ายลงลายมือชื่อเพื่อรับทราบการยกเลิกนั้น

หมวดที่ 3 การรักษาความมั่นคงปลอดภัยทางสารสนเทศ เว็บไซต์ อีเมล แชท (Information, Website, E-mail and Instant Messaging Security (Chat) Policy)

วัตถุประสงค์

1. เพื่อกำหนดแนวทาง หลักการ ข้อกำหนดการบริหารจัดการด้านความมั่นคงปลอดภัยทางสารสนเทศ เว็บไซต์ อีเมล และแชท ให้มีความมั่นคงปลอดภัยทั้งบุคคลภายใน และภายนอกบริษัทฯ
2. เพื่อสร้างความเข้าใจให้พนักงานหรือบุคคลที่ใช้อุปกรณ์เชื่อมต่อระบบเครือข่ายของบริษัทฯ ให้ปฏิบัติตามนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ และกฎหมายคอมพิวเตอร์ได้อย่างถูกต้องและเหมาะสม
3. เพื่อป้องกันหรือลดความเสี่ยงจากการโจรกรรม บุกรุก ทำลาย แทรกแซง

แนวทางปฏิบัติ

1. ให้ปฏิบัติตามนโยบายการใช้งานคอมพิวเตอร์ (Computer Usage Policy) ของบริษัทฯ
2. ให้ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์
3. ไม่อนุญาตให้ส่งข้อมูลที่เป็นความลับผ่านช่องทางที่ไม่ปลอดภัยหรือช่องทางที่ไม่มีการเข้ารหัส (Encryption) เช่น ช่องทางแชทสาธารณะ
4. ผู้ส่ง ต้องมั่นใจถึงข้อความที่ส่งนั้นไม่มีผลกระทบ หรือทำให้เสื่อมเสียต่อผู้รับ หรือบริษัทฯ ภายใต้นโยบายของบริษัทฯ หรือ กฎหมาย
5. บริษัทฯ อนุญาตให้ใช้งานส่วนตัวให้น้อยที่สุดเท่าที่จำเป็นเท่านั้น
6. ไม่อนุญาตให้ใช้ในเรื่องเกี่ยวกับสถาบัน การเมืองการปกครอง ศาสนา ลามกอนาจาร การพนัน เกม หรือ เรื่องที่ไม่เกี่ยวข้องกับบริษัทฯ ทั้งทางตรงและทางอ้อม รวมทั้งเรื่องที่มีผลประโยชน์ทับซ้อนกับบริษัทฯ ไม่ว่าจะเป็นข้อความ เสียง และรูปภาพ เด็ดขาด
7. ไม่อนุญาตให้ใช้รูป หรือ ข้อความความ ที่ไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์
8. บริษัทฯ มีสิทธิภายใต้ตามกฎหมายในการตรวจสอบ และเข้าถึง การใช้สารสนเทศ เว็บไซต์ อีเมล และแชทต่างๆ ได้ โดยรับอนุมัติจากผู้บริหารสูงสุดเท่านั้น

หมวดที่ 4 นโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Policy)

ภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 หรือ พ.ร.บ. ไซเบอร์

วัตถุประสงค์

1. เพื่อกำหนดแนวทาง หลักการ ข้อกำหนดการบริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์ ให้มีความมั่นคงปลอดภัยทั้งบุคคลภายในและภายนอกบริษัทฯ
2. เพื่อสร้างความเข้าใจให้พนักงานหรือบุคคลที่ใช้อุปกรณ์เชื่อมต่อระบบเครือข่ายของบริษัท ฯ ให้ปฏิบัติตามนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ และกฎหมายคอมพิวเตอร์ได้อย่างถูกต้องและเหมาะสม
3. เพื่อให้พนักงานและผู้ที่ใช้อุปกรณ์เชื่อมต่อเข้าระบบเครือข่ายคอมพิวเตอร์ของบริษัท ฯ สามารถใช้งานระบบคอมพิวเตอร์ของบริษัทฯ ได้อย่างถูกต้องและเหมาะสม
4. เพื่อป้องกัน หรือลดความเสี่ยงจากการโจรกรรม บุกรุก ทำลาย แทรกแซง หรือสิ่งที่สร้างความเสียหายต่อบริษัท หรือทำให้ธุรกิจของบริษัทฯ หยุดชะงัก

ความหมาย

1. ความลับ (Confidentiality) : การป้องกันความลับของข้อมูล โดยการป้องกันการเข้าถึงและการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต ทั้งข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นของบริษัทฯ
2. ความมั่นคง (Integrity) : การทำให้มั่นใจว่าข้อมูลของบริษัทฯ ไม่มีการแก้ไข ดัดแปลง หรือ ทำลายก่อนได้รับอนุญาต
3. ความพร้อมใช้งาน (Availability) : การทำให้มั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลและบริการได้อย่างรวดเร็วและเชื่อถือได้
4. ความรับผิดชอบ (Accountability) : การระบุหน้าที่รับผิดชอบของแต่ละบุคคลอย่างชัดเจน
5. การพิสูจน์ตัวตน (Authentication) : การทำให้มั่นใจสิทธิการเข้าใช้งานระบบคอมพิวเตอร์ และข้อมูลผ่านกระบวนการยืนยันตัวตนแล้ว
6. การกำหนดสิทธิ (Authorization) การทำให้มั่นใจว่าการให้สิทธิเข้าใช้งานระบบคอมพิวเตอร์ และข้อมูลเป็นไปตามสิทธิ และตามที่ได้รับอนุญาต
7. การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) การทำให้มั่นใจว่าผู้ที่มีส่วนเกี่ยวข้องในการทำธุรกรรมผ่านระบบคอมพิวเตอร์ และเครือข่ายไม่สามารถปฏิเสธได้ว่าไม่มีส่วนเกี่ยวข้องกับการทำธุรกรรมที่เกิดขึ้น

แนวทางปฏิบัติ

1. ต้องออกจากระบบ (Log off, Sign off) ทุกระบบเมื่อไม่ได้ใช้งานเป็นเวลานาน
2. ต้องปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพวงทันทีหลังเลิกงาน หรือไม่ได้ใช้งานต่อไป
3. ต้องล็อคหน้าจอหรือมี Screen Saver แบบกำหนดรหัสผ่าน หากไม่ได้ใช้งาน
4. ต้องตรวจสอบข้อมูลที่นำมาลงในเครื่องคอมพิวเตอร์ทุกครั้ง

5. ต้องได้รับอนุญาตจากผู้มีอำนาจในการลงโปรแกรมหรือระบบทุกครั้ง
6. ไม่ปิดหรือถอดถอนระบบป้องกันไวรัสหรือระบบป้องกันภัยต่างๆ และปรับปรุงให้ทันสมัยอยู่ตลอดเวลา
7. ต้องเก็บรักษารหัสผ่าน (Password) ทุกระบบเป็นความลับอยู่เสมอ ไม่ให้บุคคลอื่นนำไปใช้ หรือใช้ร่วมกัน เด็ดขาด โดยการตั้งรหัสผ่านให้เป็นไปตาม Password Standard ของบริษัทฯ

หมวดที่ 5 นโยบายการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Policy)

นโยบายการบริหารความต่อเนื่องทางธุรกิจ เป็นการวางแผนภายใต้สถานการณ์ฉุกเฉิน หรือภาวะฉุกเฉิน (Business Continuity Plan) เป็นการวางแผนจัดการกับเหตุการณ์ที่ไม่ได้มีการคาดการณ์ไว้ล่วงหน้า ที่มีผลต่อการดำเนินกิจการของบริษัทฯ อันได้แก่ ภัยธรรมชาติต่างๆ (น้ำท่วม, ภูเขาไฟระเบิด, แผ่นดินไหว เป็นต้น) โรคระบาด รวมทั้งเหตุการณ์รุนแรง หรือ การก่อการร้าย หรือ สงคราม และเหตุการณ์ที่ทำให้ระบบสารสนเทศขัดข้อง เป็นต้น

วัตถุประสงค์

1. เพื่อกำหนดและวางแผนให้บริษัทฯ สามารถดำเนินธุรกิจอย่างต่อเนื่องโดยไม่หยุดชะงัก ภายใต้สถานการณ์ฉุกเฉินทั้งภายนอกและภายในที่ได้กำหนดไว้
2. เพื่อเป็นการบริหารความเสี่ยง โดยการลดความเสี่ยงหรือผลที่จะเกิดขึ้นกับบริษัทฯ ให้น้อยที่สุด
3. เพื่อให้บริษัทฯ สามารถฟื้นฟูการดำเนินงานทางธุรกิจได้อย่างรวดเร็วหลังจากสถานการณ์กลับมาปกติ

แนวทางปฏิบัติ

1. **การวางแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan)** หมายถึง การจัดทำแผนการ ในการบริหารธุรกิจให้ดำเนินธุรกิจไปได้อย่างต่อเนื่อง ในสถานการณ์หรือ ภาวะฉุกเฉิน ทั้งภายในและภายนอก
2. **กำหนดบทบาท หน้าที่ และผู้รับผิดชอบในการจัดทำแผนความต่อเนื่องทางธุรกิจ** เป็นการกำหนดบทบาท หน้าที่ และผู้รับผิดชอบอย่างชัดเจน พร้อมข้อมูลติดต่อไว้เรียบร้อย
3. **การวิเคราะห์ความเสี่ยง และผลกระทบต่อธุรกิจ** เป็นกำหนดระดับความเสี่ยงและผลกระทบต่อธุรกิจตามลำดับความเสี่ยงสูงต่ำซึ่งการดำเนินธุรกิจไม่สามารถกระทำทุกอย่างได้ภายใต้สถานการณ์ฉุกเฉิน
4. **กำหนดสถานการณ์ความเสี่ยง** ได้แก่ สถานการณ์ที่ทำให้เกิดความเสี่ยง ได้แก่ น้ำท่วม ภูเขาไฟระเบิด แผ่นดินไหว โรคระบาด เหตุการณ์รุนแรง หรือ การก่อการร้าย หรือ สงคราม และเหตุการณ์ที่ทำให้ระบบเทคโนโลยีสารสนเทศขัดข้อง
5. **กำหนดแนวทางปฏิบัติ** เป็นการกำหนดแนวทางปฏิบัติให้สอดคล้องกับเหตุการณ์ความเสี่ยงต่างๆ เป็นคู่มือพร้อมทั้งทรัพยากร และเครื่องมือให้พร้อม
6. **ทดสอบและประเมิน** เป็นการนำแผนมาทดสอบในสถานการณ์จำลอง และทำการประเมินแผน แล้วปรับปรุงแผนให้เหมาะสม และสามารถใช้ได้จริง
7. **การนำไปปฏิบัติ** เมื่อปรับปรุงแก้ไขแผนเรียบร้อย ก็นำไปประกาศเป็นแผนเพื่อนำไปปฏิบัติจริงตามสถานการณ์ที่เกิดขึ้นจริง

5.1 มาตรฐานการสำรองและกู้กลับข้อมูล (Backup and Recovery Standard)

<u>วัตถุประสงค์</u>

1. เพื่อให้บริษัทฯ สามารถดำเนินธุรกิจไปได้อย่างต่อเนื่อง ในสถานการณ์ที่ไม่ปกติหรือสถานการณ์ฉุกเฉิน
2. เพื่อที่ลดความเสี่ยงที่จะเกิดขึ้น และรับมือกับความเสี่ยงต่างๆ ที่ทำให้บริษัท ฯ หยุดชะงัก ได้อย่างมีประสิทธิภาพ
3. เพื่อให้มีแผนที่เป็นระบบเป็นขั้นตอนในการรองรับกับเหตุการณ์ที่จะเกิดขึ้น รวมทั้งทดลอง และปรับปรุงให้ดีขึ้นเหมาะสม

<u>ความหมาย</u>

1. Business Continuity Plan (BCP) เป็นการวางแผนความต่อเนื่องของธุรกิจ จากภาวะคุกคาม และความเสี่ยงที่เกิดจากสถานการณ์ฉุกเฉิน ที่ไม่ได้มีการคาดการณ์ไว้ล่วงหน้า เช่น ภัยธรรมชาติต่างๆ โรคระบาด การก่อการร้าย หรือสงคราม เป็นต้น
2. Business Recovery Plan (BRP) หรือ Disaster Recovery Plan (DRP) เป็นแผนฟื้นฟูภัยพิบัติ ได้แก่ ภัยธรรมชาติต่างๆ เช่น น้ำท่วม ภูเขาไฟระเบิด แผ่นดินไหว รวมทั้งไฟไหม้ และการก่อการร้าย การกำหนดโอกาสเหตุการณ์ที่จะเกิด และผลกระทบที่จะได้รับ เพื่อประเมินความเสี่ยง

โอกาสที่จะเกิดเหตุการณ์		ผลกระทบที่ได้รับ		
ระดับ	ความเป็นไปได้	ระดับ	ความเสียหายที่อาจเกิดขึ้นแก่องค์กร	ระยะเวลาหยุดดำเนินงาน
H	สูง	H	เสียหายมากจนต้องปิดกิจการชั่วคราว	มากกว่า 1 วัน
L	ต่ำ	L	เสียหายแต่สามารถควบคุมสถานการณ์ได้	ไม่เกิน 1 วัน

3. Backup เป็นการสำรองข้อมูลเพื่อลดความเสี่ยงที่จะเกิดขึ้น ประกอบไปด้วย Daily Backup, Weekly Backup, Monthly Backup
    1. Full Backup เป็นการสำรองข้อมูลทั้งหมด ทั้งระบบ หรือ เฉพาะข้อมูลเพียงอย่างเดียว
    2. Incremental / Differential Backup เป็นการสำรองข้อมูลส่วนเพิ่มหรือส่วนต่างจากที่ได้ทำการ Full Backup มาแล้ว
    3. Recovery เป็นการนำข้อมูลที่ได้ทำการสำรองเอาไว้ นำมาลงในพื้นที่ได้จัดเตรียมไว้
    4. Service Level Agreement (SLA) เป็นข้อตกลงการบริการที่จะรักษาระดับคุณภาพการบริการกับบริษัทฯ กับแต่ละ Outsource Service Provider
    5. Retention Period เป็นระยะเวลาของข้อมูลทั้งหมดที่จะทำการ Recovery

ขั้นตอนการทำงาน

1. กระบวนการยอมรับและการประเมินความเสี่ยงของระบบ
   1.1 บุคคลที่เกี่ยวข้องต้องยอมรับว่าการ Backup (สำรองข้อมูล) และการ Recovery นั้นสำคัญ และจำเป็นต้องมี
   1.2 การ Backup ระบบได้มีการประเมินความตามความเสี่ยงดังต่อไปนี้ โดยจะใช้ระบบ หรือ Application ที่มีความเสี่ยงสูงเท่านั้น ซึ่งการประเมินนั้นกระทำประจำปี
   1.3 หากมีการประเมินใหม่ให้ผู้ที่ต้องการเปลี่ยนทำการส่งใบคำขอเปลี่ยนมาให้ IT
2. กระบวนการ Backup และ Retention จะต้องมีการพิจารณากันทุกปีเพื่อให้สอดคล้องกับธุรกิจ และความเสี่ยงที่จะเกิดขึ้นหรือข้อกำหนดกฎหมาย
3. การ Backup ที่ได้ทำการประเมินความเสี่ยงของระบบ
4. Backup Log จะต้องมีการตรวจสอบทุกวันตามใบบันทึกการสำรองข้อมูล
   4.1 หากมีข้อผิดพลาดในการ Backup จะต้องมีการบันทึก และแก้ไข หากมีข้อผิดพลาดหรือสำรองข้อมูลไม่ได้ติดต่อ 3 วันจะต้องรายงานต่อผู้บริหารระดับสูง
5. กระบวนการ Recovery
6. กระบวนการทดสอบ (Testing) และการตรวจสอบ (Verification)
   6.1 กระบวนการทดสอบเป็นไปตามคู่มือ/ขั้นตอนของแต่ละแผนกที่เกี่ยวข้อง มีการตรวจสอบ และปรับปรุงให้ถูกต้องเสมอ
7. กระบวนการประเมิน (Evaluation) และปรับปรุง (Improvement) จะมีการประเมินและปรับปรุงหลังจากการทดสอบ เพื่อนำไปประกาศใช้เป็นแผนฉุกเฉินฉบับล่าสุดต่อไป
8. กระบวนการนำไปใช้ (Execution)
   8.1 แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) ฝ่ายเทคโนโลยีสารสนเทศมีการทบทวนอย่างน้อยปีละ 1 ครั้ง
   8.2 เมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบอย่างมีนัยสำคัญ เพื่อให้ BCP เป็นปัจจุบันและสอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป เช่น การเปลี่ยนแปลงพนักงานที่มีหน้าที่รับผิดชอบในการดำเนินงานตามแผน

หมวดที่ 6 นโยบายการกำกับดูแลการใช้งาน Cloud (Cloud Computing Policy)

การใช้บริการบริการเช่าใช้ระบบคอมพิวเตอร์ และทรัพยากรแบบครบวงจร โดยสามารถเลือกเช่าฮาร์ดแวร์และ/หรือซอฟต์แวร์ ไม่ว่าจะเป็นระบบเครือข่าย (Server) การติดตั้งฐานข้อมูล (Database) การทดสอบระบบ (Testing) การประมวลผลที่รองรับได้หลากหลายระบบปฏิบัติการ (Platform) ตลอดจนถึงการจัดเก็บข้อมูลทั้งหมดของผู้ใช้บริการ (Storage) เพื่อเพิ่มประสิทธิภาพและประสิทธิผลในการบริหารจัดการต้นทุนด้านเทคโนโลยี

นอกจากนั้นการประยุกต์ใช้งาน Cloud Computing เป็นรูปแบบการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์เพื่อบริหารจัดการความต้องการทรัพยากรในการประมวล ผลตามความต้องการของผู้ใช้งาน ซึ่งอาจมีการกำหนดขอบเขตการใช้งานทรัพยากรการประมวลผลอย่างเฉพาะเจาะจงสำหรับผู้หนึ่งผู้ใด หรืออาจมีการใช้งานร่วมกันของกลุ่มผู้ใช้งานและนิติบุคคล เพื่อประสิทธิภาพในการใช้บริหารจัดการทรัพยากรและต้นทุนอย่างเหมาะสม การใช้งานทรัพยากรร่วมกันบนเครือข่ายส่งผลให้เกิดความซับซ้อนด้านเทคโนโลยี รวมถึงความเสี่ยงอันอาจจะเกิดขึ้นต่อระบบสารสนเทศที่ถูกจัดเก็บอยู่บนเครือข่ายที่มีการบริหารจัดการโดยบุคคลภายนอก หรือผู้ให้บริการ Cloud Computing

<u>วัตถุประสงค์</u>

1. เพื่อให้บริษัทฯ มีกรอบการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่สอดคล้องกับความต้องการของกิจการรวมทั้งดูแลให้มีการนำเทคโนโลยีสารสนเทศในส่วนที่เป็นเทคโนโลยีที่เกี่ยวกับบริการคลาวด์ มาใช้ในการสนับสนุนและพัฒนาการดำเนินธุรกิจ การบริหารความเสี่ยง
2. เพื่อให้กิจการสามารถบรรลุวัตถุประสงค์และเป้าหมายหลักของกิจการ โดยมีการใช้ทรัพยากรและการบริหารจัดการความเสี่ยงอย่างเหมาะสม สอดคล้องกับการกำกับดูแลกิจการ

<u>ความหมาย</u>

1. Cloud Service เป็นการใช้บริการบริการเช่าใช้ระบบคอมพิวเตอร์ และทรัพยากรแบบครบวงจร โดยสามารถเลือกเช่าฮาร์ดแวร์และ/หรือซอฟต์แวร์
2. SaaS (Software-as-a-Service) หมายถึง บริการด้านแอปพลิเคชันที่ทำงานบนโครงสร้างพื้นฐานระบบ Cloud Computing ซึ่งผู้ใช้บริการสามารถเข้าใช้งานแอปพลิเคชันผ่านเครือข่าย ผ่านโปรแกรมบนอุปกรณ์ของผู้ใช้บริการ เช่น เว็บเบราว์เซอร์ แอปพลิเคชันบนมือถือ เป็นต้น โดยผู้ให้บริการทำหน้าที่บริหารจัดการโครงสร้างพื้นฐานระบบคลาวด์ ซึ่งครอบคลุมถึง ความปลอดภัยทางกายภาพระบบปฏิบัติการ ระบบเครือข่าย ระบบจัดเก็บข้อมูล รวมถึงค่าพื้นฐานของแอปพลิเคชัน
3. PaaS (Platform-as-a-Service) หมายถึง บริการด้านแฟลตฟอร์มที่ทำงานบนโครงสร้างพื้นฐานระบบคลาวด์ ซึ่งผู้ใช้บริการสามารถเข้าแฟลตฟอร์มในการพัฒนาแอปพลิชั่น โดยผู้ให้บริการทำหน้าที่บริหารจัดการโครงสร้างพื้นฐานระบบคลาวด์ ซึ่งครอบคลุมถึง ความปลอดภัยทางกายภาพระบบปฏิบัติการ ระบบเครือข่าย และระบบให้บริการ เช่น เว็บเซอร์วิส ระบบจัดการฐานข้อมูล เป็นต้น อย่างไรก็ตาม การควบคุมที่เกี่ยวกับการบริหารจัดการแอปพลิเคชัน เช่น การแก้ไขเปลี่ยนแปลงโปรแกรม ผู้ใช้บริการจะเป็นผู้ดำเนินการ
4. IaaS (Infrastructure-as-a-Service) หมายถึง บริการด้านโครงสร้างพื้นฐานระบบคลาวด์ที่มีการใช้งานทรัพยากรทางด้านระบบสารสนเทศร่วมกัน เช่น ระบบปฏิบัติการ ระบบเครือข่าย หรือระบบจัดเก็บข้อมูลโดยทางผู้ให้บริการทำหน้าที่ดูแลทางกายภาพ และทรัพยากรสารสนเทศที่ใช้ในการสนับสนุนการทำงานของโครงสร้างพื้นฐานระบบคลาวด์
5. Public Cloud หมายถึงโครงสร้างพื้นฐานระบบคลาวด์ที่เปิดให้ใช้งานผ่านเครือข่ายสาธารณะ

6. Private Cloud หมายถึง โครงสร้างพื้นฐานระบบคลาวด์ที่จัดเตรียมไว้สำหรับการใช้งานโดยหน่วยงานภายในองค์กรเดียวกัน
7. Hybrid Cloud หมายถึง โครงสร้างพื้นฐานระบบคลาวด์ที่ประกอบด้วยโครงสร้างพื้นฐานระบบคลาวด์ ที่แตกต่างกันตั้งแต่สองรูปแบบขึ้นไป (Public และ Private)

<u>แนวทางปฏิบัติ</u>

1. บริษัทฯ ได้กำหนดแนวทางการกำกับดูแลและบริหารจัดการการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์ตามความต้องการของผู้ใช้งาน หรือ Cloud computing ที่ครอบคลุมกระบวนการสำคัญตั้งแต่การกำหนดกรอบการกำกับดูแลการใช้งาน Cloud Computing การกำหนดแนวทางเชิงกลยุทธ์ในการใช้งาน การกำกับผู้ให้บริการ ตลอดจนการยกเลิกหรือสิ้นสุดการใช้งาน
2. ประเภทของ Cloud Computing (Service Models) ที่อนุญาตให้ใช้งาน
   2.1 Software-as-a-Service (SaaS)
   2.2 Platform-as-a-Service (PaaS)
   2.3 Infrastructure-as-a-Service (IaaS)
3. รูปแบบของการนำไปใช้งาน (Deployment Models)
   3.1 Public Cloud
   3.2 Private Cloud
   3.3 Hybrid Cloud
4. การประเมินความเสี่ยงและการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัย ทางไซเบอร์จากการใช้งาน Cloud Computing
5. ประเมินความเสี่ยงและการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัย ทางไซเบอร์จากการใช้งาน Cloud Computing
   5.1 ความเสี่ยงด้านกลยุทธ์ เช่น ความเสี่ยงจากการพึ่งพิงผู้ให้บริการภายนอกและความสามารถในการเปลี่ยนแปลง ผู้ให้บริการ (Vendor/ Cloud Service Provider)
   5.2 ความเสี่ยงด้านปฏิบัติการ เช่น ระบบประมวลผลผิดพลาดจากระบบให้บริการหรือบุคลากร ผู้ให้บริการการใช้งานเทคโนโลยีร่วมกัน (Share Technology Risk) การละเมิดข้อกำหนดและข้อตกลงการใช้งาน Cloud Computing หรือความเสี่ยงจากการไม่สามารถเข้าถึงข้อมูลหรือการจำกัดการเข้าถึงของข้อมูลจากผู้ให้บริการ
   5.3 ความเสี่ยงด้านกฎหมาย เช่น การไม่ปฏิบัติตามกฎหมาย หลักเกณฑ์และข้อกำหนดของทางการ ทั้งภายในประเทศและต่างประเทศ
   5.4 ความเสี่ยงด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เช่น การเรียกใช้โปรแกรม (APIs) หรือช่องทาง บริหารจัดการที่ไม่ปลอดภัย

5.5 ความเสี่ยงด้านข้อมูลส่วนบุคคล (Data Privacy) และการรักษาความปลอดภัยของข้อมูล (Data Security)

5.6 ความเสี่ยงจากการใช้ผู้ให้บริการภายนอกที่มีการใช้ผู้ให้บริการภายนอกอื่นรับช่วงจัดการงาน (Sub-Contract)

6. จัดเตรียมและพัฒนาองค์ความรู้ด้านการบริหารจัดการ Cloud Computing ให้แก่ผู้ดูแลระบบ (Administrator) และบุคลากรที่เกี่ยวข้องอย่างเพียงพอ

7. กำหนดให้มีการประเมินและคัดเลือกผู้ให้บริการ ดังนี้

7.1 ตรวจสอบความพร้อมและพิจารณาความเหมาะสมของผู้ให้บริการเพื่อให้มั่นใจว่าผู้ให้บริการสามารถให้บริการได้อย่างต่อเนื่อง โดยคำนึงถึงปัจจัยสำคัญ ได้แก่ ความรู้ความสามารถ ประสบการณ์ ความสามารถทางการเงินที่สามารถ ในการให้บริการอย่างต่อเนื่อง

7.2 ประเมินมาตรฐานด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ได้แก่ การรักษาความลับข้อมูล (Confidentiality) ความถูกต้องเชื่อถือได้ของข้อมูลและระบบสารสนเทศ (Integrity) และความต่อเนื่องของการให้บริการ (Availability) เช่น ผลการประเมินมาตรฐานความปลอดภัยที่เป็นที่ยอมรับในสากล ได้แก่ ISO27001, ISO27017, PCI/DSS, TIA เป็นต้น

7.3 ประเมินผลรายงานการตรวจสอบโดยผู้ตรวจสอบที่เป็นอิสระ ด้านมาตรฐานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เช่น System and Organization Control (SOC) Report โดยพิจารณาถึงขอบเขตการตรวจสอบ ระยะเวลาที่ครอบคลุมในรายงานการตรวจสอบผลการตรวจสอบและประเด็นสำคัญในผลการตรวจสอบ ความสามารถและความน่าเชื่อถือของผู้ตรวจสอบ เป็นต้น

7.4 ประเมินความสอดคล้องกันของแนวทางการรักษาความต่อเนื่องของการให้บริการของผู้ให้บริการระบบ Cloud Computing และผลการประเมินผลกระทบทางธุรกิจ (Business Impact Analysis) ของระบบงานที่จะมีการใช้บริการบนระบบ Cloud Computing อันประกอบไปด้วย ระยะเวลากาหยุดชะงักของระบบให้บริการที่ยอมรับได้ (Maximum Tolerable Downtime: MTD) ระยะเวลาที่ยอมรับได้ในการกู้คืนระบบงานและข้อมูล (Recovery Time Objective: RTO) และชุดข้อมูลล่าสุดที่จะกู้คืนได้ (Recovery Point Objective: RPO)

7.5 ประเมินความเสี่ยงและแนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและความต่อเนื่องในการให้บริการในกรณีที่ผลการประเมินผู้ให้บริการไม่เป็นไปตามข้อกำหนดหรือมาตรฐานความปลอดภัยที่กำหนดไว้

8. จัดทำสัญญาและข้อตกลงการให้บริการ (Engage) ซึ่งมีรายละเอียดในเรื่องดังต่อไปนี้เป็นอย่างน้อย

8.1 หน้าที่และความรับผิดชอบของผู้ให้บริการ รวมถึงความรับผิดชอบต่อบริษัทในกรณีที่ผู้ให้บริการไม่สามารถปฏิบัติตามข้อตกลงได้

8.2 ขอบเขตการให้บริการ ประเภท และเงื่อนไขการให้บริการ

8.3 เงื่อนไขความเป็นเจ้าของข้อมูลของผู้ใช้บริการ สิทธิการใช้และลิขสิทธิ์ที่เกี่ยวข้องโดยผู้ใช้บริการควรเป็นเจ้าของสิทธิในข้อมูล

8.4 ข้อกำหนดด้านเงื่อนไขความรับผิดชอบในกรณีที่ผู้ให้บริการไม่สามารถให้บริการตามที่กำหนดในข้อตกลง ทั้งนี้บริษัทฯ ควรพิจารณาถึงเงื่อนไขการประเมินความเสียหาย รวมถึงข้อจำกัดในกรณีมีเงื่อนไขการจำกัด ความรับผิดในสัญญาระหว่างผู้ใช้บริการและผู้ให้บริการ

8.5 ข้อกำหนดด้านการเข้าถึงข้อมูลของผู้ให้บริการ ประกอบด้วยสิทธิการเข้าถึงและเงื่อนไขการเปิดเผยข้อมูล โดยผู้ให้บริการจากความยินยอมของผู้ใช้บริการ หรือการเปิดเผยข้อมูลโดยข้อกำหนดทางกฎหมายของประเทศ ที่ผู้ให้บริการไปตั้งศูนย์ข้อมูล ทั้งนี้ ต้องมีการแจ้งให้ผู้ใช้บริการรับทราบ

8.6 ข้อกำหนดด้านการสำรองข้อมูลและการจัดทำแผนสำรองฉุกเฉิน และแผนความต่อเนื่องทางธุรกิจสำหรับ การให้บริการ โดยมีเงื่อนไขที่ชัดเจนทางด้าน

8.6.1 สถานที่ในการกู้คืนข้อมูล (Location)

8.6.2 ระยะเวลากู้คืนระบบให้บริการ (Service Restoration)

8.6.3 ระยะเวลากู้คืนข้อมูล (Recovery Time Objective: RTO)

8.6.4 ชุดข้อมูลล่าสุดที่กู้คืนได้ (Recovery Point Objective: RPO)

8.7 ข้อกำหนดและเงื่อนไขการส่งมอบข้อมูลเมื่อมีการยกเลิก หรือสิ้นสุดการใช้บริการ

8.8 ข้อกำหนดด้านเงื่อนไขในกรณีที่ผู้ให้บริการจะให้ผู้ให้บริการรายอื่นรับดำเนินการช่วง (Subcontract of the Cloud Service Provider)

8.9 ข้อกำหนดและมาตรการป้องกันการรั่วไหลของข้อมูลที่อาจเกิดขึ้นจากผู้ให้บริการ

8.10 ข้อกำหนดด้านสิทธิในการตรวจสอบ (Rights to Audit)

8.11 ช่องทางติดต่อและผู้รับผิดชอบด้านปัญหาการใช้งานและเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการ

9. กำหนดให้มีการติดตามและประเมินผลด้านประสิทธิภาพ และการปฏิบัติตามข้อตกลงการให้บริการ อย่างน้อยปีละ 1 ครั้ง

10. การติดตามตรวจสอบประสิทธิภาพของการให้บริการ รวมทั้งมาตรการด้านความมั่นคงปลอดภัยให้สอดคล้องกับข้อกำหนดตามสัญญาต่างๆ หรือข้อตกลงในการให้บริการ

11. ต้องพิจารณาความเสี่ยงที่เกี่ยวข้องในการยกเลิกการใช้บริการระบบประมวลผลร่วมกันผ่านเครือข่ายอย่างรอบด้าน เพื่อกำหนดกลยุทธ์และจัดทำแผนการยกเลิกการใช้บริการอย่างเหมาะสม เพื่อป้องกันหรือลดผลกระทบ อันอาจจะเกิดขึ้นจากความเสี่ยง เช่น ความเสี่ยงด้านการหยุดชะงักของระบบให้บริการ ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความลับข้อมูล ความเสี่ยงด้านความถูกต้องของระบบประมวลผล เป็นต้น

หมวดที่ 7 นโยบายการบริหารความเสี่ยงทางเทคโนโลยีสารสนเทศ (IT Risk Management Policy)

ความเสี่ยงด้านเทคโนโลยีสารสนเทศมีอยู่ในทุกด้านของความเสี่ยงขององค์กรโดยเฉพาะอย่างยิ่งในองค์กรที่มีการใช้งานเทคโนโลยีสารสนเทศเป็นตัวผลักดันในการดำเนินธุรกิจ และมีบทบาทสำคัญที่เป็นโครงสร้างพื้นฐานที่ช่วยเสริมสร้างประสิทธิภาพในการกระบวนการดำเนินงานให้รองรับกลยุทธ์ทางธุรกิจ ที่ช่วยลดต้นทุนและเพิ่มศักยภาพในการแข่งขัน

วัตถุประสงค์

1. เพื่อเป็นแนวทางปฏิบัติในการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ
2. เพื่อให้การบริหารและจัดการความเสี่ยงขององค์กร มีการดำเนินการอย่างมีประสิทธิภาพ
3. เพื่อให้เป็นไปในแนวทางเดียวกันกับนโยบาย และการบริหารความเสี่ยงองค์กร (Enterprise Risk Management)

ความหมาย

1. IT Benefits/Value Enhancement Risk คือความเสี่ยงอันเนื่องมาจากการพลาดโอกาสในการใช้เทคโนโลยีสารสนเทศให้เกิดประสิทธิภาพ และประสิทธิผลต่อการดำเนินงาน หรือสร้างนวัตกรรมให้แก่องค์กร รวมถึงความเสี่ยงอันเนื่องมาจากเทคโนโลยีสารสนเทศที่ไม่ตอบสนองต่อการดำเนินธุรกิจ ซึ่งส่งผลโดยตรงต่อศักยภาพในการแข่งขันของผู้ประกอบธุรกิจ
2. IT Programmer and Project Delivery Risk คือความเสี่ยงอันเนื่องมาจากการไม่สามารถนำเทคโนโลยีสารสนเทศมาใช้ในการพัฒนาบริการหรือผลิตภัณฑ์ใหม่โดยรวมถึงความเสี่ยงที่ไม่สามารถจัดการโครงการได้อย่างมีประสิทธิภาพ หรือตามเป้าหมายที่กำหนด
3. IT Operations and Services Delivery Risk คือความเสี่ยงอันเนื่องมาจากการปฏิบัติงานประจำวันทางด้านเทคโนโลยีสารสนเทศ เช่น ความเสี่ยงสืบเนื่องมาจากการควบคุมที่ไม่เพียงพอ หรือมีการดำเนินงานที่อาจขัดต่อกฎหมายและระเบียบข้อบังคับต่างๆ

แนวทางปฏิบัติ

1. นโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดำเนินการสอดคล้องกับนโยบายการบริหารความเสี่ยงของบริษัทฯ ซึ่งมีการสื่อสารไปยังผู้ที่เกี่ยวข้อง รวมทั้งต้องมีการทบทวนและปรับปรุงอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง และต้องทบทวน โดยไม่ชักช้าเมื่อมีเหตุการณ์ใดๆ ซึ่งอาจส่งผลกระทบต่อการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ โดยควรระบุ ระเบียบวิธีปฏิบัติและกระบวนการที่สอดคล้องกับนโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่วางไว้ ทั้งนี้นโยบายการบริหารความเสี่ยงทางเทคโนโลยีสารสนเทศ ควรมีเนื้อหาครอบคลุมกระบวนการบริหารความเสี่ยง

2. การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ พิจารณาความเสี่ยงที่เป็นไปได้ทั้งหมด โดยกำหนดสถานการณ์ความเสี่ยง และปัจจัยความเสี่ยงที่เหมาะสม ซึ่งการกำหนดกระบวนการในการเก็บข้อมูล แยกหมวดหมู่ และวิเคราะห์ข้อมูลเกี่ยวกับความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ อาจจัดแบ่งตามประเภทของเหตุการณ์ ประเภทของความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ และปัจจัยความเสี่ยงต่างๆ ทั้งนี้ ควรพิจารณารวมถึงความเสี่ยงทางด้านเทคโนโลยีที่เกิดขึ้นใหม่ เช่น ความเสี่ยงทางด้านไซเบอร์ เป็นต้น
   2.1 รวบรวมและวิเคราะห์ข้อมูลความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจมีผลต่อการดำเนินงานและความสำเร็จของแผนกลยุทธ์ทางธุรกิจขององค์กร รวมทั้งแผนกลยุทธ์ทางด้านเทคโนโลยีสารสนเทศ
   2.2 มีการบันทึกข้อมูลสภาพแวดล้อมการดำเนินงานทั้งภายในและภายนอกเพื่อใช้ประกอบในการประเมินความเสี่ยง โดยสภาพแวดล้อมการดำเนินงานภายในอาจประกอบด้วย แผนกลยุทธ์และนโยบายทางด้านเทคโนโลยีสารสนเทศ โครงสร้างองค์กรทางด้านเทคโนโลยีสารสนเทศ และทรัพย์สินทางด้านเทคโนโลยีสารสนเทศ ในขณะที่สภาพแวดล้อมการดำเนินงานภายนอกอาจประกอบด้วยกฎระเบียบข้อบังคับต่างๆ ที่เกี่ยวข้อง และแนวโน้มทางด้านเทคโนโลยีสารสนเทศในกลุ่มธุรกิจ
   2.3 สำรวจและวิเคราะห์ข้อมูลความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ รวมทั้งผลกระทบหรือความเสียหายในอดีต โดยอาจมีการรวบรวมข้อมูลมาจากภายนอก ข้อมูลแนวโน้มธุรกิจ ข้อมูลของบริษัทอื่นๆ ในธุรกิจเดียวกัน หรือ มีการแบ่งปันข้อมูลกันระหว่างธุรกิจ
   2.4 บันทึกข้อมูลเหตุการณ์ความเสี่ยงที่ส่งผลหรืออาจส่งผลต่อการใช้เทคโนโลยีสารสนเทศ การส่งมอบระบบงานหรือโครงการทางด้านเทคโนโลยีสารสนเทศ รวมทั้งการปฏิบัติงานและให้บริการทางด้านเทคโนโลยีสารสนเทศ ทั้งนี้อาจรวมถึงข้อจำกัด ประเด็นปัญหา และการติดตามการแก้ไขปัญหาด้วย
   2.5 มีการจัดการและจำแนกประเภทของข้อมูลเหตุการณ์ความเสี่ยง รวมถึงมีการระบุถึงปัจจัยที่ส่งผลต่อเหตุการณ์นั้น
   2.6 พิจารณาเงื่อนไขที่มีผลต่อเหตุการณ์ความเสี่ยงจากเหตุการณ์ที่เคยเกิดขึ้นแล้ว รวมทั้งความเชื่อมโยงของเงื่อนไขต่อโอกาสเกิดและผลกระทบของแต่ละเหตุการณ์ความเสี่ยง
   2.7 วิเคราะห์และทบทวนเหตุการณ์ความเสี่ยงและปัจจัยความเสี่ยงอย่างสม่ำเสมอเพื่อระบุประเด็นความเสี่ยงใหม่ๆ เพิ่มเติม ซึ่งจะช่วยให้มีความเข้าใจเกี่ยวกับภาพความเสี่ยงขององค์กรได้ดีขึ้น
3. การกำหนดความเสี่ยงที่สามารถยอมรับได้ จากความเสี่ยงที่ได้รวบรวมในขั้นตอนข้างต้น นำมาพิจารณาถึงระดับความเสี่ยงที่บริษัทฯ สามารถยอมรับได้เมื่อมีความเสี่ยงนั้นๆ เกิดขึ้น โดยควรมีการกำหนดระดับความเสี่ยงที่สามารถยอมรับได้ (Risk Appetite) จากการพิจารณาระดับความเสี่ยงที่บริษัทฯ ยอมรับได้ รวมถึงวัฒนธรรมองค์กร หรือระดับการยอมรับความเสี่ยงของ คณะกรรมการบริษัท

4. การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยการระบุความเสี่ยงที่เป็นไปได้ทั้งหมดกำหนดสถานการณ์ความเสี่ยง และกำหนดปัจจัยความเสี่ยง ที่เหมาะสม รวมทั้งกำหนดความเสี่ยงที่สามารถยอมรับได้แล้ว จึงประเมินถึงโอกาสเกิดและผลกระทบของเหตุการณ์ ความเสี่ยงที่กำหนดไว้ โดยอาจจัดทำในรูปแบบของแผนภาพความเสี่ยง (Risk Map) เพื่อนำเสนอระดับของโอกาสเกิดและผลกระทบของแต่ละเหตุการณ์ความเสี่ยง และทะเบียนความเสี่ยง (Risk Register) เพื่อบรรยายข้อมูลรายละเอียดของ ความเสี่ยง จากนั้นจึงจัดทำโครงร่างของความเสี่ยง (Risk Profile) เพื่อรวบรวมความเสี่ยงที่เกี่ยวข้องทั้งหมด โดยโครงร่าง ของความเสี่ยงนี้ยังช่วยผู้ประกอบธุรกิจเปรียบเทียบโอกาสเกิด และผลกระทบของแต่ละความเสี่ยง และใช้ในการจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง
5. การบริหารจัดการเพื่อตอบสนองต่อความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้
   5.1 เพื่อให้การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นไปตามระดับความสำคัญ และตอบสนองต่อเป้าหมายขององค์กร จึงมีกระบวนการในการบริหารและจัดการต่อความเสี่ยง ด้วยการนำระดับความเสี่ยงที่สามารถยอมรับได้มาเปรียบเทียบกับผลการประเมินความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่ได้ดำเนินการไว้ข้างต้น ในกรณีที่ ความเสี่ยงที่หลงเหลืออยู่เกินกว่าระดับที่องค์กรยอมรับได้ ควรมีการกำหนดวิธีการบริหารจัดการเพื่อตอบสนองต่อความเสี่ยงนั้น
6. การบริหารจัดการเพื่อตอบสนองต่อความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ (Risk Response) พิจารณาจากระดับความสำคัญของความเสี่ยง ประสิทธิภาพและประสิทธิผลของการจัดการความเสี่ยง และความสามารถในการดำเนินกิจกรรมเพื่อจัดการความเสี่ยง โดยการบริหารจัดการเพื่อตอบสนองต่อความเสี่ยงสามารถดำเนินการได้ใน 4 ลักษณะ อันได้แก่ การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) การยอมรับความเสี่ยง (Risk Acceptance) การร่วมรับความเสี่ยง/ถ่ายโอน (Risk Sharing/Transfer) และการลดความเสี่ยง (Risk Mitigation)
7. การกำหนดตัวชี้วัดระดับความเสี่ยง (IT Risk Indicator) และจัดให้มีการติดตามรายงานผลตัวชี้วัดดังกล่าว
   7.1 กำหนดตัวชี้วัดระดับความเสี่ยง (IT Risk Indicator) เพื่อสามารถชี้วัดและติดตามความเสี่ยงได้อย่างรวดเร็ว รวมทั้งสามารถติดตามแนวโน้มของความเสี่ยงที่อาจเกิดขึ้น
   7.2 การรายงานผลการประเมินความเสี่ยงที่มีผลต่อผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องทั้งหมดในรูปแบบที่สามารถนำไปประกอบการตัดสินใจได้ รวมถึงรายงานผลการบริหารจัดการความเสี่ยง ประสิทธิผลของการควบคุม ข้อตรวจพบ หรือข้อปรับปรุง รวมทั้งผลกระทบจากรายการความเสี่ยง
   7.3 กำหนดหน้าที่และความรับผิดชอบของบุคลากรผู้ทำหน้าที่บริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

7.3.1 คณะกรรมการที่ได้รับการแต่งตั้งเป็นผู้รับผิดชอบ (Accountable Person) ในการให้แนวทางและอนุมัติเห็นชอบในนโยบายการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ รวมทั้งติดตามผลการปฏิบัติตามนโยบายการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

7.3.2 ผู้บริหารซึ่งมีหน้าที่ในการบริหารความเสี่ยง เช่น หัวหน้าสายงานบริหารความเสี่ยง และหัวหน้าสายงานบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศเป็นผู้ทำหน้าที่ (Responsible Person) ในการกำหนดกรอบและกระบวนการการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ รวมทั้งสนับสนุนให้มีการดำเนินงานดังกล่าว โดยผู้บริหารซึ่งมีหน้าที่ในการบริหารความเสี่ยงนี้จะเป็นผู้รับผิดชอบ (Accountable Person) ในผลการบริหารจัดการความเสี่ยงทุกรูปแบบทั่วทั้งองค์กร รวมถึงรับผิดชอบให้มีการจัดทำและปรับปรุงรายการความเสี่ยงและกิจกรรมการบริหารความเสี่ยง

7.3.3 ผู้บริหารหน่วยงานที่ปฏิบัติงานทางด้านเทคโนโลยีสารสนเทศ เช่น หัวหน้าหน่วยงานเทคโนโลยีสารสนเทศ เป็นผู้ทำหน้าที่ (Responsible Person) ในการบริหารจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

<u>หมวดที่ 8</u> นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

<u>วัตถุประสงค์</u>

1. เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยของการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเครือข่ายและคอมพิวเตอร์

<u>แนวทางปฏิบัติ</u>

1. บริษัทฯ ต้องมีการควบคุมการเข้าออกห้อง Server อย่างเพียงพอจะเป็นการป้องกันบุคคลที่ไม่ได้รับอนุญาตเข้าสู่ห้อง Server และความเสียหายอันจะเกิดจากอุปกรณ์หรือระบบต่างๆ เช่น ระบบไฟฟ้า ระบบอุณหภูมิและความชื้น ซึ่งย่อมมีความเสี่ยงต้องอุปกรณ์และข้อมูลของบริษัทฯ ดังนั้นบริษัทฯ ต้องมีการควบคุมเพื่อให้สามารถระบุตัวตนของผู้เข้าถึงห้อง Server ได้ และการเข้าถึงดังกล่าวต้องมีการอนุมัติอย่างเพียงพอ ซึ่งจำกัดไว้เฉพาะบุคคลที่จำเป็นเท่านั้น รวมทั้งการควบคุมให้มีระบบป้องกันความเสียหายที่อาจจะเกิดขึ้น เช่น การป้องกันไฟไหม้ หรือไฟฟ้าขัดข้อง เป็นต้น
2. บริษัทฯ ต้องมีการกำหนดขอบเขตพื้นที่รักษาความปลอดภัย เช่น จัดทำกำแพง บัตรผ่านประตู หรือจัดให้มีเจ้าหน้าที่บริษัทเพื่อทำการต้อนรับ และป้องกันการเข้าถึงบริเวณที่มีระบบ อุปกรณ์ประมวลผลสารสนเทศของบริษัทฯ

3. บริษัทฯ ต้องจัดให้มีการควบคุมการเข้าถึงทางกายภาพอย่างเหมาะสมสำหรับ ศูนย์คอมพิวเตอร์ และห้อง Server เช่น จัดทำประตูเข้า - ออก และให้มีการล็อคกุญแจทุกครั้งหากไม่มีการใช้งาน
4. บริษัทฯ ต้องกำหนดบุคคลที่ได้รับอนุญาตในการเข้าถึง ศูนย์คอมพิวเตอร์ ไว้เป็นลายลักษณ์อักษร พร้อมทั้งรายชื่อดังกล่าวต้องได้รับการอนุมัติจากผู้บริหาร อีกทั้งต้องมีการปรับปรุงรายชื่อ และทำการอนุมัติใหม่ทุกครั้งที่มีการเปลี่ยนแปลง
5. ระบบและอุปกรณ์สนับสนุนการทำงานหลักที่อยู่ในสภาพแวดล้อมที่ใช้งานจริง (รวมถึงเครื่องแม่ข่าย Firewall, Switch, Router อื่นๆ) ต้องถูกจัดวางภายในศูนย์คอมพิวเตอร์อย่างเหมาะสม
6. บริษัทฯ ต้องจัดให้มีการเก็บบันทึกข้อมูลการเข้าออกศูนย์คอมพิวเตอร์ และห้อง Server ทั้งเจ้าหน้าที่เทคโนโลยีสารสนเทศ เจ้าหน้าที่บริษัท และเจ้าหน้าที่จากหน่วยงานภายนอก ลงใน Log Book โดยจะต้องบันทึกรายละเอียดของผู้เข้าออก และเวลาเข้าออก และให้มีการตรวจสอบอย่างสม่ำเสมอ
7. บริษัทฯ ต้องจัดให้มีการป้องกันความเสียหายสำหรับระบบเครือข่ายและคอมพิวเตอร์ของบริษัท อย่างเหมาะสม ได้แก่

   7.1 ระบบไฟฟ้า

   บริษัทฯ ต้องจัดให้มีเครื่องสำรองไฟสำหรับระบบคอมพิวเตอร์และเครือข่ายเพื่อให้การดำเนินงานมีความต่อเนื่อง และรวมไปถึงการป้องกันความเสียหายเมื่อมีกระแสไฟฟ้าไม่คงที่

   7.2 ระบบป้องกันไฟไหม้

   บริษัทฯ ต้องติดตั้งอุปกรณ์เตือนภัยในกรณีที่เกิดไฟไหม้ เช่น เครื่องดักจับควัน เครื่องตรวจจับความร้อน และสัญญาณเตือนภัย เป็นต้น

   บริษัทฯ ต้องทำการติดตั้งอุปกรณ์ดับเพลิงภายในศูนย์คอมพิวเตอร์

   7.3 ระบบควบคุมอุณหภูมิและความชื้น

   บริษัทฯ ต้องทำการติดตั้งระบบตรวจสอบอุณหภูมิและความชื้นให้เหมาะกับระบบ และอุปกรณ์คอมพิวเตอร์

   7.4 ระบบป้องกันน้ำรั่วซึม

   บริษัทฯ ต้องทำการติดตั้งระบบป้องกันการรั่วซึมของน้ำ ที่อาจจะเกิดขึ้นจากการใช้งานเครื่องปรับอากาศ หรือ ฝ้า เพดาน รั่วซึม

7. การบังคับใช้

เจ้าหน้าที่บริษัทที่ถูกตรวจพบว่าไม่ปฏิบัติตามนโยบายฉบับนี้จะมีผลต่อการลงโทษทางวินัย รวมถึงการ พิจารณาการเลิกจ้าง

เพื่อให้ทราบโดยทั่วกันและยึดถือปฏิบัติให้เป็นไปในแนวทางเดียวกัน จึงประกาศใช้นโยบายกำกับดูแลและรักษาความปลอดภัยเทคโนโลยีสารสนเทศ

นโยบายนี้มีผลบังคับใช้ตั้งแต่วันที่ 14 ธันวาคม 2567

ลงชื่อ 

(นายศิริพล ยอดเมืองเจริญ)

ประธานคณะกรรมการบริษัท

บริษัท บางกอก แอสเซท อินเตอร์กรุ๊ป จำกัด (มหาชน)

BANGKOK ASSET
INTERGROUP

นโยบายการบริหารความต่อเนื่องทางธุรกิจ

บริษัท บางกอก แอสเซท อินเตอร์กรุ๊ป จำกัด (มหาชน)

สารบัญ

หัวข้อ ..... หน้า

1. วัตถุประสงค์ 2

2. ขอบเขต 2

3. คำย่อ และคำนิยาม 3

4. โครงสร้างและทีมงานบริหารความต่อเนื่องทางธุรกิจ 3

5. กระบวนการบริหารความต่อเนื่องทางธุรกิจ 4

5.1 ผลกระทบจากเหตุฉุกเฉินที่อาจทำให้งานสำคัญหยุดชะงัก (Major Operational Disruptions) 4

5.2 การกำหนดเป้าหมายในการกู้คืนการดำเนินงานให้กลับคืนสู่สภาพการดำเนินงานปกติ (Recovery Objective) 5

5.3 การพัฒนากลยุทธ์เพื่อบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Strategy Development) 6

5.4 แผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Planning) 6

5.5 การติดต่อสื่อสารกับผู้เกี่ยวข้อง (Communication) 7

5.6 การทดสอบและประเมิน BCP (Training, Exercising and Maintaining) 8

6. การทบทวนนโยบาย 8

BANGKOK ASSET INTERGROUP	บริษัท บางกอก แอสเซท อินเตอร์กรุ๊ป จำกัด (มหาชน)	ต้นฉบับ
	รหัส : PC-ORG-008	หน้า 1 จาก 9
นโยบาย	เรื่อง : การบริหารความต่อเนื่องทางธุรกิจ	*แก้ไขครั้งที่ : 01*
		มีผลบังคับใช้วันที่ : 14 ธันวาคม 2567

ประวัติการจัดทำ และทบทวนเอกสาร

ครั้งที่	วันที่แก้ไข	รายละเอียด
1	11 พฤศจิกายน 2566	เผยแพร่เพื่อใช้งานครั้งที่ 1 ภายหลังจากการแปรสภาพเป็นบริษัทมหาชนจำกัด
2	14 ธันวาคม 2567	ทบทวนประจำปี 2567

CONFIDENTIAL

นโยบายการบริหารความต่อเนื่องทางธุรกิจ

ของ

บริษัท บางกอก แอสเซท อินเตอร์กรุ๊ป จำกัด (มหาชน)

1. วัตถุประสงค์

เพื่อเป็นแนวทางปฏิบัติโดยครอบคลุมประเด็นสำคัญในการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) อันประกอบไปด้วย การวิเคราะห์และทบทวนความเสี่ยง การวิเคราะห์ผลกระทบทางธุรกิจ การพัฒนากลยุทธ์เพื่อบริหารความต่อเนื่องของธุรกิจ การพัฒนาแผนงาน (Business Continuity Plan: BCP) การเสริมสร้างความรู้และการอบรม และการฝึกซ้อมแผน

(1) บริษัทฯ จะต้องพัฒนาระบบ BCM ตามมาตรฐานการบริหารความต่อเนื่องทางธุรกิจ ปรับปรุงศักยภาพ BCM ให้เป็นองค์กรที่มีกระบวนการปฏิบัติงานสามารถรองรับต่อเหตุการณ์ที่คาดการณ์ไว้ล่วงหน้าและมิได้คาดการณ์ไว้ล่วงหน้าได้อย่างเหมาะสม โดยมีการวางแผน การนำไปปฏิบัติ การฝึกซ้อม ติดตามทบทวน และการปรับปรุงแก้ไขอย่างต่อเนื่อง สื่อสารทั้งภายในและภายนอกอย่างมีประสิทธิผล รวมทั้งสร้างให้เกิดเป็นวัฒนธรรมองค์กร

(2) ผู้บริหารระดับสูงมีหน้าที่รับผิดชอบ ผลักดัน และสนับสนุนการดำเนินงานด้านต่างๆ ตามกระบวนการบริหารความต่อเนื่องทางธุรกิจ ตลอดจนเสริมสร้างและพัฒนาความรู้ความสามารถของบุคลากรเพื่อให้มั่นใจว่าสามารถ ดำเนินการตามกระบวนการที่วางไว้อย่างมีประสิทธิผล

(3) คณะบริหารความต่อเนื่องทางธุรกิจมีหน้าที่พัฒนาระบบความต่อเนื่องทางธุรกิจตามขอบข่ายที่รับผิดชอบอย่างเป็นระบบ ประกอบด้วยการวางแผน นำไปปฏิบัติ ฝึกซ้อม และปรับปรุงแก้ไขอย่างต่อเนื่อง โดยกำหนดผู้รับผิดชอบในการจัดทำแผนเพื่อจัดการกิจกรรมหรือกระบวนการหลักที่สำคัญต่อการดำเนินธุรกิจ และรายงานผลต่อคณะกรรมการบริษัทอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

(4) ผู้บริหาร พนักงาน และลูกจ้างทุกคน ต้องตระหนักถึงการมีส่วนร่วม เพื่อให้องค์กรบรรลุประสิทธิผลในการบริหารความต่อเนื่องทางธุรกิจ และสร้างให้เกิดเป็นวัฒนธรรมองค์กร

2. ขอบเขต

นโยบายการบริหารความต่อเนื่องทางธุรกิจ (BCP) ฉบับนี้ บังคับใช้สำหรับเป็นแนวทางในการปฏิบัติกรณีเกิดสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉิน ที่มีผลกระทบต่อกิจกรรมหลักของบริษัทซึ่งไม่สามารถปฏิบัติงานได้ คือ สำนักงานใหญ่ เลขที่ 2 ซอยงามวงศ์วาน 9 แยก 1 ตำบลบางเขน อำเภอเมืองนนทบุรี จังหวัดนนทบุรี 11000 อันเกิดจากเหตุการณ์และภัยคุกคามที่ไม่สามารถควบคุมได้ ดังนี้

(1) เหตุการณ์การเชื่อมโยงเครือข่ายล้มเหลว

(2) เหตุการณ์ไฟฟ้าขัดข้อง

(3) เหตุการณ์อัคคีภัย

(4) เหตุการณ์อุทกภัย

(5) เหตุการณ์แผ่นดินไหว

(6) เหตุการณ์ชุมนุมประท้วง/การก่อการจลาจล

(7) เหตุการณ์โรคระบาด

(8) เหตุการณ์การถูกโจมตีทางไซเบอร์ (Cyber Attack)

3. คำย่อ และคำนิยาม

คำศัพท์	ความหมาย
การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM)	กระบวนการบริหารแบบองค์รวมซึ่งชี้บ่งภัยคุกคามที่อาจจะเกิดขึ้นต่อองค์กรและผลกระทบของภัยคุกคามนั้นต่อการดำเนินธุรกิจ และให้แนวทางในการสร้างขีดความสามารถให้องค์กรมีความยืดหยุ่น (Resilience) เพื่อการตอบสนองและปกป้องผลประโยชน์ของผู้มีส่วนได้ส่วนเสียหลัก ชื่อเสียง ภาพลักษณ์ และกิจกรรมที่สร้างมูลค่าที่มีประสิทธิผล
แผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP)	เอกสารขั้นตอนการดำเนินงานที่ให้แนวทางแก่องค์กรในการตอบสนอง การฟื้นฟู การกลับมาดำเนินการ และการติดตั้งเพื่อให้สามารถดำเนินงานได้ในระดับที่กำหนดไว้ภายหลังจากการหยุดชะงัก
ภาวะวิกฤต (Crisis)	สถานการณ์รุนแรงซึ่งหากไม่ได้มีการจัดการที่เหมาะสมอาจส่งผลกระทบที่รุนแรงต่อภาพลักษณ์ ชื่อเสียง และความสามารถในการปฏิบัติงานหรือการให้บริการขององค์กรได้
Recovery Point Objective (RPO)	จุดซึ่งข้อมูลสารสนเทศที่ใช้ในกิจกรรมต้องได้รับการฟื้นฟู เพื่อให้สามารถกลับมาดำเนินกิจกรรมต่อไปได้ โดยวัดเป็นช่วงระยะเวลาของข้อมูลที่สูญหาย (เช่น สูญหายไป 7 วัน เป็นต้น) โดยข้อมูลจะต้องได้รับการกู้คืนกลับมาหรือสร้างใหม่เพื่อทดแทนข้อมูลที่สูญหายไป
Recovery Time Objective (RTO)	ระยะเวลาเป้าหมายจากการเกิดอุบัติการณ์ที่ทำให้ผลิตภัณฑ์หรือบริการต้องกลับคืนสภาพเดิม กิจกรรมต้องกลับมาดำเนินการได้ รวมถึงทรัพยากรต้องได้รับการฟื้นฟู โดยมีหน่วยเป็น ชั่วโมง วัน เป็นต้น

4. โครงสร้างและทีมงานบริหารความต่อเนื่องทางธุรกิจ

เพื่อให้แผนบริหารความต่อเนื่องทางธุรกิจ (BCP) ถูกนำไปปฏิบัติใช้ได้อย่างมีประสิทธิภาพและเกิดประสิทธิผลจึงจัดตั้งคณะบริหารความต่อเนื่องทางธุรกิจ โดยครอบคลุมหน้าที่ความรับผิดชอบ ดังนี้

(1) บริหารความต่อเนื่องทางธุรกิจแบบองค์รวมของกระบวนการ ที่บ่งชี้ภัยคุกคามต่อองค์กรและผลกระทบต่อการดำเนินธุรกิจ วางแนวทางในการสร้างขีดความสามารถให้องค์กรมีความยืดหยุ่น เพื่อการประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับองค์กร รวมทั้งเพื่อการตอบสนองและปกป้องผลประโยชน์ของผู้มีส่วนได้ส่วนเสีย ชื่อเสียง ภาพลักษณ์ และกิจกรรมที่สร้างมูลค่าได้อย่างมีประสิทธิผล

(2) จัดทำแผนบริหารความต่อเนื่องทางธุรกิจ (BCP) สำหรับการรับมือกับสถานการณ์ต่างๆ ที่อาจเกิดขึ้น เพื่อให้องค์กรสามารถดำเนินการและตอบสนองแก่ผู้มีส่วนได้ส่วนเสียได้อย่างต่อเนื่อง

(3) เชื่อมโยงความต่อเนื่องทางธุรกิจ (BCM) กับการบริหารความเสี่ยงองค์กร (ERM) เพื่อการบรรเทาความเสี่ยง (Risk Treatment) ระดับ Operation Events

(4) พิจารณาขอบเขต ลักษณะวิกฤตการณ์และประเมินสถานการณ์ที่เกิดขึ้น

(5) พิจารณาตัดสินใจประกาศภาวะวิกฤต เพื่ออนุมัติใช้แผนบริหารความต่อเนื่องทางธุรกิจ (BCP)

(6) สั่งการให้ผู้ที่เกี่ยวข้องหรือกลุ่มที่ได้รับผลกระทบนำแผนบริหารความต่อเนื่องทางธุรกิจขององค์กร/หน่วยงานมาใช้และติดตามสถานะของการกอบกู้การปฏิบัติงานของฝ่ายงานที่ได้รับผลกระทบและรายงานสถานะตามสายงานการบังคับบัญชา

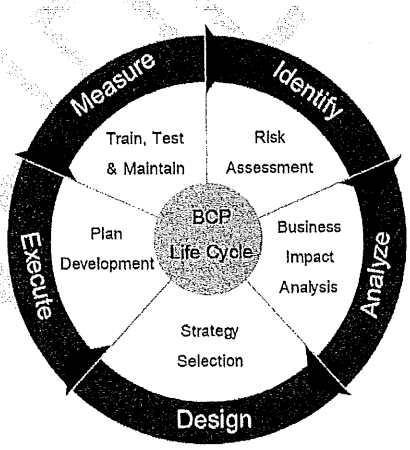
(7) ให้แนวทางการปฏิบัติงาน สนับสนุนและติดตามผลการใช้แผนบริหารความต่อเนื่องทางธุรกิจ (BCP) ในภาวะวิกฤต

(8) ชี้แจงหรือให้ข้อมูลข่าวสารภายใน และภายนอกองค์กร

5. กระบวนการบริหารความต่อเนื่องทางธุรกิจ

นโยบายกำหนดกระบวนการบริหารความต่อเนื่องทางธุรกิจมี 5 กิจกรรมหลัก ดังนี้

รูปภาพที่ 1 กระบวนการบริหารความต่อเนื่องทางธุรกิจ



5.1 ผลกระทบจากเหตุฉุกเฉินที่อาจทำให้งานสำคัญหยุดชะงัก (Major Operational Disruptions)

บริษัทฯ ต้องจัดให้มีการประเมินความเสี่ยงและโอกาสที่งานสำคัญจะหยุดชะงักจากเหตุฉุกเฉินที่อาจเกิดขึ้น รวมทั้งวิเคราะห์ผลกระทบทางธุรกิจและประเมินความเสียหายจากการหยุดชะงักของการดำเนินงานที่สำคัญ (Major Operational Disruptions) เพื่อให้บริษัทสามารถกำหนดลำดับความสำคัญของงาน และจัดสรรทรัพยากรในการบริหารการดำเนินธุรกิจอย่างต่อเนื่องได้อย่างมีประสิทธิภาพ โดยอย่างน้อยบริษัทฯ ต้องทำการประเมินความเสี่ยงและวิเคราะห์ผลกระทบทางธุรกิจดังกล่าวปีละครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญที่ส่งผลต่อความเสี่ยงและผลกระทบที่จะเกิดขึ้นนั้น โดยปฏิบัติตามวิธีการดังนี้

(1) การระบุงานสำคัญ (Critical Business Function) บริษัทฯ ควรคัดเลือกงานสำคัญที่พิจารณาว่าหากเกิดเหตุการณ์ฉุกเฉินแล้วงานดังกล่าวหยุดชะงักจะส่งผลกระทบอย่างมีนัยสำคัญต่อลูกค้า การดำเนินธุรกิจ สถานะทางการเงิน หรือชื่อเสียงของบริษัทฯ เช่น งานโอนกรรมสิทธิ์ งานจัดซื้อจัดจ้าง งานด้านการเบิกจ่าย และงานด้านการขาย เป็นต้น

(2) การประเมินความเสี่ยง (Risk Assessment) บริษัทฯ ต้องทำการประเมินความเสี่ยงและโอกาสที่อาจทำให้งานสำคัญหยุดชะงัก โดยควรประเมินเหตุการณ์ฉุกเฉินที่ทำให้เกิดการหยุดชะงักและก่อให้เกิดความเสียหายและส่งผลกระทบทางธุรกิจทั้งในระยะสั้น ระยะปานกลาง และระยะยาว เช่น อาคารและสถานที่ทำงานหรือสาขาได้รับความเสียหาย ระบบเทคโนโลยีสารสนเทศใช้งานไม่ได้ พนักงานไม่สามารถเข้าถึงหรือใช้งานอาคารได้ พนักงานไม่สามารถมาปฏิบัติงานทั้งกรณีชั่วคราวหรือถาวร เป็นต้น

(3) การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) บริษัทฯ ต้องวิเคราะห์ผลกระทบทางธุรกิจและประเมินความเสียหายจากการหยุดชะงักของงานสำคัญ เพื่อให้บริษัทฯ สามารถกำหนดลำดับความสำคัญของงาน และจัดสรรทรัพยากรในการบริหารการดำเนินธุรกิจอย่างต่อเนื่องได้อย่างมีประสิทธิภาพ โดยพิจารณาถึงผลกระทบทั้งในรูปของตัวเงิน และไม่ใช่ตัวเงินที่มีต่อลูกค้า พนักงาน อุปกรณ์ ทรัพย์สินและที่ทำงานของบริษัทฯ สถานะการเงิน ความเชื่อมั่นของลูกค้า และชื่อเสียงของบริษัทฯ รวมถึงการปฏิบัติตามกฎระเบียบ ข้อบังคับ เป็นต้น

5.2 การกำหนดเป้าหมายในการกู้คืนการดำเนินงานให้กลับคืนสู่สภาพการดำเนินงานปกติ (Recovery Objective)

บริษัทฯ ต้องจัดให้มีการกำหนดระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานปกติของแต่ละงานสำคัญ (Recovery Time Objectives) พร้อมทั้งจัดลำดับการกู้คืนการดำเนินงานของงานที่สำคัญทุกงานให้เหมาะสมกับผลกระทบที่อาจเกิดขึ้น

ให้พิจารณากำหนดประเภทของข้อมูล และชุดข้อมูลล่าสุดที่จะกู้คืนได้ (Recovery Point Objective) เพื่อให้บริษัทฯ สามารถดำเนินงานได้อย่างต่อเนื่อง และไม่ส่งผลกระทบอย่างมีนัยสำคัญต่อลูกค้า การดำเนินธุรกิจ และการปฏิบัติตามกฎระเบียบ หากเกิดเหตุฉุกเฉิน เช่น งานโอนกรรมสิทธิ์งานจัดซื้อจัดจ้าง งานด้านการเบิกจ่าย และงานด้านการขาย เป็นต้น ทั้งนี้ ข้อมูลล่าสุดที่จะกู้คืนได้อาจเป็นการกู้คืนข้อมูล ณ สิ้นวันก่อน หรือ 1 ชั่วโมงก่อนเกิดเหตุการณ์ฉุกเฉินแล้วแต่กรณี นอกจากนี้ ควรมีวิธีการในการจัดหาหรือจัดทำข้อมูลทดแทนข้อมูลสำคัญที่สูญหาย

หากบริษัทฯ มีการใช้บริการจากผู้ให้บริการ (Service Provider) บริษัทฯ ควรร่วมกับผู้ให้บริการในการกำหนดระยะเวลากลับคืนสู่สภาพการดำเนินงานปกติและชุดข้อมูลที่จะกู้คืนล่าสุด เพื่อให้ได้เป้าหมายที่เหมาะสมและสามารถปฏิบัติได้จริง

ทั้งนี้ การกำหนดระยะเวลากลับคืนสู่สภาพการดำเนินงานปกติและชุดข้อมูลที่จะกู้คืนล่าสุดเป็นปัจจัยสำคัญในการกำหนดทรัพยากรที่ต้องการใช้ จึงต้องได้รับความเห็นชอบจากคณะทำงานที่ได้รับมอบหมาย

5.3 การพัฒนากลยุทธ์เพื่อบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Strategy Development)

การกำหนดกลยุทธ์เพื่อให้หน่วยงานสามารถกลับคืนมาปฏิบัติหน้าที่ได้ตามปกติ จะทำให้หน่วยงานทุกฝ่ายของบริษัทฯ สามารถดำเนินการได้เป็นลำดับขั้นตอนตามที่ได้คาดการณ์ไว้ล่วงหน้า ซึ่งจะส่งผลให้บริษัทฯ สามารถลดอุปสรรค หรือความเสี่ยงต่อการดำเนินธุรกิจโดยต่อเนื่องจนกว่าเหตุภัยพิบัติหรือเหตุวิกฤตจะผ่านพ้นไป คณะทำงานต้องจัดทำแผนกลยุทธ์เพื่อบริหารความต่อเนื่องทางธุรกิจ เพื่อระบุวิธีการและลำดับความสำคัญของกระบวนการ/ระบบงานต่างๆ รวมถึงค่าใช้จ่ายที่เกี่ยวข้องเพื่อให้การดำเนินการที่รับผิดชอบสามารถกลับคืนมาปฏิบัติหน้าที่ได้ตามปกติ โดยจะต้องคำนึงถึงความเสี่ยงประเภทต่างๆ เช่น ความเสี่ยงในการพึ่งพาหน่วยงานอื่น ความเสี่ยงในการกระจุกตัวของงานหรือบุคลากร เป็นต้น

5.4 แผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Planning)

เพื่อให้งานสำคัญสามารถดำเนินต่อไปได้อย่างต่อเนื่อง บริษัทต้องจัดให้มี BCP ที่กำหนดไว้เป็นลายลักษณ์อักษรและได้รับอนุมัติจากคณะกรรมการบริษัท หรือคณะทำงานที่ได้รับมอบหมาย โดยควรจัดเก็บ BCP ดังกล่าวไว้ทั้งในและนอกสถานที่ทำการ

BCP จะต้องครอบคลุมทุกงานสำคัญของบริษัทฯ ตลอดจนระบบงานที่สำคัญที่บริษัทฯ ใช้บริการจากผู้ให้บริการ (Service Provider) นอกจากนี้ บริษัทฯ ควรกำหนดรายละเอียดวิธีปฏิบัติไว้ใน BCP ให้เหมาะสมกับขนาดและความซับซ้อนของธุรกิจและครอบคลุมการหยุดชะงักที่อาจเกิดขึ้นทุกสถานการณ์ รวมทั้งกรณีเกิดเหตุฉุกเฉินเป็นเวลานานหรือส่งผลเสียหายครอบคลุมพื้นที่ในวงกว้าง เช่น การเกิดโรคระบาด การไฟฟ้า หรือการสื่อสารขัดข้องในหลายพื้นที่ เป็นต้น โดยให้ทุกหน่วยงานมีส่วนร่วมในการจัดทำ BCP เพื่อรองรับงานสำคัญของตนเอง ทั้งนี้ BCP ต้องมีรายละเอียดอย่างน้อย ดังนี้

(1) ขั้นตอนการปฏิบัติงานและผู้รับผิดชอบ เพื่อให้บริษัทฯ สามารถกลับมาดำเนินงานสำคัญได้ตามระยะเวลาที่กำหนดหลังจากเกิดการหยุดชะงักการดำเนินงาน บริษัทฯ ต้องกำหนดหน้าที่และความรับผิดชอบของผู้ปฏิบัติงานแต่ละรายอย่างชัดเจน และจัดให้มีการสื่อสารและซักซ้อมความเข้าใจถึงหน้าที่ที่ต้องปฏิบัติ ตลอดจนกำหนดรายละเอียดวิธีปฏิบัติงานที่สามารถเข้าใจและปฏิบัติตามได้ว่าต้องปฏิบัติงานอะไร อย่างไร เมื่อไรและที่ไหน

(2) วิธีการและช่องทางติดต่อสื่อสารกับผู้เกี่ยวข้องทั้งภายในและภายนอกบริษัท บริษัทฯ ต้องกำหนดวิธีการและช่องทางติดต่อสื่อสาร รายชื่อผู้เกี่ยวข้องทั้งภายในและภายนอกบริษัทฯ ผู้รับผิดชอบการติดต่อสื่อสาร รวมทั้งรายละเอียดข้อมูลที่จะเปิดเผยแก่ผู้เกี่ยวข้องอย่างชัดเจน บริษัทฯ ควรจัดทำผังการติดต่อพนักงาน และจัดทำรายชื่อลูกค้า ผู้ให้บริการหลักและผู้เกี่ยวข้องอื่น ๆ รวมถึงข้อมูลที่สามารถใช้

ในการติดต่อ เช่น หมายเลขโทรศัพท์สำนักงาน หมายเลขโทรศัพท์เคลื่อนที่ หรือ E-mail เป็นต้น โดยบริษัทฯ ต้องปรับปรุงรายชื่อและข้อมูลที่ใช้ในการติดต่อให้เป็นปัจจุบันอยู่เสมอ นอกจากนี้บริษัทฯ ควรกำหนดช่องทางการสื่อสารเพิ่มเติม เช่น เว็บไซต์บริษัท Intranet หรือการเผยแพร่ผ่านสื่อต่างๆ เป็นต้น

(3) ทรัพยากรที่จำเป็นสำหรับการปฏิบัติงาน บริษัทฯ ควรจัดเตรียมหรือจัดหาทรัพยากรที่จำเป็นต่อการปฏิบัติงาน เช่น การจัดหาหรือกำหนดบุคลากรที่จะปฏิบัติงานแทนทั้งระดับพนักงานและผู้บริหาร แหล่งเงินทุน อุปกรณ์สำนักงาน ระบบเทคโนโลยีสารสนเทศ เป็นต้น

(4) การจัดตั้งศูนย์ปฏิบัติงานสำรอง (Alternate Site) เพื่อป้องกันผลกระทบจากเหตุฉุกเฉินที่เกิดขึ้นเป็นบริเวณกว้าง บริษัทอาจจัดให้มีศูนย์ปฏิบัติงานสำรองเพื่อรองรับการดำเนินการอย่างต่อเนื่อง โดยศูนย์ปฏิบัติงานดังกล่าวไม่ควรใช้สาธารณูปโภคแหล่งเดียวกันกับสถานที่ทำการหลัก รวมทั้งควรจัดให้สามารถรองรับปริมาณงานสำคัญหรือการเกิดเหตุฉุกเฉินเป็นระยะเวลานานได้ นอกจากนี้ ศูนย์ปฏิบัติงานสำรองควรมีความพร้อมที่จะปฏิบัติงานทันทีที่เกิดเหตุฉุกเฉินหรือภายในระยะเวลาที่กำหนดไว้ (Recovery Time Objectives) กรณีที่บริษัทฯ ไม่มีการจัดให้มีศูนย์ปฏิบัติการสำรอง บริษัทฯ ควรมีแนวทางการปฏิบัติงานอื่น ที่สามารถรองรับการดำเนินงานอย่างต่อเนื่องได้ ทั้งนี้ บริษัทฯ สามารถพิจารณาให้พนักงานปฏิบัติงานจากที่บ้านได้ เพื่อให้สอดรับกับระบบเทคโนโลยีสารสนเทศในรูปแบบ on Cloud

5.5 การติดต่อสื่อสารกับผู้เกี่ยวข้อง (Communication)

เพื่อป้องกันและลดความตระหนกของผู้เกี่ยวข้องและสาธารณชน รวมทั้งสามารถแจ้งเหตุแก่หน่วยงานกำกับดูแลได้ทันท่วงที บริษัทฯ ต้องวางแผนการติดต่อสื่อสารกับผู้เกี่ยวข้องทั้งภายในและภายนอกบริษัทฯ ให้สอดคล้องกับผลกระทบที่เกิด หากผลกระทบที่กล่าวส่งผลอย่างมีนัยสำคัญต่อลูกค้าหรือผู้เกี่ยวข้อง เช่น งานโอนกรรมสิทธิ์งานจัดซื้อจัดจ้าง งานด้านการเบิกจ่าย และงานด้านการขาย เป็นต้น บริษัทฯ ต้องแจ้งหรือประชาสัมพันธ์ให้ลูกค้าหรือผู้เกี่ยวข้องทราบถึงเหตุฉุกเฉิน ผลกระทบที่เกิดขึ้น ช่องทางที่ลูกค้าหรือผู้เกี่ยวข้องจะสามารถติดต่อขอซื้อสินค้าหรือใช้บริการ หรือสื่อสารกับบริษัทฯ ได้ตลอดระยะเวลาที่เกิดเหตุฉุกเฉิน และมาตรการดำเนินการของบริษัทให้ทั่วถึงกันโดยเร็ว รวมทั้งต้องสื่อสารเป็นระยะให้เห็นถึงความคืบหน้าของการดำเนินการหากเกิดเหตุฉุกเฉินเป็นเวลานาน

กรณีที่มีการหยุดการให้บริการของงานสำคัญหรือเกิดเหตุฉุกเฉินซึ่งส่งผลกระทบต่อลูกค้าของบริษัทฯ อย่างมีนัยสำคัญ บริษัทฯ ต้องแจ้งต่อหน่วยงานที่เกี่ยวข้องโดยเร็วและไม่เกินวันทำการถัดไป พร้อมทั้งรายงานรายละเอียดของเหตุการณ์ที่เกิดขึ้น ขั้นตอนการดำเนินการและระยะเวลาที่ใช้หรือคาดว่าจะใช้ในการแก้ไขปัญหา โดยให้บริษัทฯ แจ้งต่อเจ้าหน้าที่ผู้ดูแลรับผิดชอบของบริษัทฯ

5.6 การทดสอบและประเมิน BCP (Training, Exercising and Maintaining)

บริษัทฯ ควรจัดให้มีการอบรมและประชาสัมพันธ์เกี่ยวกับ BCP แก่ผู้เกี่ยวข้องทั้งภายในและภายนอกอย่างสม่ำเสมอ พร้อมทั้งต้องทดสอบ BCP ให้สอดคล้องกับสถานการณ์จริงในปัจจุบัน โดยเจ้าหน้าที่ผู้รับผิดชอบทุกระดับต้องมีส่วนร่วมในการทดสอบ และจัดให้มีการทดสอบ BCP ของงานที่สำคัญอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ โดยบริษัทฯ ควรกำหนดขอบเขตการทดสอบให้เพียงพอเพื่อให้มั่นใจว่าบริษัทฯ สามารถดำเนินงานตาม BCP ได้อย่างถูกต้องและได้ผลตามที่คาดหวังไว้

ในการทดสอบและประเมิน BCP บริษัทฯ ควรกำหนดสถานการณ์จำลองซึ่งอาจแตกต่างกันในการทดสอบแต่ละครั้ง เช่น สถานการณ์การเกิดน้ำท่วม แผ่นดินไหว การลอบวางระเบิด การเดินขบวนประท้วง โรคระบาด เป็นต้น เพื่อทดสอบความสามารถของ BCP ในการรองรับการดำเนินการอย่างต่อเนื่องในการเกิดเหตุการณ์ต่าง ๆ โดยบริษัทฯ อาจพิจารณาจากสถานการณ์ในปัจจุบัน ผลการทดสอบที่ผ่านมา หรือผลกระทบที่อาจเกิด เป็นต้น โดยการทดสอบและการประเมินต้องครอบคลุมอย่างน้อยในเรื่อง ดังต่อไปนี้

(1) ขั้นตอนการติดต่อสื่อสารกับผู้เกี่ยวข้อง ความถูกต้องและทันสมัยของรายชื่อและข้อมูลที่ใช้ในการติดต่อ

(2) ขั้นตอนการอพยพพนักงานหรือการเคลื่อนย้ายพนักงานไปยังสถานที่ที่กำหนดไว้

(3) ขั้นตอนการปฏิบัติงานตามปกติตั้งแต่เริ่มต้นจนจบกระบวนการของงานสำคัญ เช่น งานโอนกรรมสิทธิ์ งานจัดซื้อจัดจ้าง งานด้านการเบิกจ่าย และงานด้านการขาย เป็นต้น

(4) ความพร้อมของระบบคอมพิวเตอร์เครือข่าย อุปกรณ์ต่างๆ และการสำรองและกู้คืนข้อมูลสำคัญ โดยสามารถกู้คืนข้อมูลล่าสุดตามที่กำหนดไว้จากอุปกรณ์หรือสถานที่จัดเก็บได้

(5) ความพร้อมของศูนย์ปฏิบัติงานสำรอง (ถ้ามี) ศูนย์ปฏิบัติงานสำรองสามารถรองรับการเข้าไปปฏิบัติงานได้ทันทีหรือภายในระยะเวลาที่กำหนด

เพื่อปรับปรุง BCP ให้เหมาะสมและสอดคล้องกับสถานการณ์ปัจจุบัน บริษัทฯ ต้องทบทวน BCP ทั้งในระดับหน่วยงานและองค์กร และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญบริษัทฯ ต้องจัดเก็บเอกสารที่เกี่ยวข้องกับการทดสอบให้ครบถ้วนและเป็นปัจจุบัน ดังนี้

1. แผนที่ใช้ในการทดสอบ
2. สรุปผลการทดสอบ
3. สรุปการทบทวนแผน

6 การทบทวนนโยบาย

ให้คณะบริหารความต่อเนื่องทางธุรกิจทบทวนนโยบายฉบับนี้อย่างน้อยปีละ 1 ครั้ง และในกรณีที่มีการเปลี่ยนแปลงให้นำเสนอต่อคณะกรรมการบริษัท เพื่อพิจารณาอนุมัติ

BANGKOK ASSET INTERGROUP	บริษัท บางกอก แอสเซท อินเตอร์กรุ๊ป จำกัด (มหาชน)	ต้นฉบับ
	รหัส : PC-ORG-008	หน้า 9 จาก 9
นโยบาย	เรื่อง : การบริหารความต่อเนื่องทางธุรกิจ	*แก้ไขครั้งที่ : 01*
		มีผลบังคับใช้วันที่ : 14 ธันวาคม 2567

เพื่อให้ทราบโดยทั่วกันและยึดถือปฏิบัติให้เป็นไปในแนวทางเดียวกัน จึงประกาศใช้นโยบายการบริหารความต่อเนื่องทางธุรกิจ

นโยบายนี้มีผลบังคับใช้ตั้งแต่วันที่ 14 ธันวาคม 2567

ลงชื่อ _____

(นายศิริพล ยอดเมืองเจริญ)

ประธานคณะกรรมการบริษัท

บริษัท บางกอก แอสเซท อินเตอร์กรุ๊ป จำกัด (มหาชน)

CONFIDENTIAL



แผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ ประจำปี พ.ศ. 2565 - 2569

บริษัท บางกอก แอสเซท อินเตอร์กรุ๊ป จำกัด (มหาชน)

สารบัญ

ชื่อเรื่อง	หน้า
1. บททั่วไป	
บทนำ	2
ปรัชญาและปณิธาน	2
วิสัยทัศน์	2
พันธกิจ	2
เป้าหมาย	3
2. การวิเคราะห์สถานภาพด้านเทคโนโลยีสารสนเทศ	3
บทวิเคราะห์สถานภาพด้านปัจจัยต่าง ๆ	4
แนวทางการแก้ไขจุดอ่อน และอุปสรรค	5
3. ยุทธศาสตร์ เป้าหมาย มาตรการและแนวทาง	6
ยุทธศาสตร์ที่ 1 การเพิ่มขีดสมรรถนะบุคลากร และยกระดับทักษะด้านเทคโนโลยีสารสนเทศแก่ผู้ใช้งานทุกระดับ	5
ยุทธศาสตร์ที่ 2 การเพิ่มประสิทธิภาพโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศให้สามารถใช้งานได้ สะดวก รวดเร็ว ปลอดภัย และมีมาตรฐาน	6
ยุทธศาสตร์ที่ 3 การพัฒนาระบบคลังข้อมูลที่เป็นเอกภาพและมีคุณภาพ สามารถใช้ประโยชน์จากข้อมูลร่วมกันได้	7
4. แผนพัฒนาระบบสารสนเทศ	9
แผนพัฒนาระบบสารสนเทศระยะสั้น ประจำปี พ.ศ. 2565	9
แผนพัฒนาระบบสารสนเทศระยะยาว ประจำปี พ.ศ. 2565 ถึง พ.ศ 2569	12
แผนงบประมาณรายจ่าย ประจำปีงบประมาณ พ.ศ. 2565-2569	15

ประวัติการจัดทำ และทบทวนเอกสาร

ครั้งที่	วันที่แก้ไข	รายละเอียด
00	11 พฤศจิกายน 2566	เผยแพร่เพื่อใช้งานครั้งที่ 1 ภายหลังการแปรสภาพบริษัทจากบริษัทจำกัดเป็นบริษัทมหาชนจำกัด

แผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ ประจำปี พ.ศ. 2565 – 2569

ของ

บริษัท บางกอก แอสเซท อินเตอร์กรุ๊ป จำกัด (มหาชน)

บทนำ

บริษัท บางกอก แอสเซท อินเตอร์กรุ๊ป จำกัด (มหาชน) (“**บริษัท**”) เป็นบริษัทที่ได้รับการยอมรับในการจำหน่ายบ้านตกแต่งแล้วขาย อันเนื่องมาจากศักยภาพด้านการตกแต่งบ้านที่สวยงามและทันสมัย มีระบบเทคโนโลยีสารสนเทศที่สามารถใช้งานได้ทุกที่ทุกเวลามาสนับสนุนในการทำงาน ซึ่งในการดำเนินภารกิจดังกล่าวจำเป็นต้องมีโครงสร้างพื้นฐานและเครือข่ายเทคโนโลยีสารสนเทศรองรับ ที่จะทำให้ภารกิจบรรลุเป้าหมายตามวิสัยทัศน์ของบริษัท โดยมีฝ่ายเทคโนโลยีสารสนเทศเป็นหน่วยงานรับผิดชอบในการบริหารจัดการระบบเทคโนโลยีสารสนเทศ และการสื่อสารภายในบริษัทซึ่งได้พัฒนาให้อยู่ในสถานะที่มีเสถียรภาพ ความสะดวกรวดเร็ว ความปลอดภัยและพร้อมใช้งานตลอดเวลา ตลอดจนได้พัฒนาระบบและบริการต่างๆ ให้มีประสิทธิภาพและมีความทันสมัยในการที่จะให้บริการกับพนักงานและผู้บริหารหน่วยงานต่างๆ

แผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศประจำปี พ.ศ. 2565 - 2569 ของฝ่ายเทคโนโลยีสารสนเทศ ฉบับนี้จัดทำขึ้นเพื่อเป็นแนวทางรองรับการพัฒนาด้านเทคโนโลยีสารสนเทศของบริษัทโดยตอบสนองต่อแผนกลยุทธ์ นโยบาย เป้าหมายและวัตถุประสงค์ของการดำเนินงานของบริษัทให้เหมาะสมกับสภาวะเศรษฐกิจ สังคมและความก้าวหน้าทางเทคโนโลยี

ปรัชญา และปณิธาน

“ฝ่ายเทคโนโลยีสารสนเทศมีจุดมุ่งหมายในการให้บริการเทคโนโลยีสารสนเทศ เพื่อสนับสนุนบริษัทในการดำเนินการตามพันธกิจ อย่างราบรื่น มีประสิทธิภาพและประสิทธิผล”

วิสัยทัศน์

“เป็นหน่วยงานหลักในการพัฒนาระบบเทคโนโลยีสารสนเทศและนำบริษัทไปสู่การเป็นองค์กรเทคโนโลยีสารสนเทศที่ไร้กระดาษ สามารถตอบสนองความต้องการของลูกค้าที่ทันสมัย และอย่างรวดเร็ว”

พันธกิจ

1. วางแผน และกำหนดกลยุทธ์ด้านเทคโนโลยีสารสนเทศ เพื่อสนับสนุน เพื่อให้สอดคล้องกับการดำเนินงานตามพันธกิจขององค์กร และทันต่อการเปลี่ยนแปลงของสภาวะการณ์
2. บริการสิ่งอำนวยความสะดวกต่างๆ สำหรับกิจกรรมด้านเทคโนโลยีสารสนเทศ
3. ให้บริการระบบเครือข่าย และระบบเทคโนโลยีสารสนเทศ แบบไร้ขอบเขต ไร้ซึ่งสถานที่ และเวลา

4. พัฒนาบุคลากรทุกระดับ ให้มีขีดสมรรถนะ และทักษะด้านเทคโนโลยีสารสนเทศที่เหมาะสมกับการปฏิบัติงาน
5. พัฒนาเพื่อเพิ่มประสิทธิภาพระบบเทคโนโลยีสารสนเทศ และระบบฐานข้อมูลที่สามารถสนับสนุนภารกิจขององค์กรได้อย่างถูกต้อง และรวดเร็ว

<u>เป้าหมาย</u>

1. มุ่งพัฒนาเทคโนโลยีสารสนเทศ (Digital Transformation) สู่ Paperless Company เพื่อให้บริษัทมีประสิทธิภาพและตอบสนองต่อลูกค้าได้อย่างรวดเร็ว
2. พัฒนาฝ่ายสารสนเทศให้เป็นหน่วยงานบริการที่มีปลอดภัย และมีมาตรฐานสากล
3. สร้างองค์กรที่ใช้เทคโนโลยีสารสนเทศให้เป็นที่ยอมรับ และสามารถตอบสนองต่อความต้องการได้อย่างสูงสุด

<u>การวิเคราะห์สถานภาพด้านเทคโนโลยีสารสนเทศ</u>

เพื่อให้บรรลุวัตถุประสงค์และเป้าหมายของการพัฒนาระบบเทคโนโลยีสารสนเทศของบริษัทได้ดำเนินการศึกษาวิเคราะห์สถานภาพและปัจจัยต่างๆ ที่เกี่ยวข้องกับการพัฒนาระบบเทคโนโลยีสารสนเทศในปัจจุบัน และแนวโน้มในอนาคตอันใกล้ ตลอดจนปัจจัยต่างๆ ที่มีผลกระทบต่อการพัฒนาด้านเทคโนโลยีสารสนเทศ ภายในองค์กร ซึ่งสามารถสรุปได้ดังนี้

1) จุดแข็ง/ข้อได้เปรียบ (Strength)
   (1) ผู้บริหารมีความรู้ด้านเทคโนโลยีสารสนเทศ
   (2) บุคลากรมีความรู้ความสามารถและกระตือรือร้นในการหาความรู้เพิ่มเติม
   (3) มีอุปกรณ์และเครื่องมือเพียงพอที่พร้อมให้บริการ
   (4) มีระบบสารสนเทศสนับสนุนทุกหน่วยงาน
   (5) บริการด้วยความจริงใจและเป็นกันเอง
   (6) มีงบประมาณเพียงพอสำหรับใช้ในการดำเนินงานภายในของฝ่ายสารสนเทศ
   (7) มีการพัฒนาระบบ (Application) และเว็บไซต์ให้ทันสมัยอยู่เสมอ

2) จุดอ่อน/ปัญหา (Weakness)
   (1) บริษัทเพิ่งเริ่มกิจการที่เป็นมาตรฐาน
   (2) บุคลากรในด้านเทคโนโลยีที่มีความสามารถไม่เพียงพอต่อความต้องการ และหายาก
   (3) บุคลากรยังมีการตั้งเป้าหมายชัดเจนในการทำงานไม่ชัดเจน
   (4) การให้บริการด้านต่างๆ ของฝ่ายสารสนเทศ ไม่มีการเผยแพร่ให้หน่วยงานต่างๆ ทราบอย่างทั่วถึง
   (5) ขาดประสบการณ์ และทักษะเฉพาะทางที่ต้องอาศัยความรู้ด้านเทคนิคชั้นสูง

(6) บุคลากรพัฒนา และเรียนรู้ไม่ทันต่อการเปลี่ยนแปลงเทคโนโลยีสารสนเทศที่รวดเร็ว

(7) มีระบบการใช้งานหลายระบบ และซับซ้อน

(8) มีบางระบบไม่สามารถเชื่อมโยงกันได้

3) โอกาส (Opportunity)

(1) องค์กรให้ความสนใจ และยอมรับการเปลี่ยนแปลงทางด้านเทคโนโลยีสารสนเทศ

(2) ผู้บริหารเข้าใจ และให้การสนับสนุนอย่างจริงจังกับการพัฒนาเทคโนโลยีสารสนเทศ

(3) เทคโนโลยีใหม่เกิดขึ้นอย่างมากมาย ทำให้สามารถเลือกสิ่งที่ต้องการและ ใช้กับองค์กรได้ง่ายขึ้น

(4) นโยบายให้การสนับสนุนด้านเทคโนโลยีสารสนเทศ และงบประมาณ

(5) เทคโนโลยีใหม่ๆ ส่งผลให้เกิดการพัฒนาทำให้มีความรวดเร็ว และตอบสนองต่อความต้องการมากขึ้น

4) อุปสรรค (Threat)

(1) การเปลี่ยนแปลงเทคโนโลยีที่รวดเร็ว

(2) พนักงานไม่เข้าใจขอบเขตการทำงานหรือการปฏิบัติงานของฝ่ายเทคโนโลยีสารสนเทศ

(3) พนักงานบางส่วนยังไม่สามารถปรับตัวต่อการเปลี่ยนแปลงของเทคโนโลยียุคดิจิตอลที่แท้จริง

(4) ระบบคอมพิวเตอร์ที่ใช้งานในปัจจุบันยังมีขีดความสามารถจำกัด

<u>บทวิเคราะห์สถานภาพด้านปัจจัยต่างๆ</u>

บริษัทมีระบบเทคโนโลยีสารสนเทศ และการสื่อสารทั้งในส่วนของระบบเครือข่าย และระบบงานสารสนเทศ เพื่อรองรับการปฏิบัติงานด้านต่างๆ ทั้งนี้สามารถวิเคราะห์ และประเมินออกเป็นจุดแข็ง จุดอ่อน ข้อได้เปรียบและข้อเสียเปรียบได้ ดังต่อไปนี้

ปัจจัย	จุดแข็ง/ข้อได้เปรียบ	จุดอ่อน/ปัญหา
ปัจจัยด้านอุปกรณ์ และซอฟต์แวร์	บริษัทมีอุปกรณ์คอมพิวเตอร์ที่เพียงพอต่อเจ้าหน้าที่	ระบบเทคโนโลยีสารสนเทศของบริษัท อยู่ระหว่างการเชื่อมโยงเข้าด้วยกัน
ปัจจัยด้านเครือข่าย	บริษัทมีการเชื่อมต่อระบบเครือข่ายด้วย Cloud Base	ระบบเครือข่ายของผู้ให้บริการภายนอกยังไม่เสถียร

ปัจจัย	จุดแข็ง/ข้อได้เปรียบ	จุดอ่อน/ปัญหา
ปัจจัยด้านบุคลากร	บริษัทมีบุคคลากรด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ	บุคคลากรบางกลุ่มไม่สามารถเปลี่ยนแปลงเพื่อตอบสนองในยุคดิจิตอลแท้จริง บุคลากรด้านเทคโนโลยีสารสนเทศมี Turn Over ที่สูงเนื่องจากเป็นที่ต้องการของตลาด
ปัจจัยด้านข้อมูล	บริษัทมีการให้บริการข้อมูลข่าวสารและการประชาสัมพันธ์ ผ่านเครือข่ายอินเทอร์เน็ตอย่างต่อเนื่อง	บริษัทไม่มีฐานข้อมูลกลุ่มเป้าหมายทางการตลาดอย่างรวดเร็วและเพียงพอ
ปัจจัยด้านงบประมาณ	บริษัทมีการกำหนดงบประมาณสำหรับการพัฒนาระบบเทคโนโลยีสารสนเทศอย่างต่อเนื่อง	ค่าใช้จ่ายในการพัฒนาระบบเทคโนโลยีสารสนเทศมีมูลค่าสูง

<u>แนวทางการแก้ไขจุดอ่อนและอุปสรรค</u>

บริษัทมีแนวทางในการแก้ไขจุดอ่อนด้านบุคลากรโดยการประสานงานอย่างใกล้ชิดระหว่างคณะทำงานด้านเทคโนโลยีสารสนเทศ และบุคลากรด้านเทคโนโลยีสารสนเทศรวมไปถึงมีการตั้งงบประมาณด้านเทคโนโลยีสารสนเทศที่เพียงพออย่างต่อเนื่อง เพื่อให้เทคโนโลยีสารสนเทศต่างๆ มีความทันสมัย รวดเร็ว ตอบสนองต่อผู้ใช้ อย่างมีเสถียรภาพ สำหรับด้านระบบ และเครื่องมือด้านเทคโนโลยีสารสนเทศ ที่มีการเปลี่ยนแปลงอย่างรวดเร็ว ซึ่งอาจทำให้ระบบ และเครื่องมือที่มีอยู่ไม่มีความทันสมัยนั้น บริษัทได้วางแผนการบำรุงรักษาระบบและเครื่องมือต่างๆ อย่างสม่ำเสมอ

<u>ยุทธศาสตร์ เป้าประสงค์ มาตรการและแนวทาง</u>

ยุทธศาสตร์ที่ 1

การเพิ่มขีดสมรรถนะบุคลากร และยกระดับทักษะด้านเทคโนโลยีสารสนเทศแก่ผู้ใช้งานทุกระดับ

เป้าประสงค์

1. เพื่อพัฒนาบุคลากรทุกระดับให้มีสมรรถนะและขีดความสามารถในการปฏิบัติงานโดยใช้เทคโนโลยีสารสนเทศอย่างเหมาะสม

มาตราการ

1.1 จัดทำหลักสูตรด้านเทคโนโลยีสารสนเทศสำหรับบุคลากรอย่างเสมอทั้ง Online และ Offline

1.1.1 จัดทำหลักสูตรด้านเทคโนโลยีสารสนเทศสำหรับบุคลากร 3 กลุ่ม คือ ผู้บริหาร พนักงานทั่วไป และพนักงานฝ่านเทคโนโลยีสารสนเทศ

1.1.2 ให้พนักงานฝ่ายเทคโนโลยีสารสนเทศพัฒนาตนเองอย่างน้อย 40ชั่วโมงต่อปี

ยุทธศาสตร์ที่ 2

การเพิ่มประสิทธิภาพโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศให้สามารถใช้งานได้สะดวก รวดเร็ว ปลอดภัย และมีมาตรฐานสากล

เป้าประสงค์

1. เพื่อให้มีระบบสื่อสารระหว่าง บุคลากรในหน่วยงานและ ระหว่างอุปกรณ์/เครื่องมือสารสนเทศ ที่สามารถใช้สื่อสารได้สะดวก รวดเร็ว และปลอดภัย
2. เพื่อให้มีโครงสร้างพื้นฐานระบบสารสนเทศที่เหมาะสม เพียงพอ พร้อมใช้งาน และมีความมั่นคงปลอดภัยภายใต้กฎหมาย

มาตราการ

1.1 เลือกสรร และปรับปรุงระบบเครือข่ายคอมพิวเตอร์ให้มีประสิทธิภาพ

1.1.1 จัดหา ปรับเปลี่ยนอุปกรณ์ และโครงข่ายสายสัญญาณระบบเครือข่ายคอมพิวเตอร์ให้สามารถใช้งานได้อย่างรวดเร็ว ปลอดภัย ไม่มีสะดุด

1.1.2 พัฒนาระบบการให้บริการด้านเครือข่ายคอมพิวเตอร์ภายในองค์กรให้ครอบคลุม

1.2 เลือกสรรและปรับปรุงระบบการให้บริการด้านคอมพิวเตอร์อย่างเป็นระบบ และมีประสิทธิภาพ

1.2.1 จัดหาและปรับเปลี่ยนเครื่องคอมพิวเตอร์ เพื่อสนับสนุนภารกิจของทุกหน่วยงานอย่างต่อเนื่องและมีประสิทธิภาพ

1.2.2 ปรับปรุงระบบการให้บริการติดตั้ง ซ่อมบำรุง อุปกรณ์เครือข่าย อุปกรณ์คอมพิวเตอร์ ให้สามารถติดตามและตรวจสอบได้

1.3 ปรับปรุงระบบคอมพิวเตอร์ของทุกหน่วยงานให้มีประสิทธิภาพ

1.3.1 จัดหาและปรับเปลี่ยนอุปกรณ์คอมพิวเตอร์ของทุกหน่วยงานให้มีประสิทธิภาพอย่างต่อเนื่อง

1.4 มีโปรแกรมลิขสิทธิ์สนับสนุนการใช้งานอย่างเพียงพอ

1.4.1 จัดซื้อโปรแกรมลิขสิทธิ์ที่เหมาะสม และอย่างเพียงพอ

1.4.2 สนับสนุนการใช้โปรแกรมระบบเปิด หรือฟรีแวร์

ยุทธศาสตร์ที่ 3

การพัฒนาระบบคลังข้อมูลที่เป็นเอกภาพ รวดเร็ว และมีคุณภาพ ไร้กระดาษ และสามารถใช้ประโยชน์จากข้อมูลร่วมกันได้

เป้าประสงค์

1. เพื่อให้ระบบคลังข้อมูลกลางขององค์กรมีประสิทธิภาพ และประสิทธิผล ด้วยระบบดิจิตอลสามารถเรียกใช้งานร่วมกันได้ทุกที ทุกทาง และทุกเวลา
2. เพื่อให้มีระบบวิเคราะห์ และจัดเก็บข้อมูลแบบ Big Data
3. เพื่อสนับสนุนการบริหาร และการตัดสินใจ ได้อย่างรวดเร็ว ทันต่อความต้องการ

มาตราการ

1.1 ปรับปรุงและพัฒนาระบบคลังข้อมูลกลางขององค์กรให้มีประสิทธิภาพ และประสิทธิผล

1.1.1 จัดหา ปรับเปลี่ยนอุปกรณ์ที่สนับสนุนระบบคลังข้อมูล

1.1.2 ปรับปรุงระบบคลังข้อมูลให้มีประสิทธิภาพ ประสิทธิผล และมีความทันสมัย

1.1.3 ส่งบุคลากรของฝ่ายเทคโนโลยีสารสนเทศ เข้าอบรมระบบคลังข้อมูล เพื่อพัฒนาให้มีศักยภาพที่สูงขึ้น

1.2 ปรับปรุง และพัฒนาระบบวิเคราะห์และจัดเก็บข้อมูลแบบ Big Data

1.2.1 ปรับปรุงระบบคลังข้อมูลให้มีประสิทธิภาพ ประสิทธิผล สามารถรองรับการจัดเก็บข้อมูลแบบ Big Data

1.2.2 ฝึกอบรมบุคลากรให้มีประสบการณ์การทำงานให้สอดคล้องกับข้อมูลแบบ Big Data

1.3 พัฒนาระบบสารสนเทศ และการบูรณาการเชื่อมโยงข้อมูลเพื่อสนับสนุนการบริหาร และการตัดสินใจ

1.3.1 ออกแบบระบบฐานข้อมูลของระบบสารสนเทศ ให้สอดคล้องกับการทำงานขององค์กร เพื่อช่วยสนับสนุนการบริหารและการตัดสินใจ ได้อย่างรวดเร็ว

1.3.2 พัฒนาระบบคลังข้อมูลด้วยเทคโนโลยีใหม่ๆ โดยใช้เทคโนโลยีอย่างเหมาะสม

แผนการพัฒนาระบบสารสนเทศ

บริษัทกำหนดแผนในการพัฒนาฝ่ายสานสนเทศ ระยะ 5 ปี (พ.ศ. 2565 -2569) ประกอบแผนระยะสั้น 1 ปี (พ.ศ. 2565) และแผนระยะยาว 5 ปี (พ.ศ.2565-2569) โดยได้กำหนดผลลัพธ์สำคัญสู่ความสำเร็จในช่วงของการพัฒนาภายใต้ 4 ยุทธศาสตร์ ซึ่งจะต้องดำเนินการควบคู่กันไปจึงจะทำให้การพัฒนาประสบความสำเร็จดังนี้

มิติ	ผลลัพธ์สำคัญสู่ความสำเร็จ	มาตรการพัฒนา
ความพึงพอใจ	1) ผู้รับบริการ มีความพึงพอใจระดับสูงขึ้นไปมากกว่า 75% ในการให้บริการ	1) สร้างความพึงพอใจที่ดีให้กับผู้รับบริการได้อย่างต่อเนื่อง
คุณภาพ	1) ระบบเทคโนโลยีสารสนเทศขององค์กรอยู่ในเกณฑ์มาตรฐานระดับดีเยี่ยมและได้รับการยอมรับ	1) สรรหาและปรับปรุงระบบเทคโนโลยีสารสนเทศให้ได้มาตรฐานและมีประสิทธิภาพอย่างต่อเนื่อง
ประสิทธิภาพ	1) มีระบบการบริหารจัดการที่มีประสิทธิภาพ	1) พัฒนาระบบบริหารและการจัดการให้มีความคล่องตัวมีประสิทธิภาพและประสิทธิผลสูงสุด
การพัฒนาองค์กร	1) มีงบประมาณ เครื่องมือและเทคโนโลยีสนับสนุนการปฏิบัติงานอย่างพอเพียง 2) มีบุคลากรที่มีความรู้ความสามารถเฉพาะทางด้านการบริหารจัดการอย่างเพียงพอ	1) มีการบริหารจัดการงบประมาณและทรัพยากรที่มีประสิทธิภาพ 2) สนับสนุนทรัพยากรบุคคลให้สอดคล้องกับภารกิจด้านเทคโนโลยีสารสนเทศ

แผนพัฒนาระบบสารสนเทศระยะสั้น ประจำปี พ.ศ. 2565

เป้าหมาย	โครงการ	ระยะเวลาดำเนินการ / เดือน											
		1	2	3	4	5	6	7	8	9	10	11	12
<u>ยุทธศาสตร์ที่ 1</u> การเพิ่มขีดสมรรถนะบุคลากร และยกระดับทักษะด้านเทคโนโลยีสารสนเทศแก่ผู้ใช้งานทุกระดับ													
1.1 เพื่อพัฒนาเพื่อพัฒนาบุคลากรทุกระดับให้มีสมรรถนะและขีดความสามารถในการปฏิบัติงานโดยใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมบุคลากรทุกระดับให้มีสมรรถนะและขีดความสามารถในการปฏิบัติงานโดยใช้เทคโนโลยีสารสนเทศอย่างเหมาะสม	ฝึกอบรมด้านคอมพิวเตอร์สำหรับบุคคลากรทั่วไป			○			○			○			○
	ตัวชี้วัด : จำนวนหลักสูตรเพื่อพัฒนาบุคลากรทั่วไป ด้านสารสนเทศ (ครั้ง)			1			1			1			1
	ฝึกอบรมด้านด้านการบริหารระบบสารสนเทศสำหรับบุคคลากรด้านเทคโนโลยีสารสนเทศ (40ชั่วโมง)												
	ตัวชี้วัด : จำนวนหลักสูตรเพื่อพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศ (40 ชั่วโมง)												

เป้าหมาย	โครงการ	ระยะเวลาดำเนินการ / เดือน											
		1	2	3	4	5	6	7	8	9	10	11	12
<u>ยุทธศาสตร์ที่ 2</u> การเพิ่มประสิทธิภาพโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศให้สามารถใช้งานได้ สะดวก รวดเร็ว ปลอดภัย และมีมาตรฐาน													
2.1 เพื่อให้มีระบบสื่อสารระหว่าง บุคลากรในหน่วยงานและ ระหว่างอุปกรณ์/เครื่องมือสารสนเทศ ที่สามารถใช้สื่อสารได้สะดวก รวดเร็ว และปลอดภัย 2.2 เพื่อให้มีโครงสร้างพื้นฐานระบบสารสนเทศที่เหมาะสม เพียงพอ พร้อมใช้งาน และมีความมั่นคงปลอดภัย	งานให้บริการและซ่อมบำรุงระบบคอมพิวเตอร์			○			○			○			○
	ตัวชี้วัด : จำนวนครั้งที่คอมพิวเตอร์ชำรุดน้อยกว่า (ครั้ง)	5	5	5	5	5	5	5	5	5	5	5	5
	งานจัดหาโปรแกรมลิขสิทธิ์และโปรแกรมทดแทน (ฟรีแวร์)				○				○				○
	ตัวชี้วัด : ร้อยละความสำเร็จในการดำเนินงานจัดหาโปรแกรม				20				50				10
	โครงการพัฒนาระบบเครือข่ายความเร็วสูง High Speed Network และ Security						○						
	ตัวชี้วัด : ร้อยละความสำเร็จในการดำเนินงาน						50						
	โครงการพัฒนาระบบเครือข่ายไร้สาย ความเร็วสูง Wi-Fi									○			
	ตัวชี้วัด : ร้อยละความสำเร็จในการดำเนินงาน									90			

เป้าหมาย	โครงการ	ระยะเวลาดำเนินการ / เดือน											
		1	2	3	4	5	6	7	8	9	10	11	12
<u>ยุทธศาสตร์ที่ 2</u> การเพิ่มประสิทธิภาพโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศให้สามารถใช้งานได้ สะดวก รวดเร็ว ปลอดภัย และมีมาตรฐาน													
	โครงการพัฒนาระบบ AD Server						○						○
	ตัวชี้วัด : ร้อยละความสำเร็จในการดำเนินงาน						70						10
<u>ยุทธศาสตร์ที่ 3</u> การพัฒนาระบบคลังข้อมูลที่เป็นเอกภาพและมีคุณภาพ สามารถใช้ประโยชน์จากข้อมูลร่วมกันได้													
3.1 เพื่อให้ระบบคลังข้อมูลกลางขององค์กรมีประสิทธิภาพ สามารถเรียกใช้งานร่วมกันได้ 3.2 เพื่อให้มีระบบวิเคราะห์และจัดเก็บข้อมูลแบบ Big Data 3.3 เพื่อสนับสนุนการบริหารและการตัดสินใจ	โครงการพัฒนาระบบคลังข้อมูล Big Data												○
	ตัวชี้วัด : ร้อยละความสำเร็จในการดำเนินงานโครงการพัฒนาระบบคลังข้อมูล Big Data และพัฒนาระบบหลักให้มีประสิทธิภาพมากยิ่งขึ้น และให้เชื่อมโยงกัน												20

แผนพัฒนาระบบสารสนเทศระยะยาว ประจำปี พ.ศ. 2565 ถึง พ.ศ 2569

เป้าหมาย	โครงการ	ระยะเวลาดำเนินการ / เดือน				
		2565	2566	2567	2568	2569
ยุทธศาสตร์ที่ 1 การเพิ่มขีดสมรรถนะบุคลากร และยกระดับทักษะด้านเทคโนโลยีสารสนเทศแก่ผู้ใช้งานทุกระดับ						
1.1 เพื่อพัฒนาบุคลากรทุกระดับให้มีสมรรถนะและขีดความสามารถในการปฏิบัติงานโดยใช้เทคโนโลยีสารสนเทศอย่างเหมาะสม	ฝึกอบรมด้านคอมพิวเตอร์สำหรับบุคคลากรทั่วไป	←				→
	ตัวชี้วัด : จำนวนหลักสูตรเพื่อพัฒนาบุคลากรด้านสารสนเทศ	4	4	4	4	4
	ฝึกอบรมด้านด้านการบริหารระบบสารสนเทศ สำหรับบุคคลากรด้านเทคโนโลยีสารสนเทศ (ชั่วโมง)	←				→
	ตัวชี้วัด : จำนวนหลักสูตรเพื่อพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศ (ชั่วโมง)	40	40	40	40	40

เป้าหมาย	โครงการ	ระยะเวลาดำเนินการ / เดือน				
		2565	2566	2567	2568	2569
<u>ยุทธศาสตร์ที่ 2</u> การเพิ่มประสิทธิภาพโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศให้สามารถใช้งานได้ สะดวก รวดเร็ว ปลอดภัย และมีมาตรฐานสากล						
2.1 เพื่อให้มีระบบสื่อสารระหว่างบุคลากรในหน่วยงานและ ระหว่างอุปกรณ์/เครื่องมือสารสนเทศ ที่สามารถใช้สื่อสารได้สะดวก รวดเร็ว และปลอดภัย 2.2 เพื่อให้มีโครงสร้างพื้นฐานระบบสารสนเทศที่เหมาะสม เพียงพอ พร้อมใช้งาน และมีความมั่นคงปลอดภัย	งานให้บริการและซ่อมบำรุงระบบคอมพิวเตอร์	←				→
	ตัวชี้วัด : จำนวนครั้งที่คอมพิวเตอร์ชำรุดน้อยกว่า	60	60	60	60	60
	งานจัดหาโปรแกรมลิขสิทธิ์และโปรแกรมทดแทน (ฟรีแวร์)	←				→
	ตัวชี้วัด : จำนวน license ในการดำเนินงานจัดหาโปรแกรม	50	12.5	12.5	12.5	12.5
	โครงการพัฒนาระบบเครือข่ายความเร็วสูง High Speed Network และ Security	←				→
	ตัวชี้วัด : ร้อยละความสำเร็จในการดำเนินงาน	30	20	20	15	15

เป้าหมาย	โครงการ	ระยะเวลาดำเนินการ / เดือน				
		2565	2566	2567	2568	2569
<u>ยุทธศาสตร์ที่ 2</u> การเพิ่มประสิทธิภาพโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศให้สามารถใช้งานได้ สะดวก รวดเร็ว ปลอดภัย และมีมาตรฐาน						
	โครงการพัฒนาระบบ AD Server	←	—	—	—	→
	ตัวชี้วัด : จำนวนของ AD ที่เพิ่มขึ้นในระบบ AD Server	50	12.5	12.5	12.5	12.5
<u>ยุทธศาสตร์ที่ 3</u> การพัฒนาระบบคลังข้อมูลที่เป็นเอกภาพและมีคุณภาพ สามารถใช้ประโยชน์จากข้อมูลร่วมกันได้						
3.4 เพื่อให้ระบบคลังข้อมูลกลางขององค์กรมีประสิทธิภาพ สามารถเรียกใช้งานร่วมกันได้ 3.5 เพื่อให้มีระบบวิเคราะห์และจัดเก็บข้อมูลแบบ Big Data 3.6 เพื่อสนับสนุนการบริหารและการตัดสินใจ	โครงการพัฒนาระบบคลังข้อมูล Big Data (Business Transformation) and Improve Core Business System Productivity	←	—	—	—	→
	ตัวชี้วัด : ร้อยละความสำเร็จในการดำเนินงานโครงการพัฒนาระบบคลังข้อมูล Big Data และระบบหลักให้มีประสิทธิภาพและให้เชื่อมโยงกัน	12	22	22	22	22

แผนงบประมาณรายจ่าย ประจำปีงบประมาณ พ.ศ. 2565-2569

ยุทธศาสตร์	โครงการ	ปีงบประมาณ พ.ศ.					รวมทั้งสิ้น
		2565	2566	2567	2568	2569	
<u>ยุทธศาสตร์ที่ 1</u> การเพิ่มขีดสมรรถนะบุคลากร	ฝึกอบรมด้านคอมพิวเตอร์สำหรับบุคคลากรทั่วไป	10,000	10,000	10,000	10,000	10,000	50,000
	ฝึกอบรมด้านด้านการบริหารระบบสารสนเทศ สำหรับบุคคลากรด้านเทคโนโลยีสารสนเทศ	20,000	20,000	20,000	20,000	20,000	100,000
<u>ยุทธศาสตร์ที่ 2</u> การเพิ่มประสิทธิภาพโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ	งานให้บริการและซ่อมบำรุงระบบคอมพิวเตอร์	20,000	20,000	20,000	20,000	20,000	100,000
	จัดซื้อคอมพิวเตอร์/แท็บเล็ตให้เพียงพอกับพนักงาน	600,000	600,000	600,000	600,000	600,000	3,000,000
	งานจัดหาโปรแกรมลิขสิทธิ์และโปรแกรมทดแทน (ฟรีแวร์)	600,000	150,000	150,000	150,000	150,000	1,200,000
	โครงการพัฒนาระบบเครือข่ายความเร็วสูง High Speed Network /Security	300,000	200,000	200,000	200,000	200,000	1,100,000
	โครงการพัฒนาระบบ AD Server	200,000	50,000	50,000	50,000	50,000	400,000

ยุทธศาสตร์	โครงการ	ปีงบประมาณ พ.ศ.					รวมทั้งสิ้น
		2565	2566	2567	2568	2569	
<u>ยุทธศาสตร์ที่ 3</u> การพัฒนาระบบคลังข้อมูลที่เป็นเอกภาพและมีคุณภาพ	โครงการพัฒนาระบบคลังข้อมูล Big Data (Business Transformation)/ พัฒนาระบบหลักให้มีประสิทธิภาพและมีการเชื่อมโยงกัน	1,000,000	1,700,000	1,700,000	1,700,000	1,700,000	7,800,000
รวมทั้งสิ้น		2,750,000	2,750,000	2,750,000	2,750,000	2,750,000	13,750,000

*งบประมาณ + ค่าใช้จ่าย ของฝ่ายเทคโนโลยีสารสนเทศ ประมาณการ 1 % ของรายได้

ประวัติการการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 มีนาคม 2565	น.ส.ธนิศร ธนวงศ์เกษม
2	1.1	1. แก้ไขผู้อนุมัติตามรายงานตรวจสอบภายในครั้งที่ 1 ปี 2565 จาก บริษัท สอบบัญชี ไอ วี แอล จำกัด 2. ปรับปรุงในส่วนงบประมาณและโครงการให้เหมาะสมจากรายงานตรวจสอบภายในครั้งที่ 1 ปี 2565 จาก บริษัท สอบบัญชี ไอ วีแอล จำกัด	1 สิงหาคม 2565	น.ส.ธนิศร ธนวงศ์เกษม

เพื่อให้ทราบโดยทั่วกันและยึดถือปฏิบัติให้เป็นไปในแนวทางเดียวกัน จึงประกาศใช้แผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ ประจำปี พ.ศ. 2565 - 2569 แผนฉบับนี้มีผลบังคับใช้ตั้งแต่วันที่ 11 พฤศจิกายน 2566

ลงชื่อ _____

(นายศิริพล ยอดเมืองเจริญ)

ประธานคณะกรรมการบริษัท

บริษัท บางกอก แอสเซท อินเตอร์กรุ๊ป จำกัด (มหาชน)

ขั้นตอนการเข้าใช้งานห้อง Server

วัตถุประสงค์ เพื่อให้การใช้งานห้อง Server มีความปลอดภัย ทั้งอุปกรณ์ และข้อมูลที่อยู่ภายในห้อง Server สูงสุด จึงกำหนดแนวทางในการปฏิบัติในการเข้าใช้งานห้อง Server ดังนี้

1. บุคคลผู้มีสิทธิเข้าใช้งานห้อง Server ของบริษัท
   1.1. เจ้าหน้าที่สารสนเทศ ที่มีหน้าที่รับผิดชอบดูแลเครื่อง Server และอุปกรณ์เครือข่าย(Network) รวมทั้งอุปกรณ์ที่เกี่ยวข้องทั้งหมด
   1.2. ประธานกรรมการบริหาร
   1.3. เจ้าหน้าที่ ที่มีหน้าที่ดูแลอุปกรณ์อื่นๆ ภายในห้อง Server เช่น เครื่องปรับอากาศ ระบบไฟฟ้า เจ้าหน้าทำความสะอาด Smoke Detector อุปกรณ์ดับเพลิง เป็นต้น
2. การขอเข้าใช้ห้อง Server มีขั้นตอนดังนี้
   2.1. เจ้าหน้าที่สารสนเทศที่มีหน้าที่รับผิดชอบโดยตรง สามารถเข้าออกได้ตลอดเวลา โดยการบันทึกรายละเอียดการปฏิบัติงาน และลงลายมือชื่อในบันทึกการเข้าใช้ห้อง Server หลังจากเข้าใช้งานห้อง Server เรียบร้อยแล้ว
   2.2. บุคลากรอื่นของบริษัท จะต้องขออนุญาตเข้าใช้ห้อง Server โดยการกรอกแบบฟอร์มขออนุญาตการเข้าห้อง Server ที่ได้รับการอนุมัติจากผู้บริหารฝ่ายคอมพิวเตอร์ ส่งให้เจ้าหน้าที่สารสนเทศผู้ดูแลห้องก่อนเข้าใช้งาน อย่างน้อย 1 ชั่วโมงในกรณีปกติ แล้วบันทึกรายละเอียดการปฏิบัติงาน และลงลายมือชื่อในบันทึกการเข้าใช้ห้อง Server หลังจากเข้าใช้งานห้อง Server เรียบร้อยแล้ว
   2.3. ประธานกรรมการบริหาร สามารถเข้าห้อง Server ได้ตลอดเวลา โดยการแจ้งต่อเจ้าหน้าที่สารสนเทศที่รับผิดชอบก่อนเข้าห้อง Server แล้วลงบันทึกรายละเอียด และลงลายมือชื่อในบันทึกการเข้าใช้ห้อง Server หลังจากเข้าใช้งานห้อง Server เรียบร้อยแล้ว
   2.4. บุคคลภายนอกบริษัท จะต้องขออนุญาตการเข้าปฏิบัติงานในห้อง Server โดยการกรอกแบบฟอร์มการขออนุญาตการเข้าห้อง Server ที่ได้รับการอนุมัติจากผู้บริหารฝ่ายคอมพิวเตอร์ ส่งให้เจ้าหน้าที่สารสนเทศที่ดูแลห้อง Server ก่อนเข้าใช้งานอย่างน้อย 6 ชั่วโมงในกรณีปกติ และจะต้องมีเจ้าหน้าทีของสารสนเทศดูแล ลงบันทึกรายละเอียดการปฏิบัติงาน และลงลายมือชื่อในบันทึกการเข้าใช้ห้อง Server หลังจากเข้าใช้งานห้อง Server เรียบร้อยแล้ว
3. ระยะเวลาการเข้าใช้งานห้อง Server มีรายละเอียด ดังนี้

3.1. วันและเวลาที่ปฏิบัติงานตามปกติ คือ จันทร์-เสาร์ 8.30-17.30 น.

3.2. วันหยุด หรือวันนักขัตฤกษ์ จะต้องทำหนังสือหรือหลักฐาน และแผนปฏิบัติงาน แจ้งให้เจ้าหน้าที่ทราบล่วงหน้า อย่างน้อย 2 วันทำการ

3.3. กรณีฉุกเฉิน หรือเหตุฉุกเฉิน เจ้าหน้าที่ ที่เกี่ยวข้อง หรือได้รับอนุญาต สามารถเข้าปฏิบัติงานได้ทันที และตลอดเวลา โดยแจ้งต่อเจ้าหน้าที่สารสนเทศผู้ดูแลห้อง Server ให้ทราบถึงเหตุผลและความจำเป็นในการเข้าใช้งาน

ผู้อนุมัติ

ลงชื่อ _____

( )

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ _____

ลงชื่อ _____

( )

ผู้รับผิดชอบ

วันที่ _____

1. วัตถุประสงค์

1.1. เพื่อเป็นมาตรฐาน/แนวทางปฏิบัติในจำแนกข้อมูลภายในบริษัทให้ชัดเจน และปลอดภัย

1.2. เพื่อเป็นมาตรฐาน/แนวทางปฏิบัติการบริหารจัดการข้อมูลภายในให้ปลอดภัย และแบ่งแยกตามแผนก

1.3. เพื่อป้องกัน และควบคุมข้อมูลที่มีสำคัญของบริษัทให้ปลอดภัย ไม่ให้มีความเสี่ยงจากการรั่วไหลของข้อมูล

2. ความหมาย

2.1. **Confidential** (Top Confidentiality Level) เป็นข้อมูลที่เป็นความลับสูงสุด ระหว่างผู้ที่ได้รับอนุญาตเท่านั้น เช่น ข้อมูลเงินเดือน ข้อมูลที่เป็นกลยุทธบริษัท ข้อมูลการเงินของบริษัท เป็นต้น

2.2. **Restricted** (Medium Confidentiality Level) เป็นข้อมูลที่จำกัดเฉพาะกลุ่ม เฉพาะแผนก เช่น ข้อมูลทางกฎหมาย เป็นต้น

2.3. **Internal Use Only** (Lowest Level of Confidentiality) เป็นข้อมูลที่ใช้ภายในบริษัทเท่านั้น สามารถแลกเปลี่ยนระหว่างฝ่าย ระหว่างแผนกได้ เช่น ผังองค์กร ค่าใช้จ่ายแต่ล่ะแผนก เป็นต้น

2.4. **Public** (Everyone can see the Information) เป็นข้อมูลที่สามารถเปิดเผยไปยังสาธารณะชนได้ เช่น ข้อมูลประชาสัมพันธ์บริษัท ข้อมูลที่ให้กับนักข่าว ข้อมูลที่รายงานต่อกระทรวงพาณิชย์ เป็นต้น

3. ขั้นตอนการจำแนกข้อมูล

3.1. ผู้ดูแล IT infrastructure จะมีการให้ทบทวนการจำแนกข้อมูล ส่งไปยังเจ้าของ อย่างน้อยปีล่ะ 1 ครั้ง

3.2. ผู้ดูแลทั้ง IT Infrastructure เป็นผู้รวบรวม และดูแลในการปรับปรุงรายการของข้อมูล การจำแนกข้อมูลให้เป็นปัจจุบันอย่างสม่ำเสมอ

3.3. นำเสนอต่อผู้บริหาร IT ลงนามรับทราบ

3.4. การจำแนกข้อมูลในระบบ Share files ของบริษัท

4. ขั้นตอนการบริหารจัดการ Files Sharing

4.1. ผู้ใช้ กรอกรายละเอียด ในแบบคำขอรับสิทธิ์การใช้ Share files หรือ เพิ่ม Folder ใน Server ผ่านระบบ เช่น ชื่อ-นามสกุล, ตำแหน่งงาน, แผนก, ฝ่าย แล้ว เลือก Server / Folder ที่ต้อง ก่อนส่งไปยังผู้มีอำนาจอนุมัติ

4.2. เมื่อเอกสารถูกอนุมัติผ่านระบบมายังเจ้าหน้าที่ฝ่ายสารสนเทศที่ดูแล จะดำเนินการตรวจสอบดังนี้

4.3. กรณีที่กรอกคำขอไม่ถูกต้อง หรือ ข้อมูลไม่ครบถ้วน เจ้าหน้าที่ฝ่ายสารสนเทศ จะปฏิเสธการขอ แล้วจะถูกส่งกลับไปยังผู้ขอ ให้แก้ไขข้อมูลจนกว่าจะครบถ้วน และถูกต้อง

4.4. กรณีที่กรอกคำขอมีข้อมูลถูกต้อง และครบถ้วน เจ้าหน้าที่ฝ่ายสารสนเทศดำเนินกำหนดสิทธิ์ให้ตามคำขอ แล้วส่งผ่านให้ผู้จัดการฝ่ายสารสนเทศอนุมัติ โดยการกด Completed ในระบบ เป็นอันเสร็จสิ้นกระบวนการการขอสิทธิ์

5. ขั้นตอนขอสิทธิ์ใช้งาน

5.1. ผู้ขอกรอกรายละเอียดแบบคำร้องขอรับสิทธิ์การใช้ระบบงานผ่านระบบ Kintone และส่งไปยังผู้มีอำนาจอนุมัติ

5.2. เมื่อเอกสารถูกอนุมัติผ่านระบบมายังเจ้าหน้าที่ฝ่ายสารสนเทศที่ดูแล จะดำเนินการตรวจสอบดังนี้

5.2.1. กรณีที่กรอกคำขอไม่ถูกต้อง หรือ ข้อมูลไม่ครบถ้วน เจ้าหน้าที่ฝ่ายสารสนเทศ จะปฏิเสธการขอ แล้วจะถูกส่งกลับไปยังผู้ขอ ให้แก้ไขข้อมูลจนกว่าจะครบถ้วน และถูกต้อง

5.2.2. กรณีที่กรอกคำขอมีข้อมูลถูกต้อง และครบถ้วน เจ้าหน้าที่ฝ่ายสารสนเทศดำเนินกำหนดสิทธิ์ให้ตามคำขอ แล้วส่งผ่านให้ผู้จัดการฝ่ายสารสนเทศอนุมัติ โดยการกด Completed ในระบบ เป็นอันเสร็จสิ้นกระบวนการการขอสิทธิ์

6. ตารางรายละเอียดของแต่ละ Folder

ชื่อ Folder	วัตถุประสงค์	เจ้าของ	การจำแนกข้อมูล
Back_up_Bkk_Sale	ใช้สำหรับเก็บข้อมูลเก่าของแต่ละแผนก	แผนกIT	Internal Use Only
BAIG_ACC	ใช้ Share files สำหรับแผนกบัญชี	แผนกการเงินและบัญชี	Internal Use Only
Bangkok	ใช้ Share files ในบริษัท	แผนกIT	Internal Use Only
Comsec	ใช้ Share files สำหรับแผนก CEO office	แผนก CEO office	Internal Use Only
DC Admin	ใช้ Share files สำหรับแผนก DC	แผนกDC	Internal Use Only
Document	ใช้สำหรับเก็บไฟล์เอกสารต่างๆ	แผนกDC	Internal Use Only
Finance	ใช้ Share files สำหรับแผนกการเงินและบัญชี	แผนกการเงินและบัญชี	Internal Use Only
Finance Admin	ใช้ Share files สำหรับแผนกการเงินและบัญชี	แผนกการเงินและบัญชี	Internal Use Only

Finance2	ใช้Share files สำหรับแผนกการเงินกับ CEO	CEO	Internal Use Only
Form_Contract	ใช้สำหรับเก็บฟอร์มต่างๆ ของบริษัท	แผนกDC	Internal Use Only
HR	ใช้ Share files สำหรับแผนกHR	แผนกHR	Internal Use Only
IT	ใช้ Share files สำหรับแผนกIT	แผนกIT	Internal Use Only
Power_Bi	ใช้ Share files สำหรับไฟล์ Power Bi	แผนกIT	Internal Use Only
Marketing	ใช้ Share files สำหรับแผนก Marketing	แผนกMarketing	Internal Use Only
Program	ใช้เก็บไฟล์โปรแกรมทั้งหมดที่ต้องใช้งาน	แผนกIT	Internal Use Only
Renovate	ใช้ Share files สำหรับแผนก Renovate	แผนกRenovate	Internal Use Only
CTO	ใช้เก็บไฟล์ของ scan ของ CTO	CTO	Internal Use Only
Sale_co	ใช้เก็บไฟล์ของแผนกขาย	แผนกขาย	Internal Use Only
Scan_ agent	ใช้เก็บไฟล์ของแผนก Agent	แผนกAgent	Internal Use Only
CAO	ใช้เก็บไฟล์ของCAO	CAO	Internal Use Only
Team_list	ใช้ Share files สำหรับแผนกลิสต์	แผนกลิสต์	Internal Use Only
Team_sale	ใช้ Share files สำหรับแผนกขาย	แผนกขาย	Internal Use Only
Transfer_Before_After	ใช้ Share files สำหรับแผนก Renovate และการตลาด	แผนก Marketing	Internal Use Only
Finance_Cloud	ใช้ Share files สำหรับแผนกการเงินและบัญชี	แผนกการเงินและบัญชี	Internal Use Only

ประวัติการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	5 มกราคม 2566	วรวุฒิ เทพหัสดิน ณ อยุธยา
3	2.0	นำ Procedure-023 มารวมเนื้อหา และเพิ่มรายละเอียดจำแนกข้อมูล	1 มีนาคม 2567	ชาญยุทธวัฒนาศักดิกุล

ลงชื่อ_____

(ชาญยุทธ วัฒนาศักดิกุล)

ผู้รับผิดชอบ

วันที่ 1 มีนาคม 2567

ผู้อนุมัติ

ลงชื่อ_____

(ชนินท์ ธนมศิเกษม)

ประธานเจ้าหน้าที่เทคโนโลยีสารสนเทศ

วันที่ 1 มี.ค. 2567

ขั้นตอนการพัฒนาระบบสาระสนเทศ

1. การเริ่มพัฒนาระบบ ผู้จัดการ/ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ส่งการสำรวจความต้องการ (User Requirements Specification) ให้กับแผนกต่างๆ ในไตรมาส 4 ของทุกปี
2. ผู้จัดการ/ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ นำ User Requirements Specification ที่ได้ตอบกลับมา ไปพิจารณาความเป็นไปได้ (Feasibility) กับทีมงาน พร้อมทั้งพิจารณาระบบต่างๆ ที่ใช้อยู่ของบริษัทฯ ว่ามีระบบไหนที่ต้องปรับปรุงให้มีประสิทธิภาพมากยิ่งขึ้นหรือไม่
3. ผู้จัดการ/ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ นำโครงการที่ได้พิจารณาทั้งหมด เสนอผู้บริหารเพื่อขออนุมัติ
   3.1. กรณีโครงการที่ได้รับการอนุมัติ จะประชุมกับผู้เกี่ยวข้องทั้งหมด เพื่อจะจัดทำเป็นโครงการ (Project) โดยระบุหัวข้อการพัฒนา วัตถุประสงค์ และระยะเวลาดำเนินงานลงในแผนพัฒนาระบบ
   3.2. กรณีโครงการที่ไม่ได้รับการอนุมัติ จะส่งคืนให้ผู้ขอเพื่อไปทบทวนหาข้อมูลเพิ่มเติม หรือ รอการอนุมัติอีกครั้งเมื่อเหมาะสม
4. รวบรวมโครงการที่อนุมัติทั้งหมด มาใส่ในแผนงานพัฒนาระบบประจำไตรมาส/ประจำปี นำเสนอประธานกรรมการบริหาร เพื่ออนุมัติเป็นแผนพัฒนาระบบต่อไป
5. เมื่อแผนงานผ่านการอนุมัติแล้ว ผู้จัดการ/ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ดำเนินการพัฒนาระบบ หากต้องสรรหาผู้พัฒนาระบบจากภายนอก จะต้องเป็นไปตามขบวนการจัดซื้อ เช่น ประกวดราคาและขอบเขตที่ต้องการ ผ่านทางฝ่ายจัดซื้อ แล้วนำมาพิจารณาแต่ละรายกับประธานกรรมการบริหาร เพื่อที่จะเลือกผู้พัฒนาที่เหมาะสม
6. เมื่อได้ผู้พัฒนาระบบผ่านการคัดเลือกแล้ว ผู้จัดการ/ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ IT จัดการจ้างผู้พัฒนาระบบ ซึ่งเป็นไปตามเงื่อนไขและกระบวนการจัดซื้อจัดจ้าง โดยทำใบขอซื้อผ่านระบบจัดซื้อ DBC
7. การชำระเงินเป็นไปตามเงื่อนไขที่ได้ตกลงกันไว้ในวัน Kick-off พร้อมทั้งกำหนด Project Timeline หากมีการเปลี่ยนแปลงใดๆ จะดำเนินการให้เสร็จสิ้นการจะดำเนินการพัฒนาต่อไป
8. ผู้จัดการ/ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ IT จะรวบรวมเป็น Project Planning รายงานความคืบหน้าในการประชุมประจำเดือน และ นำเสนอต่อประธานเจ้าหน้าที่บริหาร ทราบถึงความคืบหน้าแต่ล่ะโครงการ
9. ผู้จัดการ/ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ทำการแจ้งความคืบหน้า ปัญหา อุปสรรค กำหนดการแล้วเสร็จที่อาจจะมีการเปลี่ยนแปลงได้ พร้อมทั้งรายละเอียดการพัฒนาระบบกับส่วนงานที่เกี่ยวข้องผ่านระบบ Slack

10. เมื่อระบบถูกพัฒนาเสร็จ จะทำการทดสอบ Functional Testing โดยเจ้าหน้าที่ IT พร้อมกับบันทึกผลการทดสอบ และลงนามผู้ทดสอบ ว่าเป็นไปตาม User Requirements Specification หรือไม่
    10.1. หากไม่ผ่านการทดสอบ มี Bug/Error หรือปัญหาต่างๆ ทางเจ้าหน้าที่ IT จะส่งผลการทดสอบให้ผู้พัฒนาระบบกลับไปแก้ไข แล้วนำมาทดสอบใหม่อีกครั้ง
    10.2. หากการทดสอบระบบไม่มีปัญหาใดๆ เกิดขึ้น พร้อมกับบันทึกผลการทดสอบ และลงนามผู้ทดสอบ
11. กำหนด Test Case/Test Script เพื่อให้บรรลุการทดสอบครบวงจรของระบบ
    11.1. หากไม่ผ่านการทดสอบ มี Bug/Error หรือปัญหาต่างๆ ทางเจ้าหน้าที่ IT จะส่งผลการทดสอบให้ผู้พัฒนาระบบกลับไปแก้ไข แล้วนำมาทดสอบใหม่อีกครั้ง
    11.2. หากการทดสอบระบบไม่มีปัญหาใดๆ เกิดขึ้น พร้อมกับบันทึกผลการทดสอบ และลงนามผู้ทดสอบ
12. ผู้จัดการ/ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ IT นำระบบที่ทำการทดสอบที่เป็นไปตามวัตถุประสงค์ที่กำหนดแล้ว นำมาสรุปเสนอกับเจ้าของระบบ หรือ ผู้ขอใช้ระบบ และผู้ที่เกี่ยวข้องในระบบลงนามรับรอง (Sign Off) เพื่อเสนอต่อประธานกรรมการบริหารลงนามอนุมัติ ในระบบปฏิบัติจริง (Production System)
13. เมื่อประธานกรรมการบริหารอนุมัติ ผู้จัดการ/ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ IT แจ้งกำหนดการกับผู้ที่เกี่ยวข้องถึงวันเริ่มใช้ระบบใน Production System จริงๆ ผ่านระบบ Slack พร้อมกับกำหนดการอบรมการใช้งานกับผู้ใช้งานที่เกี่ยวข้องทั้งหมด
14. ผู้ใช้งานจะต้องเข้าอบรมตามที่แผนก IT ได้เตรียมไว้ พร้อมทั้งลงนามการฝึกอบรม
15. การติดตามหลังการใช้งาน (Post Installation) ในระยะ 3 เดือนหลังจากการขึ้นระบบ หากผู้ใช้งาน เกิดปัญหาจากการใช้งานระบบ จะทำการแจ้งไปยังผู้จัดการ/ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ IT /เจ้าหน้าที่ IT Infrastructure /เจ้าหน้าที่ IT Support ผ่านระบบ Slack ผู้จัดการ/ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ IT จะจัดเก็บข้อมูลการแจ้งปัญหาจากผู้ใช้งาน พิจารณาว่าปัญหาการใช้งานดังกล่าวมีความจำเป็นจะต้องแก้ไขระบบใหม่หรือไม่
    15.1. หากเป็นปัญหาใหญ่ และจำเป็นต้องแก้ไขระบบใหม่ผู้จัดการ/ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ IT จะนำเสนอประธานกรรมการบริหารเพื่อพิจารณาอนุมัติการพัฒนาระบบอีกครั้ง
    15.2. หากเป็นปัญหาเพียงเล็กน้อย ก็พิจารณาเป็นการปรับปรุงให้ระบบดีขึ้น

16. ผู้จัดการ/ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ IT สรุปผลการพัฒนาระบบเปรียบเทียบ Project Planning แล้วนำเสนอแผนงาน Project ประจำไตรมาส และ Project Planning กับประธานกรรมการบริหารทุกสิ้นเดือน เพื่อรายงานความคืบหน้าของแผนงานที่อยู่ระหว่างการดำเนินงาน และรายงานผลหัวข้อที่ดำเนินการเรียบร้อยแล้ว

ประวัติ

ประวัติการปรับปรุงเอกสาร				
ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	15 มีนาคม 2565	น.ส.ณัฐธิดา สิงห์คง
2	2.0	แก้ไขระบบจัดซื้อ และปรับปรุงการอนุมัติ	5 มกราคม 2566	น.ส.กร ธรรมาพาณิชย์

ลงชื่อ กร ธ

(กร ธรรมาพาณิชย์)

ผู้รับผิดชอบ

วันที่ 5/01/66

ผู้อนุมัติ

ลงชื่อ ธนิดร ธนวงศ์เกษม

(ธนิดร ธนวงศ์เกษม)

ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ

วันที่ 5/01/66

ขั้นตอนการเข้าใช้สิทธิ์ระบบงานต่างๆ

ขั้นตอนการจัดทำทะเบียนคุมสิทธิ์

1. ผู้จัดการ IT จัดทำทะเบียนคุมสิทธิ์การเข้าถึงระบบงาน ของส่วนงานต่างๆ โดยแยกตามตำแหน่งงาน
2. นำส่งให้ผู้บริหารแต่ละส่วนงาน ตรวจสอบ และลงนามรับทราบ
3. รวบรวมข้อมูลที่ได้มีการปรับปรุงเรียบร้อยแล้ว นำเสนอประธานกรรมการบริหารพิจารณาอนุมัติ
4. หลังจากผ่านการอนุมัติแล้วเจ้าหน้าที่ IT ผู้ดูแลระบบ จะนำทะเบียนคุมสิทธิ์การเข้าถึงระบบงานไปใช้อ้างอิงการกำหนดสิทธิ์เพื่อเป็นมาตรฐานของสิทธิ์แต่ระบบต่อไป

ขั้นตอนการสอบทานสิทธิ์

1. กำหนดการสอบทานสิทธิ์ เริ่มตั้งแต่วันที่ 1 กุมภาพันธ์ ถึง 30 มิถุนายน ของทุกปี
2. เจ้าหน้าที่ IT ผู้ดูแลระบบ จะทำข้อมูลของสิทธิ์ในการใช้งานระบบที่ได้กำหนดไว้ ให้กับผู้บริหาร
3. รวบรวมข้อมูลที่ได้ทั้งหมด แล้วแยกเป็นแผนก ส่งไปยังผู้บริหารแต่ละฝ่าย เพื่อตรวจสอบ แล้วลงนามเมื่อตรวจสอบเสร็จสิ้น
4. ผลการตรวจสอบที่ได้คืนมา
   4.1. หากมีการแก้ไขสิทธิ์ ในกรณีเอาออก เจ้าหน้าที่ IT ผู้ดูแลระบบ จะดำเนินแก้ไขปรับปรุงให้ตามที่ระบุไว้ แล้วตอบกลับยังผู้บริหารส่วนนั้น
   4.2. หากมีการแก้ไขสิทธิ์ ในกรณีขอเพิ่ม ก็ให้แจ้งผู้บริหารให้ปฏิบัติตามขั้นตอนการขอใช้สิทธิ์เพิ่ม
5. รวบรวมข้อมูลที่ได้ปรับปรุงแก้ไขแล้ว นำเสนอต่อประธานกรรมการบริหารลงนามรับทราบ
6. ในกรณีที่มีการพิจารณาจากผู้บริหารให้เป็นระบบสำคัญ หรือ ขออนุญาตให้ตรวจสอบความเคลื่อนไหวอย่างใกล้ชิด เป็นลายลักษณ์อักษร จะมีการตรวจสอบ Monitoring Log ให้
   6.1. หากเจอว่ามีสิ่งผิดปกติเกิดขึ้น จะรายงานต่อประธานกรรมการบริหารรับทราบทันที
   6.2. หากไม่เจอว่ามีสิ่งปกติเกิดขึ้น ให้ลงนาม แล้วส่งผลรายงานประจำเดือนต่อผู้บริหาร IT รับทราบ

ขั้นตอนการขอใช้สิทธิ์

1. เมื่อพนักงานใหม่เข้ามาทำงาน ส่วนงานทรัพยากรบุคคลจะเป็นผู้แจ้งรายชื่อพนักงานเข้าใหม่ พร้อมทำการขอรับสิทธิ์การใช้งาน ระบบพื้นฐาน ได้แก่ E-MAIL ผ่านการอนุมัติในระบบ Kintone
2. เจ้าหน้าที่ IT จะทำการสร้าง E-MAILให้แก่พนักงานใหม่ แล้วพิมพ์ Username และ Password ของE-MAIL ใส่ซองจดหมาย ปิดผนึก ส่งให้แก่ พนักงานใหม่ในวันแรกของการทำงาน พร้อมเซ็นรับเอกสาร

3. ส่วนงานต้นสังกัดที่ต้องการขอรับสิทธิ์ให้แก่พนักงานใหม่ จะต้องจัดทำแบบคำร้องขอรับสิทธิ์การใช้ระบบงาน ผ่านระบบ Kintone โดยระบุข้อมูลของพนักงาน ระบบงานที่ต้องการใช้ และ Function ที่ต้องการเข้าใช้ รวมถึงการอนุมัติเรื่องต่างๆ ในระบบงานนั้นๆ โดยผู้จัดการส่วนงานต้นสังกัดผ่านระบบ Kintone
7. เมื่อแบบคำร้องขอรับสิทธิ์การใช้ระบบงานผ่านการอนุมัติแล้ว IT Developer /IT Infrastructure จะดำเนินจัดการตามระบบงานที่มีสิทธิ์ โดยการทำการตรวจสอบคำร้องขอรับสิทธิ์ เปรียบเทียบกับทะเบียนคุมสิทธิ์การเข้าถึงระบบงานของตำแหน่งงานนั้นๆ ว่าเป็นไปตามที่กำหนดไว้หรือไม่ หากตรวจสอบแล้วไม่เป็นไปตามสิทธิ์ที่กำหนด IT Developer /IT Infrastructure ทำการแจ้งไปยังผู้ร้องขอรับสิทธิ์ผ่านระบบ Kintone ให้ทำการตรวจสอบรายละเอียดในแบบคำร้องอีกครั้ง
8. เมื่อทุกอย่างถูกต้อง IT Developer /IT Infrastructure ผู้ดูแลระบบ ดำเนินการสร้างรหัสผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของแต่ละระบบงานที่มีการขอรับสิทธิ์ โดยผู้จัดการส่วน IT อนุมัติ ก่อนส่งไปทาง E-MAIL ของผู้ใช้งาน
9. ผู้ร้องขอทำการบันทึกรับโดยกดปุ่ม Complete เพื่อยืนยันการรับรหัสผู้ใช้งาน (Username) และรหัสผ่าน (Password) ผ่านระบบ Kintone

ขั้นตอนการเลิกใช้สิทธิ์

1. ก่อนพนักงานพ้นสภาพการเป็นพนักงานของบริษัทฯ เจ้าหน้าที่ส่วนงานทรัพยากรบุคคลแจ้งผู้จัดการส่วนงาน IT ผ่านระบบ Slack (ใช้อ้างอิงในการลบรหัสผู้ใช้งาน (Username) ของพนักงานคนนั้นออกจากระบบงานต่างๆ)
2. IT Developer /IT Infrastructure ผู้ดูแลระบบ ทำการตรวจสอบวันที่พ้นสภาพการเป็นพนักงานกับวันที่แจ้งขอระงับสิทธิ์การใช้งาน นำมาใช้ตั้งกำหนดการณ์ทำงานของส่วนงาน IT ในการระงับสิทธิ์ของพนักงานออกจากระบบ
   2.1. กรณีแจ้งย้อนหลัง
      2.1.1. IT Developer /IT Infrastructure ผู้ดูแลระบบ ดำเนินการลบสิทธิ์ผู้ใช้งานออกจากระบบต่างๆ
      2.1.2. เสนอหลักฐานการแจ้งขอระงับสิทธิ์จากเจ้าหน้าที่ส่วนงานทรัพยากรบุคคล และผู้จัดการส่วนงานของพนักงานพ้นสภาพ
      2.1.3. เจ้าหน้าที่พิจารณาอนุมัติตรวจสอบการลักลอบเข้าใช้ระบบหลังพ้นสภาพการเป็นพนักงาน

2.1.4. เมื่ออนุมัติให้ตรวจสอบแล้ว IT Developer /IT Infrastructure ผู้ดูแลระบบ ดำเนินการตรวจสอบโดยจะใช้ระยะเวลาดำเนินการภายใน 30 วันทำการ

2.1.5. เมื่อตรวจสอบแล้วจะรวบรวมข้อมูลการเข้าใช้ระบบของพนักงานตั้งแต่วันที่พ้นสภาพการเป็นพนักงาน จนกระทั่งวันที่ลบสิทธิ์ออกจากระบบ นำเสนอผู้จัดการส่วนงานของพนักงานพ้นสภาพรับทราบ

2.2. กรณีแจ้งปกติ

2.2.1. IT Developer /IT Infrastructure ผู้ดูแลระบบ ดำเนินการลบรหัสผู้ใช้งาน (Username) เรียบร้อยแล้ว

2.2.2. ทำการบันทึกวันที่ลบ และสถานะการลบลงในแบบคำร้องขอรับสิทธิ์การใช้ระบบงานผ่านระบบ Kintone

3. ผู้จัดการส่วนงาน IT จะทำการตรวจสอบสถานะผู้ใช้งาน (Username) ปัจจุบัน ว่าได้ลบรหัสผู้ใช้งาน (Username) ของพนักงานที่พ้นสภาพการเป็นพนักงานครบถ้วนแล้วหรือไม่ ตามรอบการตรวจสอบของแต่ละระบบงาน โดยเปรียบเทียบรหัสผู้ใช้งาน (Username) ปัจจุบันในระบบต่าง ๆ กับรายชื่อพนักงานปัจจุบันของบริษัทฯ ซึ่งได้รับจากส่วนงานทรัพยากรบุคคล แล้วบันทึกผลการตรวจสอบลงในเอกสารการตรวจสอบสถานะผู้ใช้งาน และแจ้งผ่านระบบ Slack ว่าเรียบร้อยแล้ว

ผู้อนุมัติ

ลงชื่อ ชนิดา ชนองศ์เกษม

(ชนิดา ชนองศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 10 มี.ค. 65

ลงชื่อ นัฐริกา สิงห์ทอง

(น.ส. นัฐริกา สิงห์ทอง)

ผู้รับผิดชอบ

วันที่ 10 มี.ค 65

ขั้นตอนการป้องกันไวรัสคอมพิวเตอร์/มัลแวร์

วัตถุประสงค์ เพื่อป้องกันความเสี่ยงที่เกิดจากไวรัสคอมพิวเตอร์/มัลแวร์ หรือสิ่งคุกคามจากสิ่งไม่พึงประสงค์ทั้งภายใน และภายนอกบริษัท รวมทั้งปกป้องรักษาระบบคอมพิวเตอร์ให้ปลอดภัยสูงสุด ดังนี้

ติดตั้งและตรวจสอบเครื่องมือในการกำจัดไวรัสคอมพิวเตอร์/มัลแวร์

1. ติดตั้ง และตรวจสอบ ระบบป้องกันไวรัสคอมพิวเตอร์/มัลแวร์สำหรับเครื่องแม่ข่าย รวมทั้งให้มีการอัปเดตเวอร์ชั่นล่าสุด จากเจ้าของผลิตภัณฑ์นั้นๆ
2. ติดตั้งและตรวจสอบ ระบบป้องกันไวรัสคอมพิวเตอร์/มัลแวร์ให้กับคอมพิวเตอร์ทุกเครื่องขององค์กร รวมทั้งต้องจัดให้มีการอัปเดตเวอร์ชั่นล่าสุด จากเจ้าของผลิตภัณฑ์นั้นๆ
3. กำหนดหน้าที่ และความรับผิดชอบในการตรวจจับและทำลายไวรัสคอมพิวเตอร์/มัลแวร์ โดยเฉพาะฝ่ายเทคโนโลยีสารสนเทศ มีหน้าที่รับผิดชอบในการตรวจจับ และทำลายไวรัสคอมพิวเตอร์/มัลแวร์บนเครื่องคอมพิวเตอร์ส่วนบุคคล ไม่ให้แพร่กระจายทำความเสียหายกับข้อมูลขององค์กร
4. กำหนดให้ IT Infrastructure มีหน้าที่รับผิดชอบในการตรวจจับและทำลายไวรัสคอมพิวเตอร์/มัลแวร์อย่างสม่ำเสมอบน Servers และอุปกรณ์เครือข่าย เพื่อป้องกันความเสียหายกับข้อมูลขององค์กร
5. กำหนดให้ฝ่ายเทคโนโลยีสารสนเทศ ต้องมีการแจ้งข่าวเกี่ยวกับไวรัสคอมพิวเตอร์/มัลแวร์ หากมีการระบาดของไวรัสคอมพิวเตอร์/มัลแวร์ตัวใหม่ทันที
6. หากมีการระบาดใหญ่ในองค์กร ให้มีมาตรการขั้นเด็ดขาด โดยการประกาศเป็นภาวะฉุกเฉิน ให้นำคอมพิวเตอร์ทุกเครื่องมาตรวจสอบ หรือ ฆ่าไวรัสคอมพิวเตอร์/มัลแวร์ทุกเครื่อง ก่อนนำไปใช้งานหรือต่อเข้าเครือข่ายของบริษัท
7. กำหนดให้ IT Infrastructure ทำรายงานสถิติการติดไวรัสคอมพิวเตอร์/ มัลแวร์ของเครื่องคอมพิวเตอร์ส่วนบุคคลที่แสดงอยู่บนเซิร์ฟเวอร์แม่ข่ายสำหรับป้องกันไวรัสคอมพิวเตอร์/ มัลแวร์ขององค์กร อย่างน้อยเดือนละ 1 ครั้งต่อ ผู้บริหารฝ่ายคอมพิวเตอร์

ผู้อนุมัติ

ลงชื่อ ชนิดา ชนวงศ์เกษม

(ชนิดา ชนวงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 10 มี.ค. 65

ลงชื่อ วรวุฒิ เทพทัศดิน ณ อยุธยา

(วรวุฒิ เทพทัศดิน ณ อยุธยา)

ผู้รับผิดชอบ

วันที่ 10 มี.ค 65

ขั้นตอนการทำลายสื่อบันทึกข้อมูลอิเล็กทรอนิกส์

วัตถุประสงค์ เพื่อป้องกันการรั่วไหลของข้อมูลจากอุปกรณ์อิเล็กทรอนิกส์ หรือ จากการบันทึกข้อมูลอิเล็กทรอนิกส์ ทั้งที่ตั้งใจ หรือไม่ตั้งใจ ที่จะมีผลทำให้เกิดความเสียหายต่อบริษัทได้ ดังนี้

1. เจ้าหน้าที่ IT จะทำหน้าที่ในตรวจสอบอุปกรณ์คอมพิวเตอร์ คอมพิวเตอร์ หรืออุปกรณ์ต่อพ่วง โดยการจำแนกอุปกรณ์ คอมพิวเตอร์ หรืออุปกรณ์ต่อพ่วง ก่อนที่จะทำการขาย หรือ บริจาค หรือ ทำลายทิ้งดังนี้

ประเภทสื่อบันทึก	ลักษณะการใช้งาน		
	นำกลับมาใช้ใหม่	ข้อมูลที่เป็นความลับและนำกลับใช้ใหม่	ไม่นำกลับมาใช้ใหม่
CD/DVD	-	-	ทุบ หัก หรือทำลายให้เสียหาย หรือ เผา
Harddisk ในคอมพิวเตอร์	Format	Format แบบ Zero-filling	ทุบ หรือทำลายให้เสียหาย
Flash drive/Thumb drive/Handy drive	Format	Format 3 ครั้ง	ทุบ หรือทำลายให้เสียหาย หรือ เผา
เทปบันทึกข้อมูล	Format	Format แบบ Zero-filling	ทุบ หรือทำลายให้เสียหาย หรือ เผา
สื่อบันทึกที่มีระบบปฏิบัติการ เช่น Mobile Phone, Tablet	ใช้คำสั่ง Factory Data Reset	-ระบบ IOS ใช้การ Factory Data Reset -ระบบปฏิบัติการอื่นๆ ใช้ Reset phone	ทุบ หรือทำลายให้เสียหาย หรือ เผา
สื่อบันทึกข้อมูลแบบถอดแยกได้	Format	Format แบบ Zero-filling	ทุบ หรือทำลายให้เสียหาย หรือ เผา
กระดาษ	ขีดข้อความทิ้งก่อนนำมาใช้งาน	ห้ามนำกลับมาใช้	ใช้เครื่องทำลายเอกสารก่อนทิ้ง

2. เจ้าหน้าที IT จะทำการบันทึกผลการทำลายอุปกรณ์ นำเสนอต่อผู้บริหารฝ่ายคอมพิวเตอร์ลงนามรับทราบ

ผู้อนุมัติ

ลงชื่อ ธนิกร ธนวงศ์เกษม

(ธนิกร ธนวงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 10 มี.ค. 2565

ลงชื่อ วรกุล เทพทัสสิน ณ อยุธยา

(วรกุล เทพทัสสิน ณ อยุธยา)

ผู้รับผิดชอบ

วันที่ 10 มี.ค 65

ขั้นตอนการสำรองข้อมูล OS

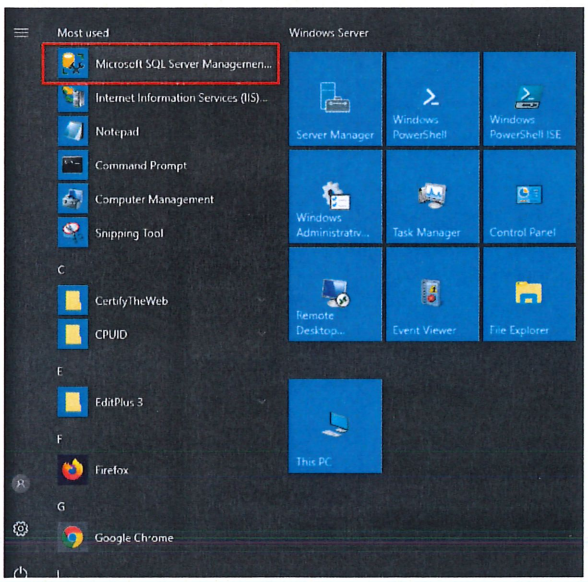
วัตถุประสงค์ เพื่อให้การบริการระบบสารสนเทศเป็นไปอย่างต่อเนื่อง จึงกำหนดให้ฝ่ายสารสนเทศต้องดำเนินการสำรองข้อมูลระบบ OS ไว้ทั้งหมด โดยให้ทำการสำรองไว้ในสื่อบันทึกที่สามารถนำขึ้นใช้งานได้ในกรณีที่ระบบปฏิบัติการหลักล้มเหลว

ข้อกำหนด กำหนดให้มีการสำรองข้อมูลของระบบงาน OS โดยมีการตั้งเวลาการสำรองข้อมูล ดังนี้

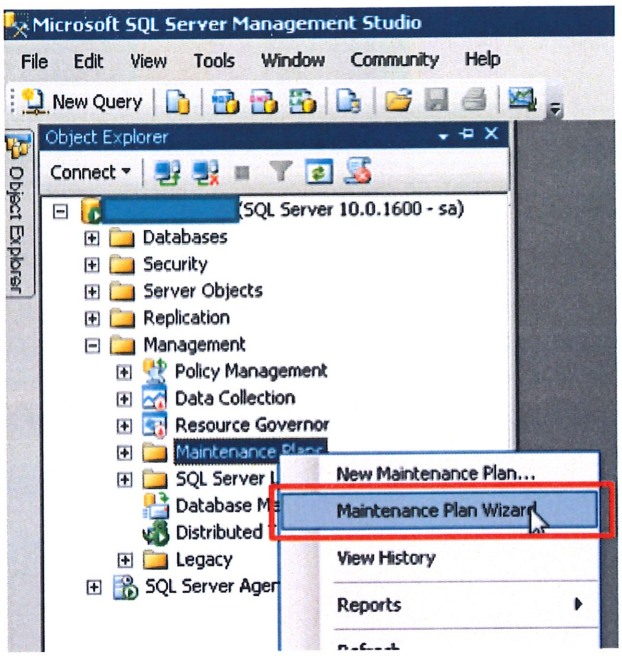
- Daily: มีการสำรองข้อมูลแบบ Incremental ทุกๆวัน เวลา 02.00น. และไฟล์จะถูกเก็บไว้เป็นระยะเวลา 3เดือนแบบ Rotation
- Weekly: มีการสำรองข้อมูลทั้งหมดวันอาทิตย์ เวลา 02.00น. และไฟล์จะถูกเก็บไว้เป็นเวลา 3 เดือนแบบ Rotation

ขั้นตอนการสำรองข้อมูล

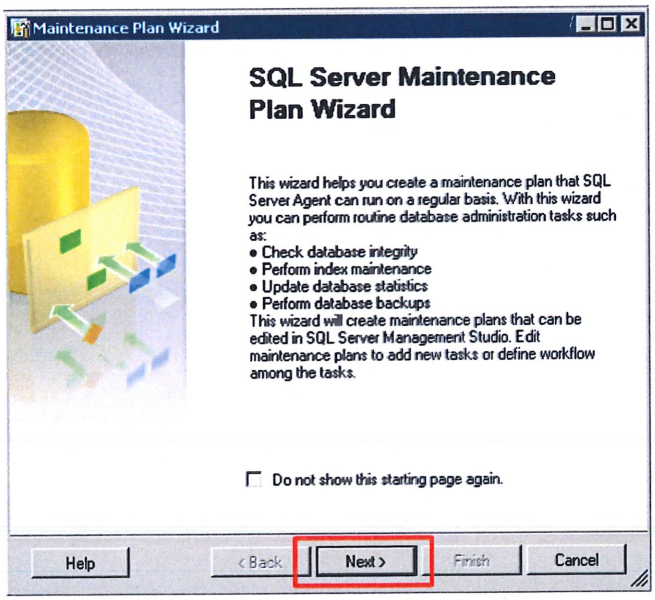
1. เข้าที่ Start > Programs > Microsoft SQL Server Management



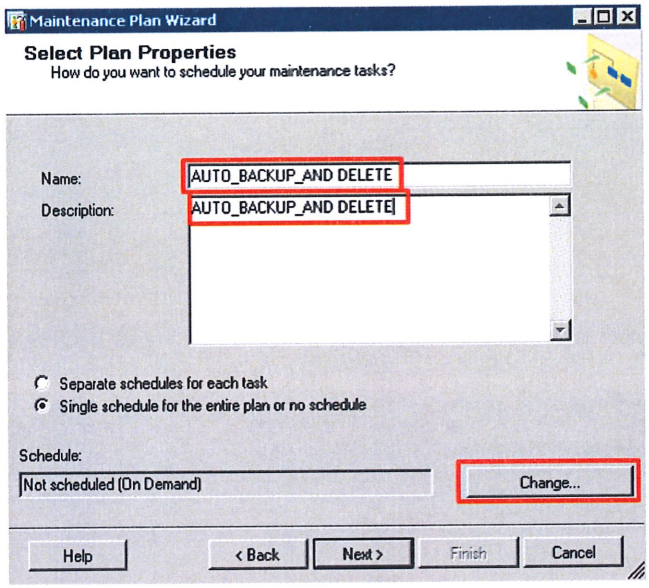
2. เลือกเมนู Management > คลิกขวาที่ Maintenance Plans> เลือก Maintenance Plan Wizard



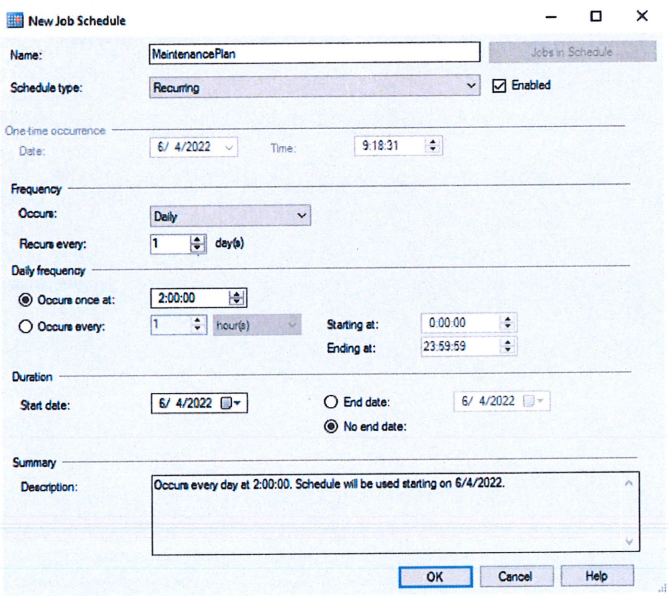
3. คลิก Next



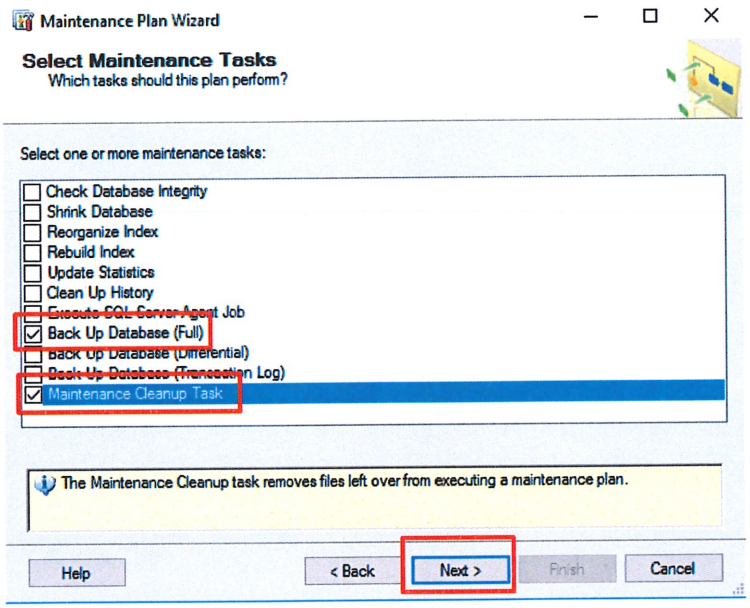
4. ใส่ชื่อของ AUTO Backup ใส่ Descriptionของ AUTO Backup จากนั้นกด Change



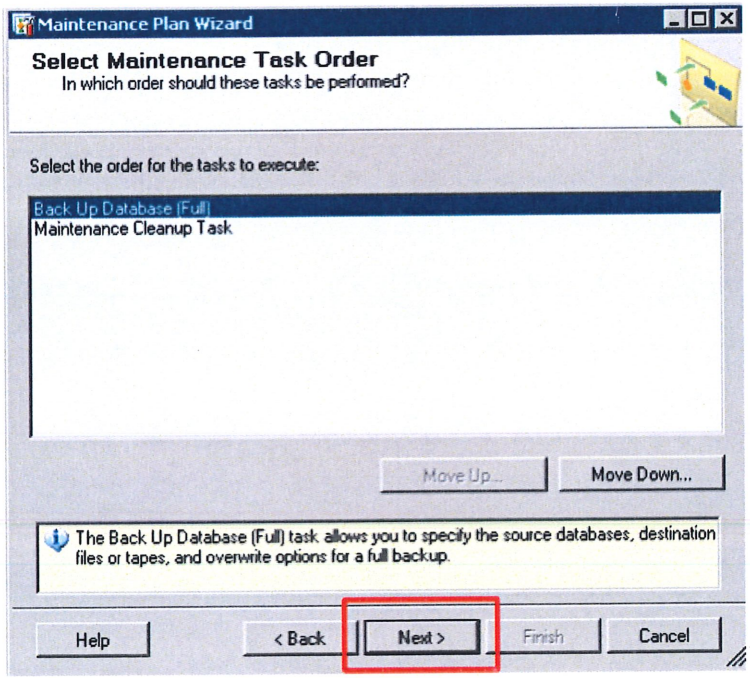
5. กำหนดเวลาที่ต้องการ Backup database เสร็จแล้วกด OK



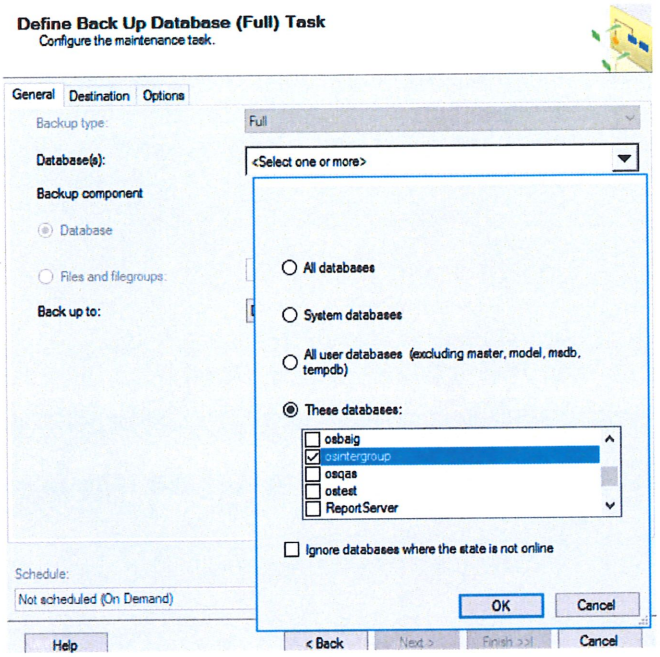
6. เลือก Back Up Database (Full) และ Maintenance Cleanup Task จากนั้นกด Next



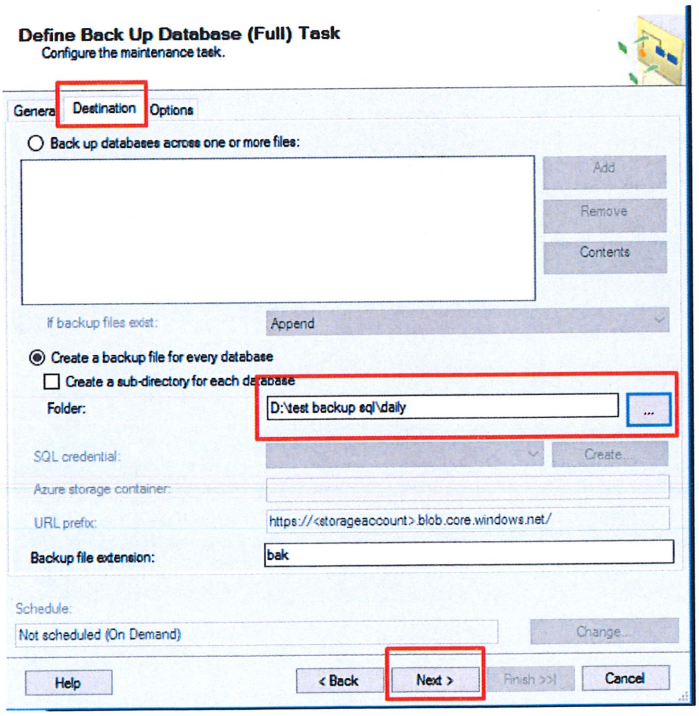
7. กด Next อีกครั้ง



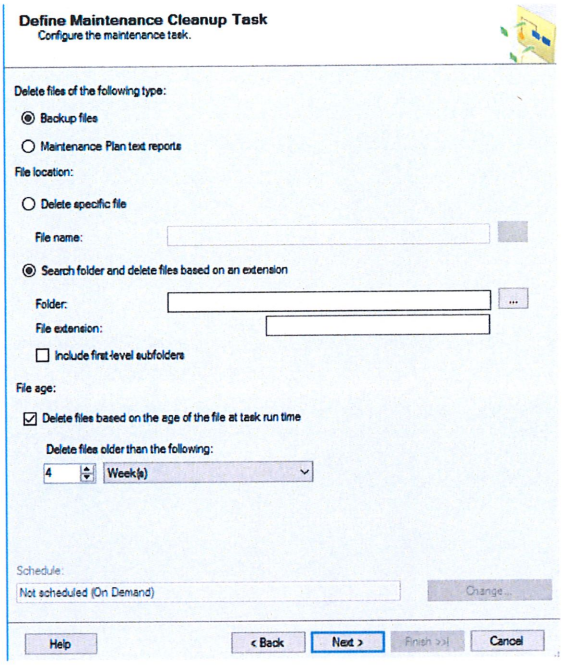
8. เลือก Database ที่ต้องการ Backupจากนั้นกด OK



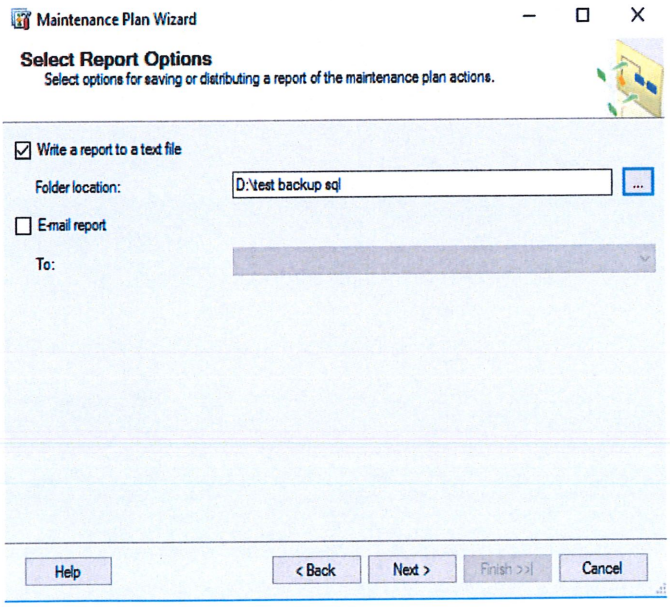
9. เลือกไปที่ tab Destination เลือก Folder ที่จะจัดเก็บ Back UP กด Next



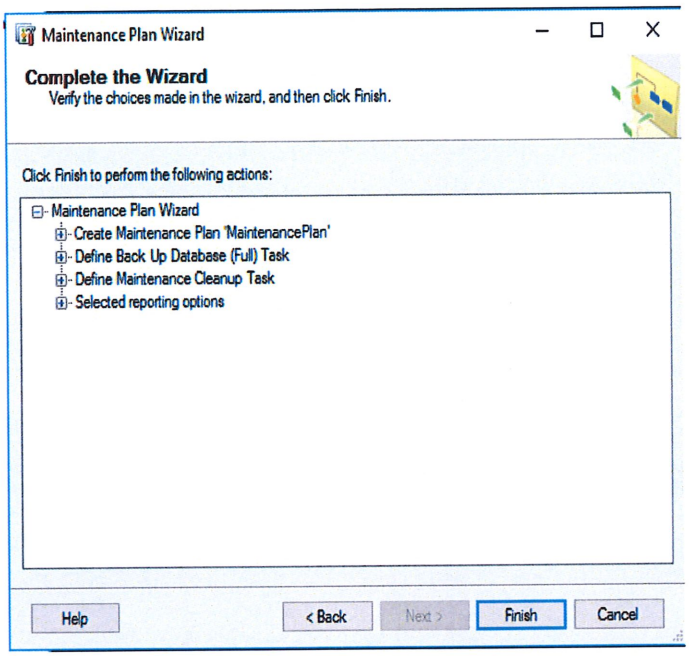
10. เลือกเงื่อนไขในการลบไฟล์ Backup กด Next



11. เลือกโฟล์เดอร์ที่จะจัดเก็บ report การทำ backup กด Next

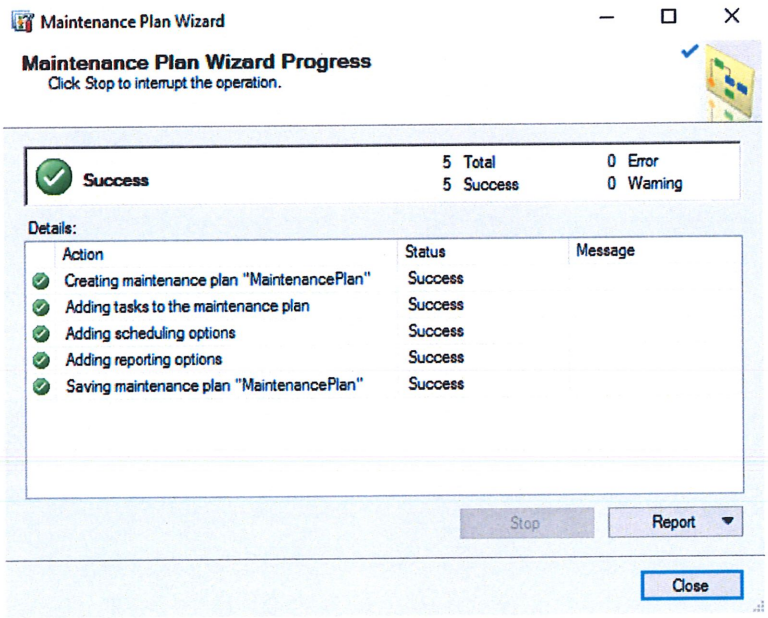


12. กด Finish

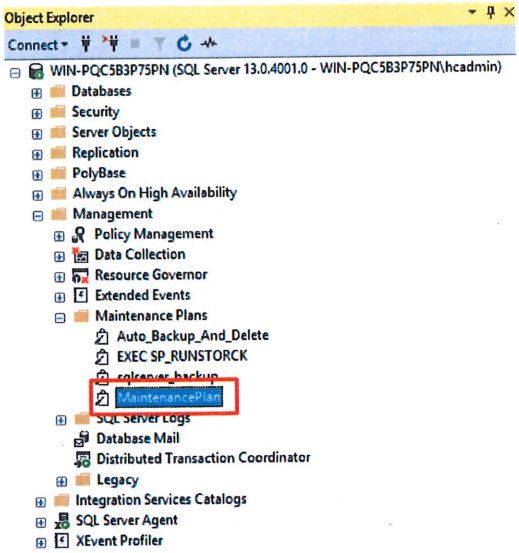


13. กด Close

14. เข้าไปดูว่า Job Schedule ว่าทำงานหรือไม่ใน Maintenance Plan Wizard



15. Plans ที่ถูกสร้างจะมาแสดงที่ tab ด้านข้าง



ขั้นตอนการกู้คืนข้อมูลระบบ OS

Database: OSintergroup

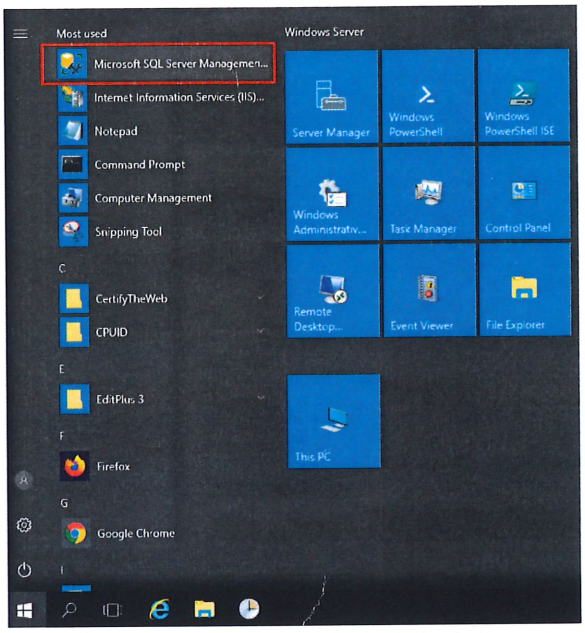
ขั้นตอนการปฏิบัติ

1. ตรวจสอบรายการ Backup ที่ทำไว้พร้อมทั้งทำการเลือกไฟล์ที่จะใช้ Recovery file backup เก็บไว้ที่ : 203.150.20.210
2. ติดตั้งระบบ MS SQLServer2016 ที่เครื่องคอมพิวเตอร์สำรอง
3. ปรับแต่งค่าการใช้งาน (Configuration) ระบบเครือข่ายประจำเครื่อง (Network)
4. ทำการกู้คืนฐานข้อมูล (Database Backup) ขั้นตอนอยู่ในไฟล์ “คู่มือ Restore SQL database OS.xlsx
5. แก้ไข connection ที่ระบบOS
   5.1. ที่ไฟล์ชื่อว่า Web.config ตามข้อมูลข้างล่าง

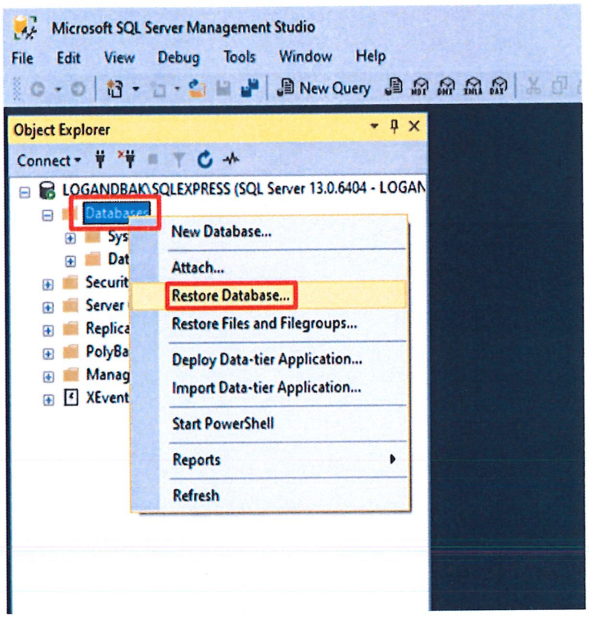
```
<!--localhost-->

<add name="BOSDbContext" connectionString="data source=LOGANDBAK;initial
catalog=test;persist security info=True;user
id=sa;password=1234;multipleactiveresultsets=True;application name=EntityFramework"
providerName="System.Data.SqlClient" />
```

   5.2. ทำการPublish ดูที่ไฟล์ “คู่มือ การตั้งค่าIISและPublish OS.xlsx”
6. ทดสอบระบบ
7. ทำการ Restore

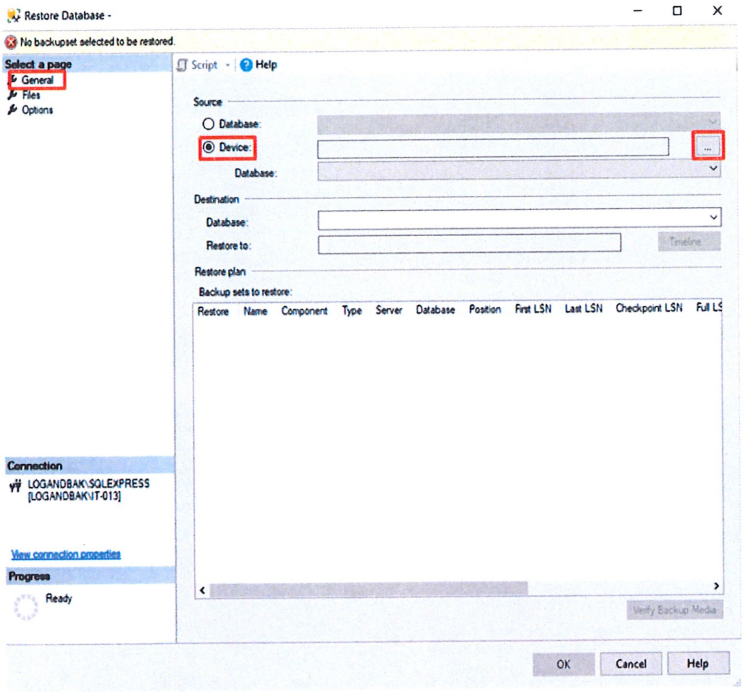
8. เข้าที่ Start > Programs > Microsoft SQL Server Management



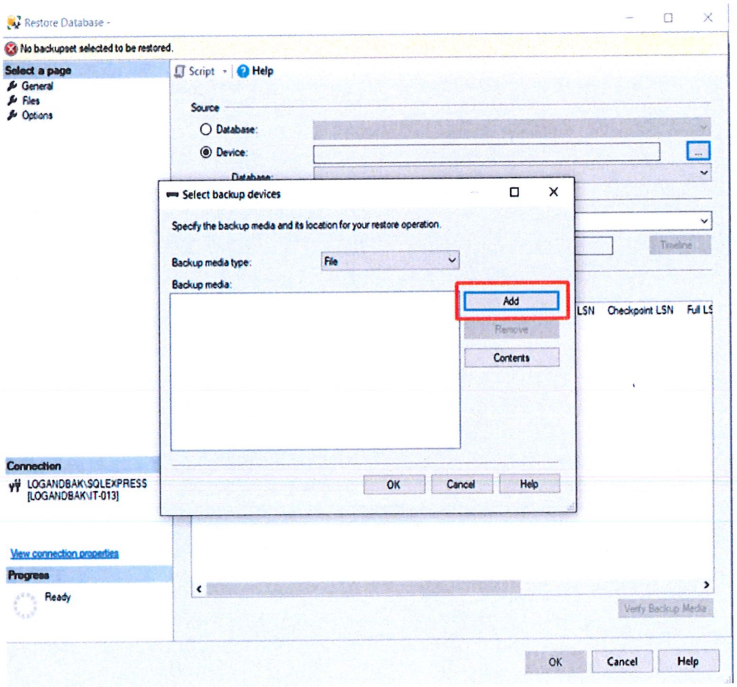
9. คลิกขวาที่ Database เลือก Restore Database



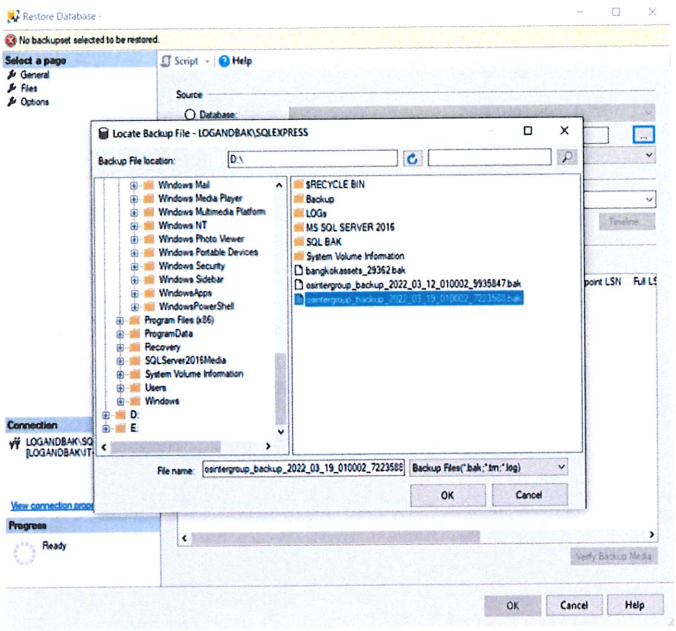
10. ที่หัวข้อ General => เลือก Device คลิกที่ปุ่มสามจุดด้านหลัง เพื่อเลือกไฟล์ที่ต้องการrestore



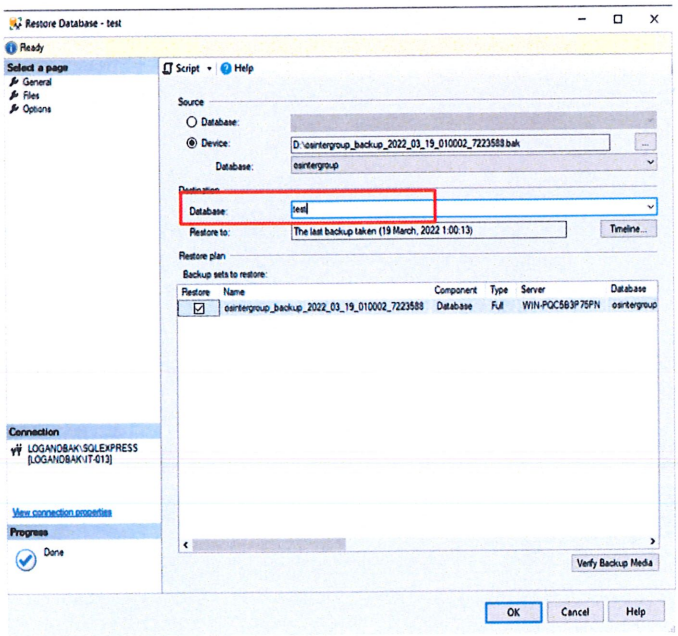
11. กดปุ่ม Add เพื่อเลือกไฟล์ที่ต้องการ



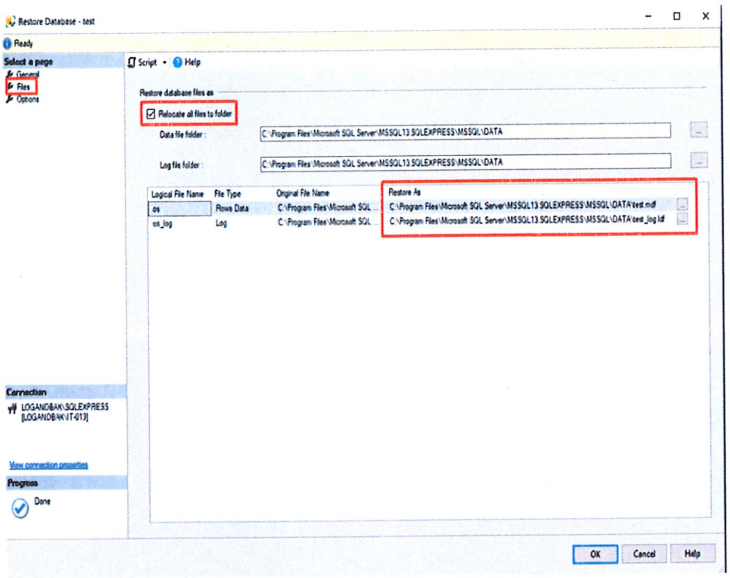
12. เลือกไฟล์ที่ต้องการ restore จากนั้นกดปุ่ม OK



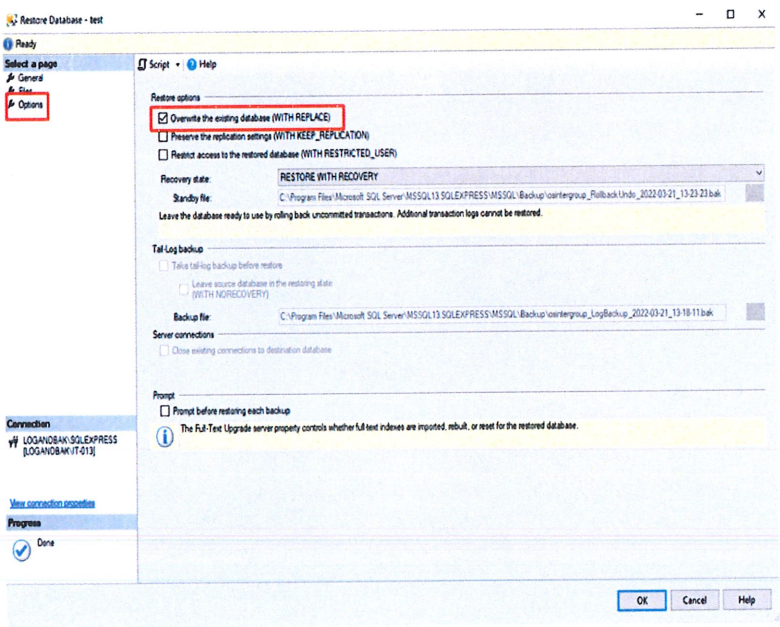
13. ที่ช่อง Database ให้ใส่ชื่อ database ปลายทางที่ต้องการ restore ออกมา



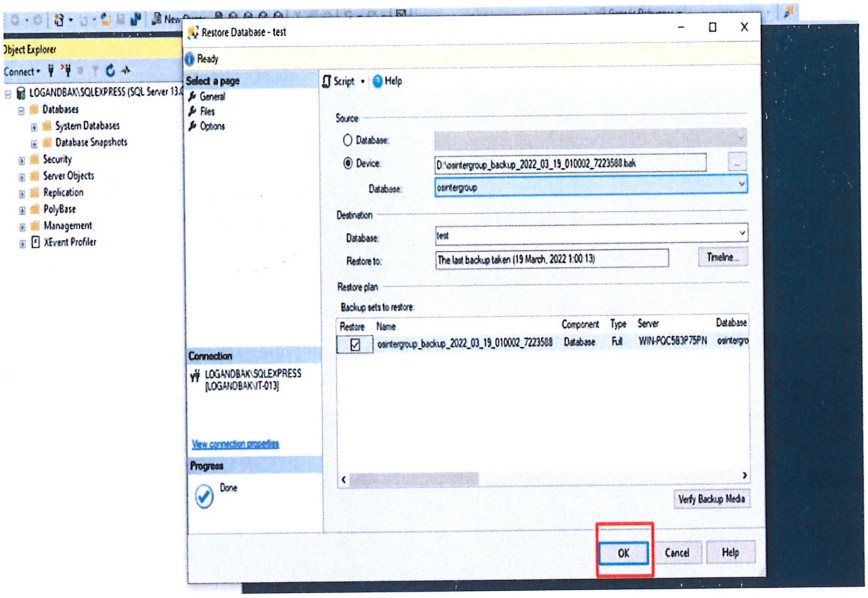
14. จากนั้นไปที่หัวข้อ Files => คลิกถูกที่หัวข้อ Relocate all files to folder แล้วมาตรวจสอบตรง Restore As ว่าไปปลายทางที่ถูกระบุไว้ถูกต้องแล้ว



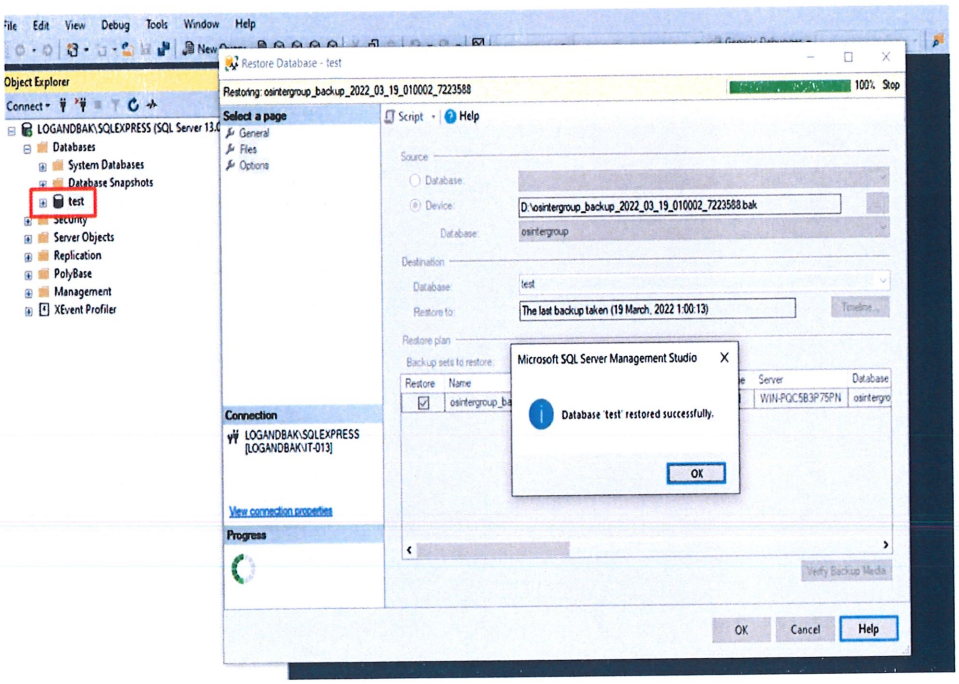
15. จากนั้นไปที่หัวข้อ Option => คลิกถูกที่หัวข้อ Overwrite the existing database (WITH REPLASE)



16. กดปุ่ม OK เพื่อดำเนินการ



17. เสร็จสิ้น



ตัวอย่างผลการทดสอบการสำรองข้อมูลและการกู้คืน OS

IT-Procedure-034
(OS Testing).docx

ประวัติการการปรับปรุงเอกสาร				
ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	15 มีนาคม 2565	ณัฐธิดา สิงค์คง
2	2.0	ปรับปรุงเอกสารให้สอดคล้องกับ IT-Procedure-050	15 พฤศจิกายน 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา

ผู้อนุมัติ

ลงชื่อ วรวุฒิ เทพหัสดิน ณ

(วรวุฒิ เทพหัสดิน ณ อยุธยา)

ผู้รับผิดชอบ

วันที่ 15/11/65

ลงชื่อ

( )

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 15/11/65

ขั้นตอนการติดตั้งซอฟต์แวร์คอมพิวเตอร์

วัตถุประสงค์ เพื่อให้เป็นไปตามมาตรฐานในการติดตั้ง Software/Application ที่เป็นหลัก ให้ทำงานได้อย่างมีประสิทธิภาพเหมาะสมกับการใช้งาน ดังนี้

1. การติดตั้งระบบ OS
   1.1. ให้เปิด browser และ ไปที่ http://www.osintergroup.com
   1.2. กรอก user และ Password ที่ได้รับจากทางแผนกสารสนเทศ
2. การติดตั้งระบบ ERP
   2.1. ให้เปิด browser และ ไปที่ https://businesscentral.dynamics.com/f36b0000-fc67-467e-834d-9aa70841856b/production?company=BAIG-MASTERDATA
   2.2. กรอก user และ Password ที่ได้รับจากทางแผนกสารสนเทศ
3. การติดตั้งระบบ Kintone
   3.1. ให้เปิด browser และ ไปที่ https://bai.cybozu.com
   3.2. กรอก user และ Password ที่ได้รับจากทางแผนกสารสนเทศ
4. การติดตั้งระบบ Trello
   4.1. ให้เปิด browser และ ไปที่ https://www.trello.com
   4.2. กรอก user และ Password ที่ได้รับจากทางแผนกสารสนเทศ
5. การติดตั้งระบบ kwanjai
   5.1. ให้เปิด browser และ ไปที่ https://kwanjai.builk.com/login
   5.2. กรอก user และ Password ที่ได้รับจากทางแผนกสารสนเทศ
6. การติดตั้งระบบ Fastinspec
   6.1. ให้เปิด browser และ ไปที่ https://api.fastinspect.co/backend/public/login/developer
   6.2. กรอก user และ Password ที่ได้รับจากทางแผนกสารสนเทศ
7. การติดตั้งระบบ survey
   7.1. ให้เปิด browser และ ไปที่ sv.bangkokassets.com
   7.2. กรอก user และ Password ที่ได้รับจากทางแผนกสารสนเทศ
8. การติดตั้งระบบ survey บ้านมือหนึ่ง
   8.1. ให้เปิด browser และ ไปที่ sv1.bangkokassets.com

8.2. กรอก user และ Password ที่ได้รับจากทางแผนกสารสนเทศ

9. การติดตั้งระบบ slack

9.1. ให้เปิด browser และ ไปที่bangkokasset.slack.com

9.2. กรอก user และ Password ที่ได้รับจากทางแผนกสารสนเทศ

10. การติดตั้งระบบเบิกกุญแจ

10.1. ให้เปิด browser และ ไปที่ baigkey.com

10.2. กรอก user และ Password ที่ได้รับจากทางแผนกสารสนเทศ

11. การติดตั้งระบบ เก็บTicket

11.1. แจ้งปัญหา IT ให้เปิด browser และ ไปที่ IT.baigkey.com

11.2. กรอก user และ Password ที่ได้รับจากทางแผนกสารสนเทศ

12. การติดตั้งระบบ CRM

12.1. ให้เปิด browser และ ไปที่ crm.zoho.com

12.2. กรอก user และ Password ที่ได้รับจากทางแผนกสารสนเทศ

13. การติดตั้งระบบ HumanOS

13.1. ให้เปิด browser และ ไปที่ https://backend.humanos.biz/

13.2. กรอก user และ Password ที่ได้รับจากทางแผนกบุคคล

14. การติดตั้งระบบ E-Memo (Z.com)

14.1. ให้เปิด browser และ ไปที่ https://bai.zocomsign.com

14.2. กรอก user และ Password ที่ได้รับจากทางแผนกสารสนเทศ

15. การติดตั้ง Microsoft office 365 หรือ Microsoft office 2021

15.1. ให้เปิด browser และไปที่ www.office.com

15.2. กรอก user และ password ที่ได้รับจากทางแผนกสารสนเทศ สังเกตมุมบนขวาจะเห็นคำว่า Install Office หรือ ติดตั้ง office

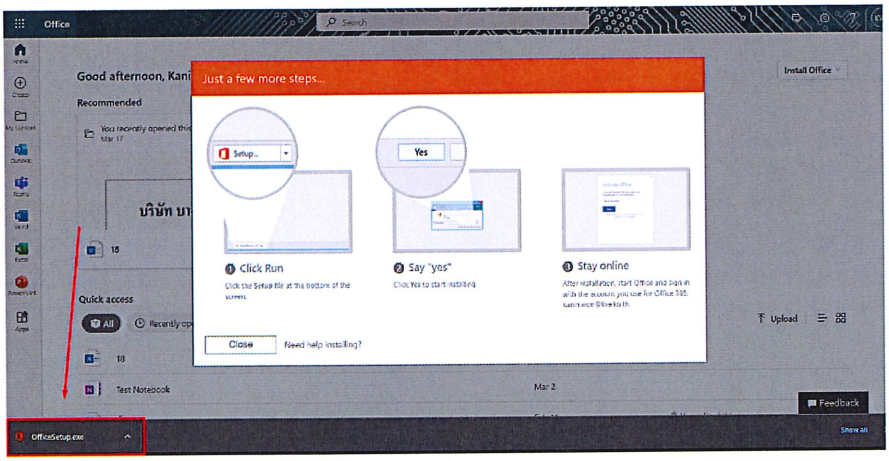


16. เลือก แอป Microsoft 365 หรือ 2021

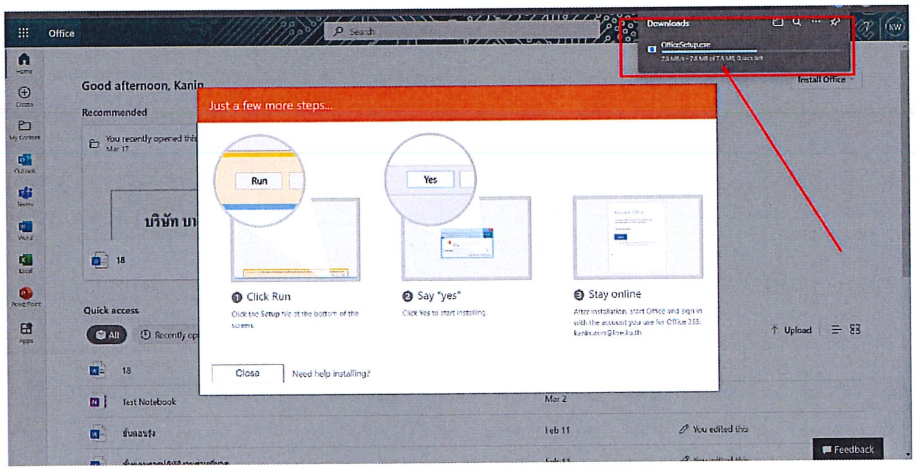


17. หลังจากนั้นจะมีตัวดาวน์โหลดขึ้นมา

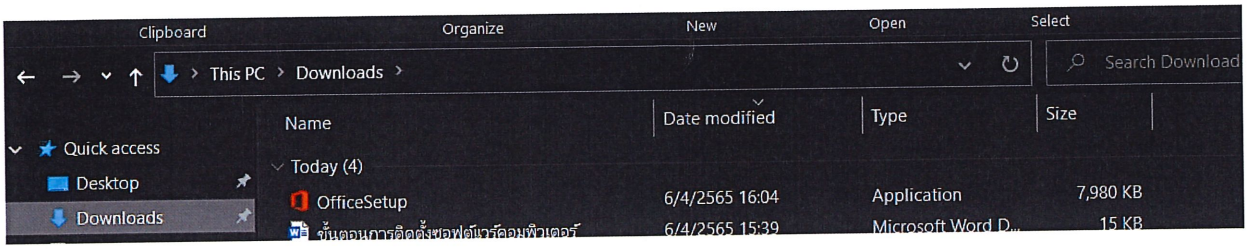
17.1. ในกรณีโหลดผ่าน google chrome



17.2. ในกรณีโหลดผ่าน Microsoft edge



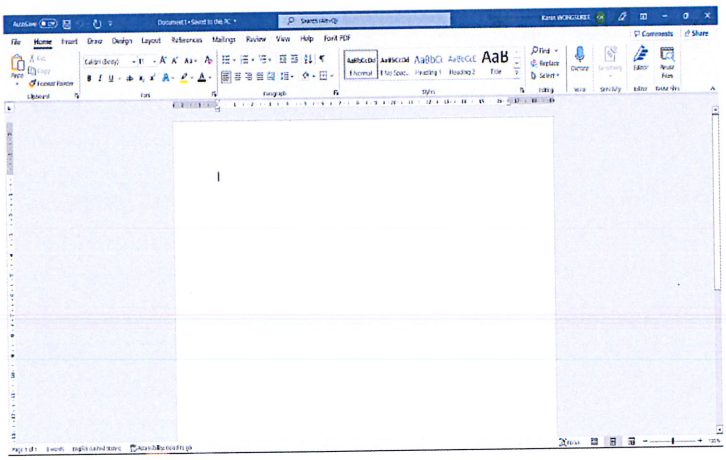
18. ไฟล์จะอยู่ใน This PC ➔ Downloads



19. เมื่อดาวน์โหลดเสร็จให้กดติดตั้ง Office



20. รอจนกระทั่งติดตั้งเสร็จสิ้น และสามารถเริ่มใช้งานได้ทันที



ประวัติการการปรับปรุงเอกสาร				
ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	10 มีนาคม 2565	กร ธรรมมาพาณิชย์
2	1.1	เพิ่มระบบ HumanOS, E-Memo(Z.com)	4 มีนาคม 2567	ชาญยุทธ วัฒนาศักดิกุล

ลงชื่อ_____

(นาย ชาญยุทธ วัฒนาศักดิกุล)

ผู้รับผิดชอบ

วันที่ 4 มีนาคม 2567

ผู้อนุมัติ

ลงชื่อ_____

(นางสาว ธนิศร ธนวงศ์เกษม)

ประธานเจ้าหน้าที่เทคโนโลยีสารสนเทศ

วันที่ 4 มี.ค. 2567

ขั้นตอนการใช้งานและการใช้ Administrator ของระบบ DBC (Dynamics 365 Business Central)

(DBC หรือ Dynamics 365 Business Central เป็นโปรแกรมสำเร็จรูปของทาง Microsoft ที่ดูแลโดยทาง UBIZ)

1. คู่มือขั้นตอนการใช้งานอยู่ในไฟล์ชื่อ "UBIZ-WI_DBC365_Training AppAdmin (TH&ENG)_V2.pdf"

Link : UBIZ-WI_DBC365_Training AppAdmin (TH&ENG)_V2.pdf

PHASE I – Training and Testing

Microsoft Dynamics – DBC 365 Implementation Project

Work Instruction

Application Administration

By

Ubiz Solution Co., Ltd.

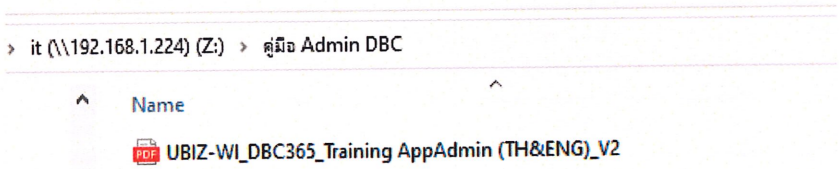
(Revision 00)

Project Name : DBC 365 Implementation
Doc. Type : Workflow & Approval
Prepared By: Ubiz Solution
Date: 30/5/2019
File : UBIZ-WI_TRAINING APP ADMINISTRATION
Page : Page I

Table of Contents

1. Understanding Users, Profiles, and Role Centers 1
1.1 เกี่ยวกับ Profile และ Role Center (Profile and Role Center) 1
2. Managing Users and Permissions 3
2.1 การสร้างหรือแก้ไข Permission Set (Create or Modify a Permission Set) 3
2.2 การเพิ่มผู้ใช้งาน (Adding Users) 7
2.3 การกำหนด User Personalize (Specify User Personalize) 14
2.4 การกำหนด User Group (Specify User Group) 17
3. Creating New Companies 19
3.1 การคัดลอกบริษัท (Copy Company) 19
4. Auditing Changes in Business Central 21
4.1 การทำงานกับการบันทึกการเปลี่ยนแปลงข้อมูล (Working with the Change Log) 21
4.2 การตั้งค่าการบันทึกการเปลี่ยนแปลงข้อมูล (Setup Change Log) 22
4.3 การดูประวัติการบันทึกการเปลี่ยนแปลงข้อมูล (View Change log entries) 24
5. Use Job Queues to Schedule Tasks 26
5.1 สร้าง Job Queue Entry (Create Job Queue Entry) 26
5.2 การดูประวัติการเก็บ Log Files (View Log Files) 29

2. โดยไฟล์ถูกจัดเก็บไว้ใน storage ของแผนกสารสนเทศ อยู่ในโฟลเดอร์ it\คู่มือ Admin DBC



ผู้อนุมัติ

ลงชื่อ ชนิดา ชนงศ์เกษม

(ชนิดา ชนงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 10 มี.ค.65

ลงชื่อ ณัฐชิตา สิงห์ดง

(น.ส. ณัฐชิตา สิงห์ดง)

ผู้รับผิดชอบ

วันที่ 10 มี.ค 65

ขั้นตอนการใช้ Administrator ของระบบ OSintergroup

User Admin หรือผู้ดูแลระบบ มีรับสิทธิ์สูงสุดในการเข้าถึงระบบ สามารถเพิ่ม/ลบ/แก้ไขชื่อผู้ใช้งาน และกำหนดสิทธิ์การใช้งานของผู้ใช้งานแต่ละคน โดยมีขั้นตอนดังนี้

1. ทำการ Login จากLink : http://osintergroup.com โดยระบุ User name และ Password ที่เป็น Admin

   ตัวอย่าง User name : Admin

   Password : M1k2@++--**//

2. การเพิ่มชื่อผู้ใช้งาน เมื่อได้รับแจ้งในฟอร์ม ขอรับสิทธิ์การใช้งานระบบ ให้ทำการเพิ่มรายชื่อผู้ใช้งานในระบบ ดังนี้

   2.1. คลิกไปที่เมนู ข้อมูลระบบ เลือกหัวข้อ รายชื่อพนักงาน

   2.2. คลิกไปที่ เพิ่มพนักงานใหม่

   2.3. กรอกรายละเอียดข้อมูลพนักงาน

      2.3.1. ชื่อพนักงาน

      2.3.2. ประเภทพนักงาน

      2.3.3. ตำแหน่ง

      2.3.4. แผนก

      2.3.5. เบอร์โทรศัพท์

      2.3.6. Email

      2.3.7. ในส่วน username และ password ระบบจะใส่ค่ามาให้ก่อน โดย username และ password จะเป็นค่าเดียวกัน

   2.4. กด บันทึก

   2.5. แจ้ง user name และ password ให้ผู้ใช้งานผ่านอีเมล และแจ้งให้ผู้ใช้งานแก้ไข password ทันที

   2.6. เข้าไปกรอกสถานะในแบบฟอร์ม ขอรับสิทธิ์การใช้งานระบบ

3. เมื่อได้รับแจ้งรายชื่อพนักงานลาออก ให้ทำการเปลี่ยนสถานะเป็น**พ้นสภาพ**

   3.1. ค้นหารายชื่อที่ต้องการเปลี่ยนสถานะ

   3.2. แก้ไขสถานะ จากเดิมพนักงาน เปลี่ยนเป็น **พ้นสภาพ**

   3.3. กดปุ่มลบ จากนั้นกด OK เพื่อยืนยันสถานะ **พ้นสภาพ**

4. การกำหนดสิทธิ์การใช้งาน ในแบบฟอร์ม ขอรับสิทธิ์การใช้งานระบบ จะถูกระบุจากผู้ขอใช้งานให้เปิดใช้งานโมดูลไหนบ้าง จากนั้นให้มาทำการเปิดการใช้งานที่ระบบ ดังนี้
   4.1. คลิกเข้าไปที่ชื่อผู้ใช้งานที่ต้องการ
   4.2. ที่หัวข้อ สิทธิ์ในระบบ คลิกถูกที่หัวข้อที่ต้องการเปิดสิทธิ์การใช้งาน
   4.3. กด บันทึก
   4.4. เข้าไปกรอกสถานะในแบบฟอร์ม ขอรับสิทธิ์การใช้งานระบบ
5. กดออกจากระบบทุกครั้งเมื่อใช้งานเสร็จทุกครั้ง

ประวัติการการปรับปรุงเอกสาร				
ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	15 มีนาคม 2565	ณัฐธิดา สิงห์คง
2	1.1	แก้ไขขั้นตอนยกเลิกผู้ใช้งานในระบบ	4 มีนาคม 2567	ชาญยุทธ วัฒนาศักดิกุล

ลงชื่อ_____

(นาย ชาญยุทธ วัฒนาศักดิกุล)

ผู้รับผิดชอบ

วันที่ 4 มีนาคม 2567

ผู้อนุมัติ

ลงชื่อ_____

(นางสาว ธนิศร ธนวงศ์เกษม)

ประธานเจ้าหน้าที่เทคโนโลยีสารสนเทศ

วันที่ 4 มีนาคม 2567.

ขั้นตอนการใช้ Administrator ของระบบ Kintone

User Admin หรือผู้ดูแลระบบ มีรับสิทธิ์สูงสุดในการเข้าถึงระบบ สามารถเพิ่ม/ลบ/แก้ไขชื่อผู้ใช้งาน และกำหนดสิทธิ์การใช้งานของผู้ใช้งานแต่ละคน โดยมีขั้นตอนดังนี้

kintone

Guidebook for First-Time kintone Users



Published by Cybozu, Inc.

Beginner Level Section

~ From creating apps to beginning operating ~

Use kintone's basic functions

Create an app from the beginning ..... P5~P10

Register kintone users ..... P11~P14

Use the app you created ..... P15~P18

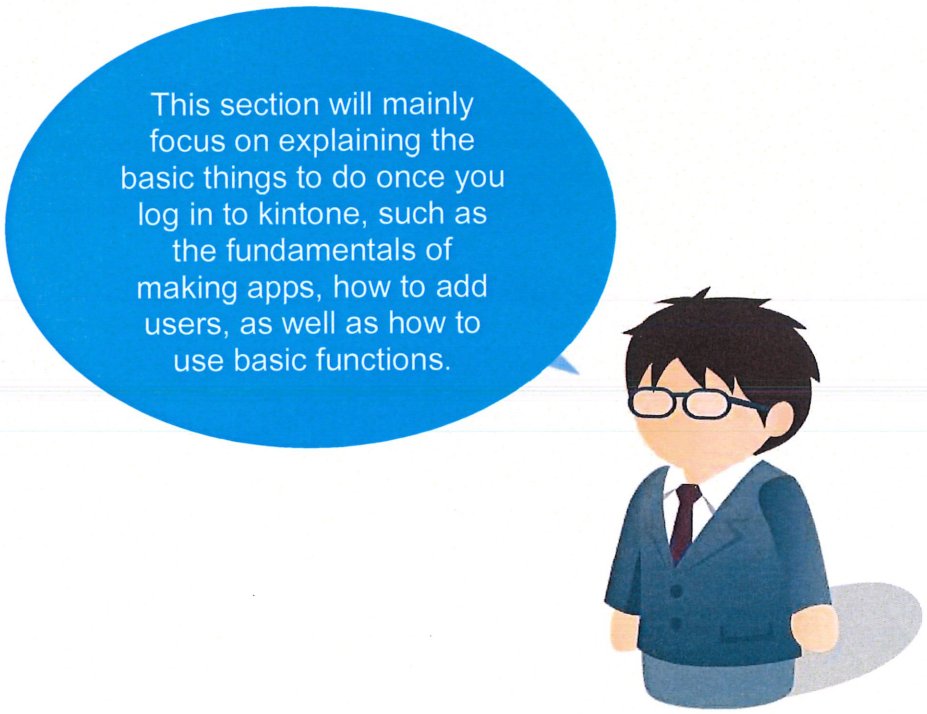
Comment functions ..... P19~P20

Change log ..... P21~P22

Benefits of using kintone apps P23

Import Excel files to create apps ..... P24~P27

Add from the app store P28~P30



Create an app from the beginning

In this section, we will utilize an actually usable app as an example of how to create an app. Now let's create a task management chart that can be shared among team members.

Challenge

Managing team member tasks as easily as possible



kintone Promotion Team

Ami

I have no idea what tasks are assigned to my team members… Even if I ask the members to take on new tasks, I can't manage their progress, and there might be some conflict over who said what. I want to manage the team's tasks, but with excel, I can already predict that the members will get lazy and forget to update their progress… What should I do?

Problem-solving app

Team task management



Records 1 - 6 of 6

Task Title	Assignee	Deadline	Status
Flyer design creation	Kana Masuda	Feb 02, 2016	Not yet
Web page recreation	Kana Masuda	Jan 19, 2016	Not yet
Event planning and management	Yuta Sasaki	Feb 01, 2016	Not yet
Tanaka pharmaceutical company	Yuta Sasaki	Feb 10, 2016	Not yet
Poster for advetisement	Yuta Sasaki	Jan 11, 2016	Not yet
Yamamoto corporation case coverage	Yukako Suzuki	Jan 15, 2016	Not yet

The app we will create in this section will make representative names, deadlines, and progress easily visible as a list. Not only can you see in real time which staff member is handling what tasks, you can also keep a log of what tasks have been completed in the past.

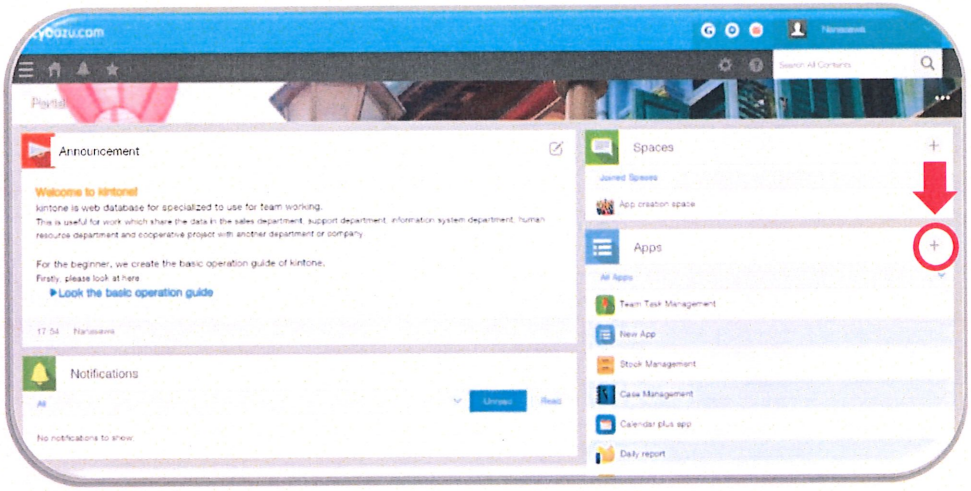
1. List up necessary items

Before creating a team task management app, first check necessary items. In this app, we will include the following five items:

- Task title
- Name of the person in charge
- Deadlines
- Progress
- Detailed contents

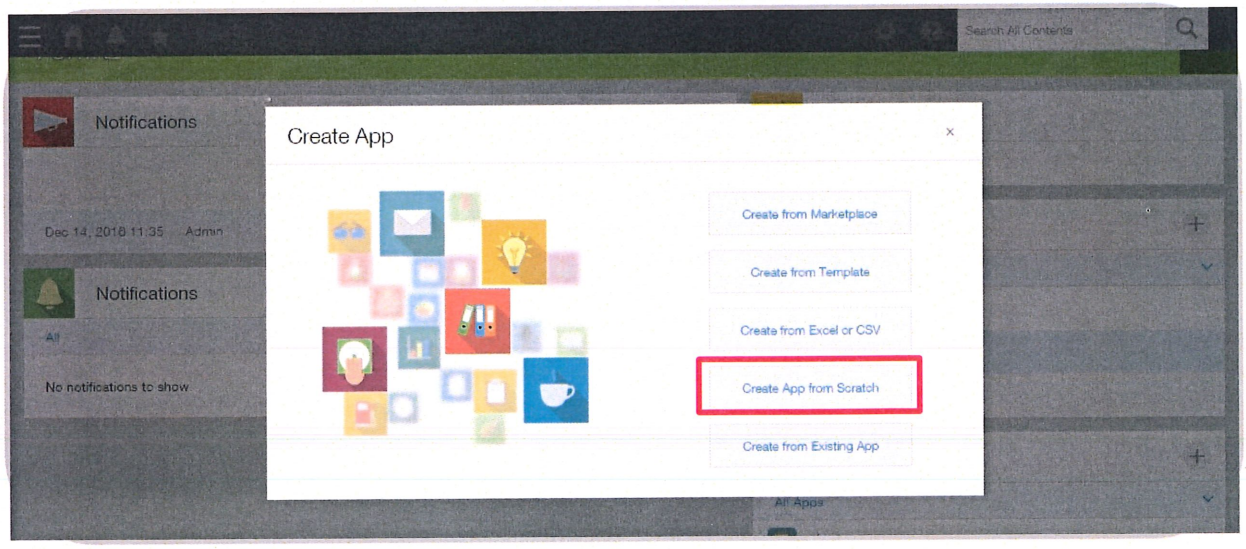
2. Click the “Create App” button and move to the creation screen

Click the + on the kintone top page



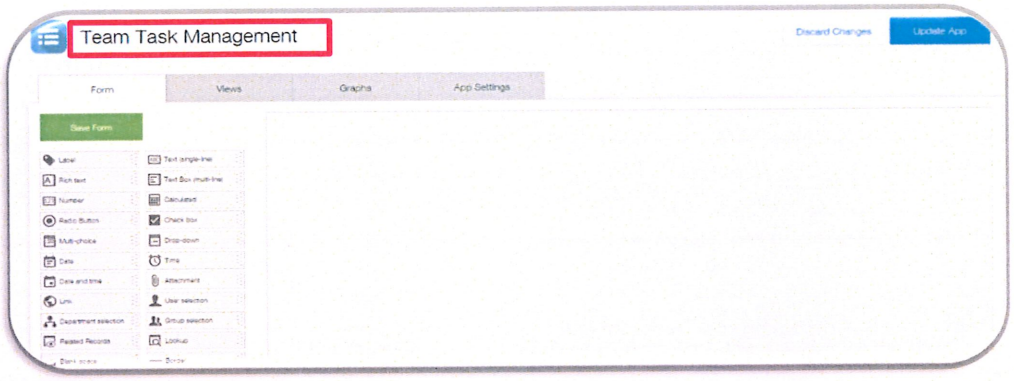
3. Select anappcreation method

For this app, we will select the fourth item from the top, “create from the beginning.” This method allows you to freely create an app from a blank state.



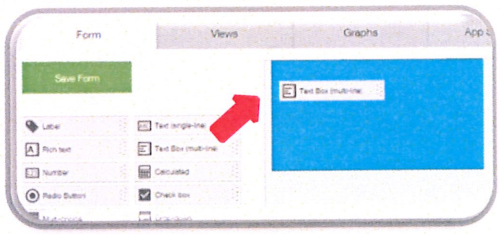
4. Enter app name

We will name this app "Team Task Management."



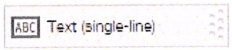
5. Set an entry form

Here, we will set a form for registering team tasks. In kintone, you can arrange the fields and alignment freely by dragging and dropping the parts.



Click and hold down the icon with the mouse and slide to a different location, then let go of the button.

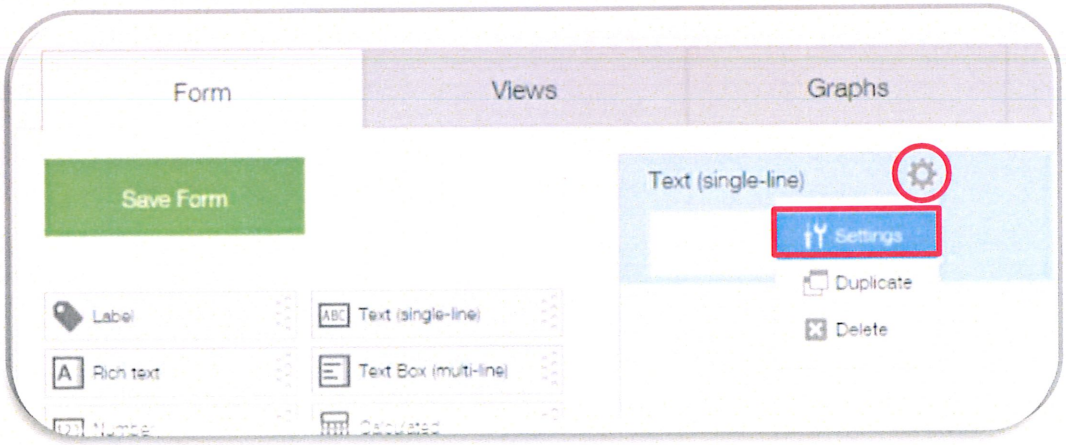
5-1 Set an entry form



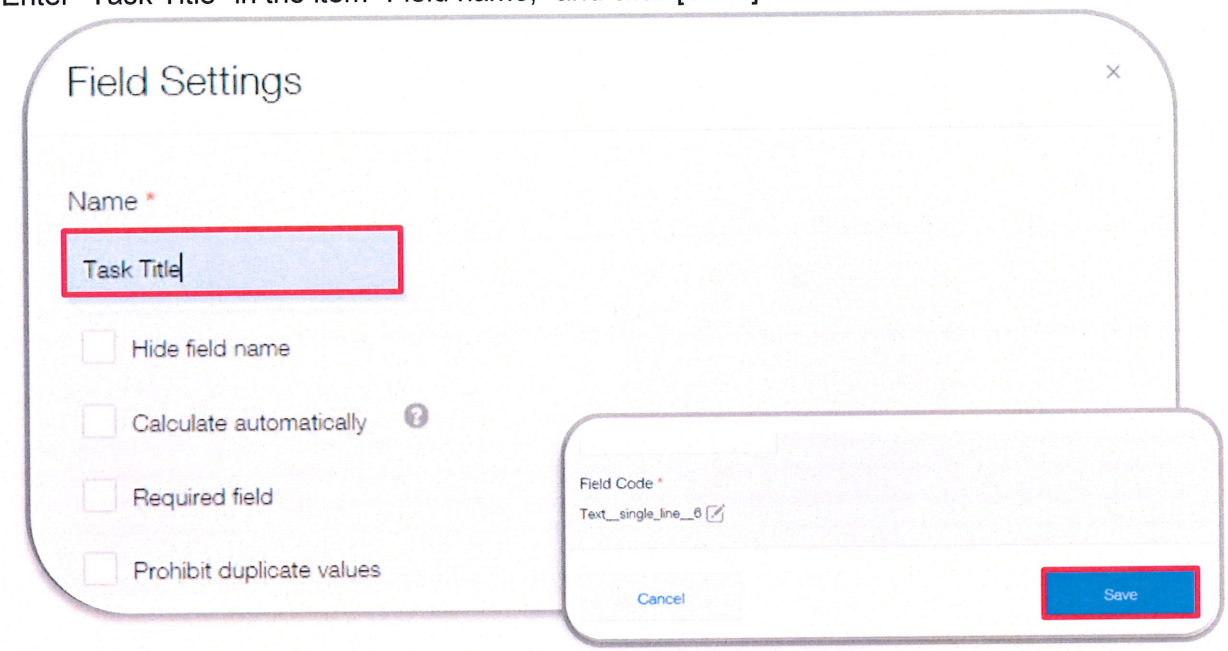
Drag and drop the [Text (single-line)] icon to the field on the right.

5-2 Change the names of parts

Hover your mouse over the cogwheel icon on the right of the [Text (single-line)]. Click the Settings menu after it appears.



Enter “Task Title” in the item “Field name,” and click [Save].



5-3 **Place other parts in the same way as you did in sections 5-1 and 5-2**

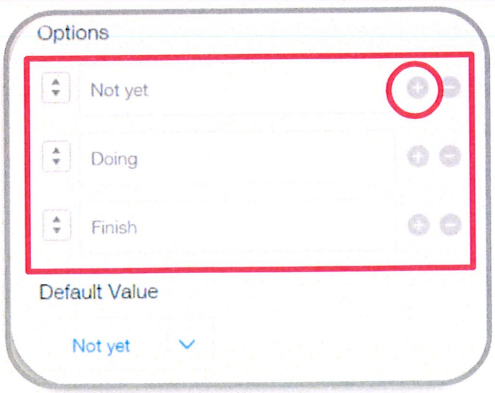
Drag and drop the User selection icon to the field on the right. Click “Settings” and change the field name to “Name of the person in charge.”

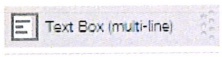
Drag and drop the Date icon to the field on the right. Click “Settings” and change the field name to “Deadline.”

Drag and drop the Drop-down icon to the field on the right. Click “Settings” and change the field name to “Progress.”

Enter “Not started,” “In progress,” and “Completed” in the “Items and order” item column, located in the center of the settings screen.

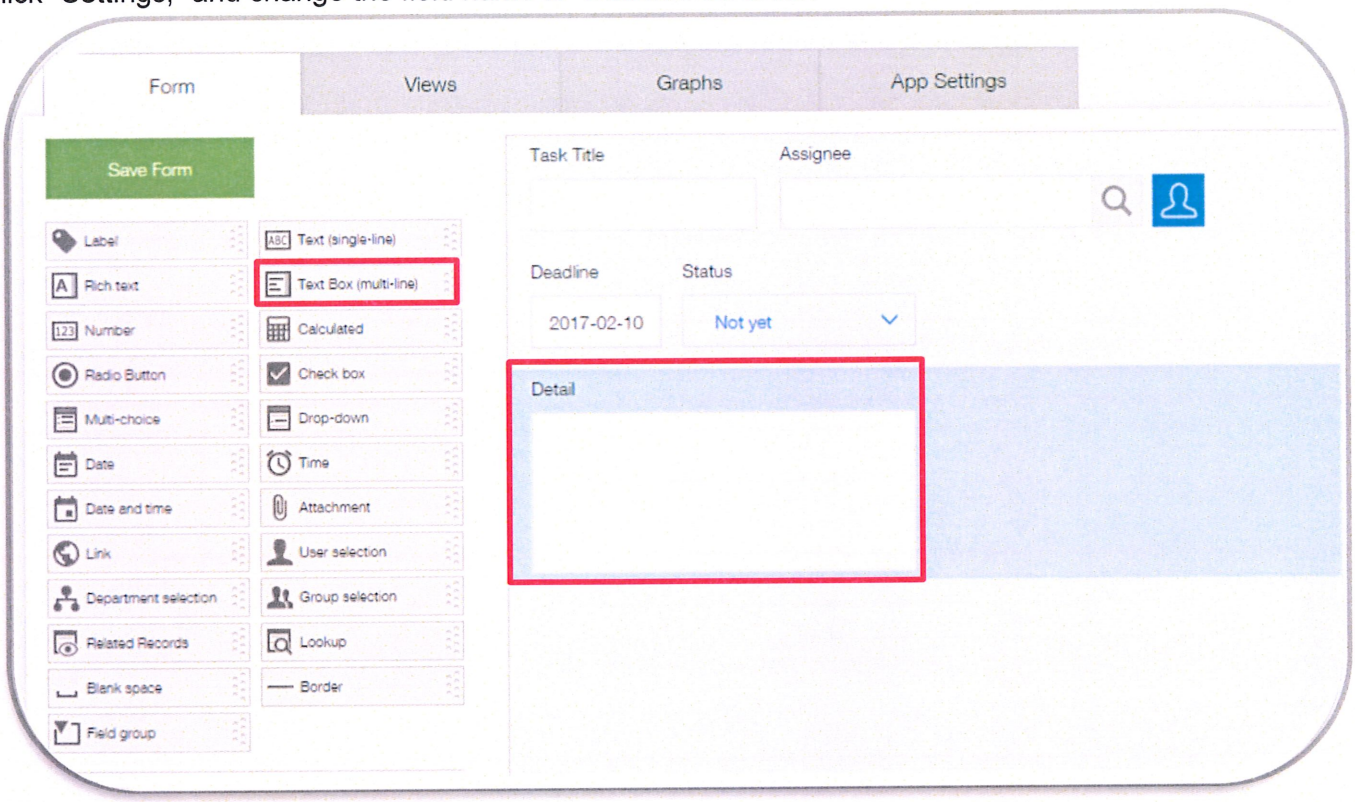
There are only two item columns in the default settings, but you can add item columns by clicking the ⊕ icon.



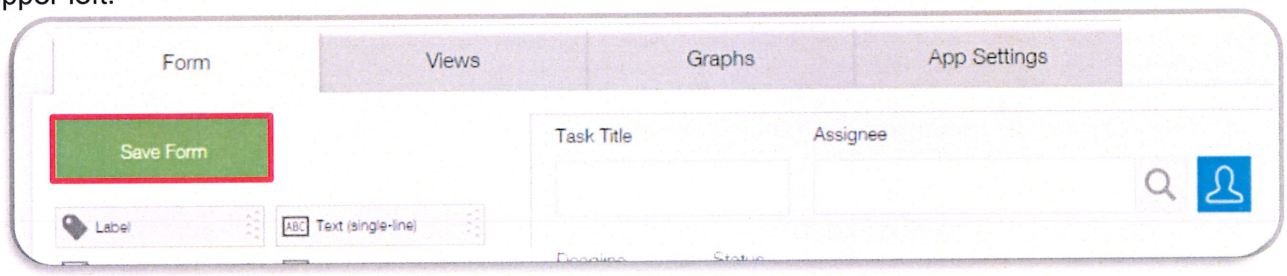
Drag and drop the 

icon to the field on the right.

Click “Settings,” and change the field name to “Detailed contents.



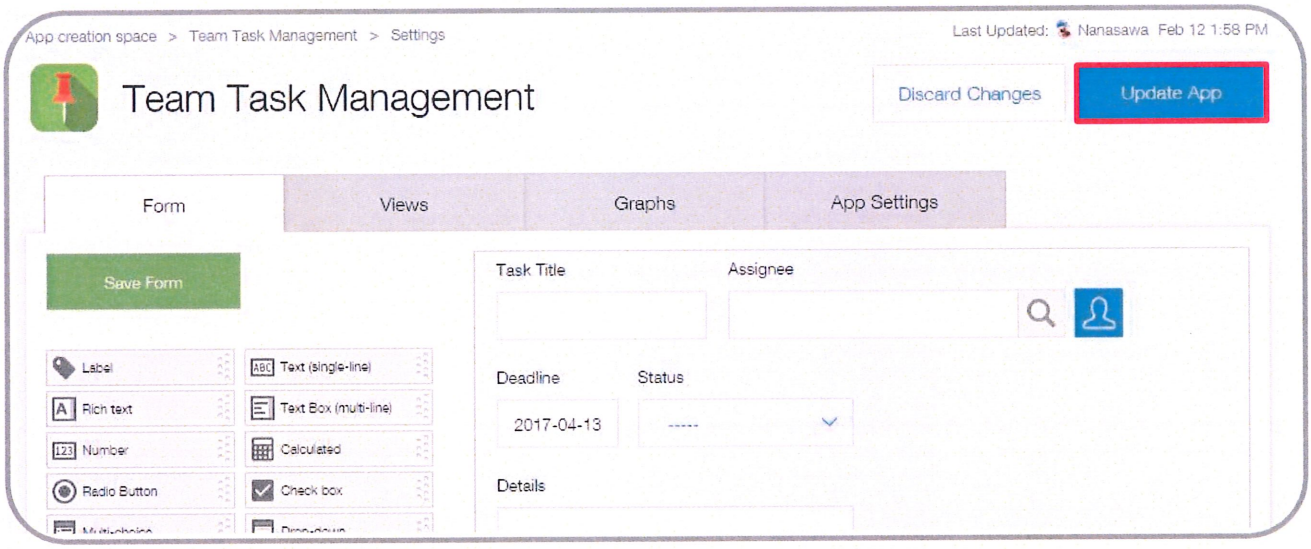
This concludes the item settings. If there are no problems with the contents, click “Save form” on the upper left.



5-4 Click “Publish app” to begin operating the app

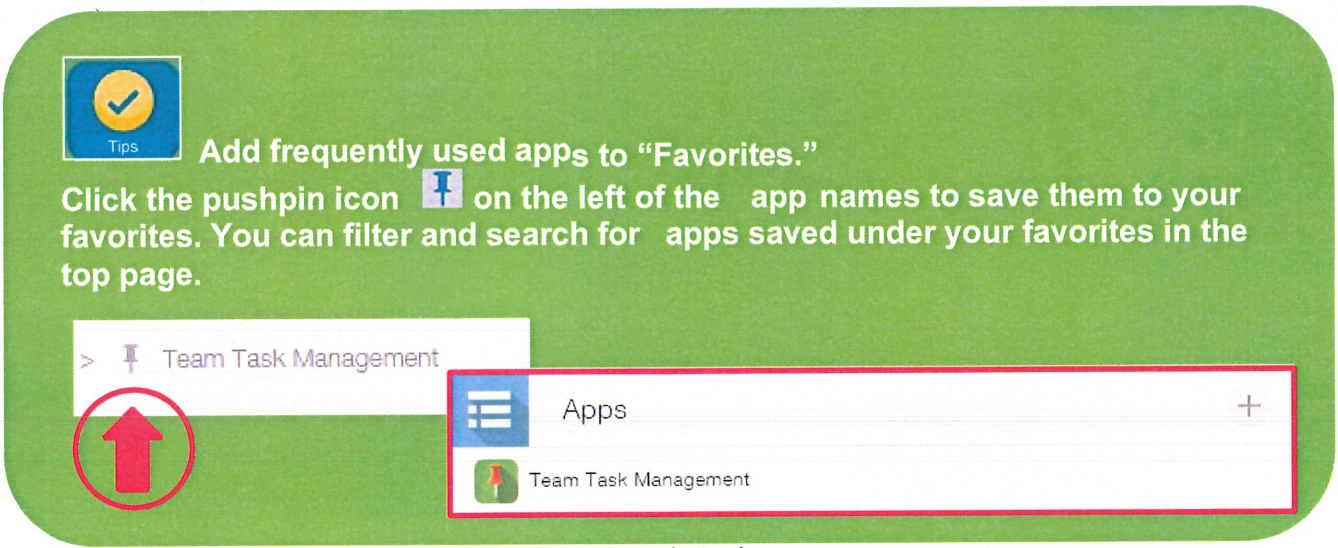
This concludes the basic settings of the app.

Click “Publish app” to begin operating the app.



The “Team Task Management App” is complete!

You now have a box to manage your team’s tasks. Register tasks, designate people, and share tasks



with the team using the app to visualize your team’s tasks.

Register kintone users

Once the Team Task Management App is complete, in the next step, we will register app users. In this situation, we will register five members from the same team (marketing).

※You can register users before starting creating apps.

Members to add (Marketing Dept.)



Noboru Sato　Tomomi Koyama　Kana Masuda　Yuta Sasaki　Yukako Suzuki

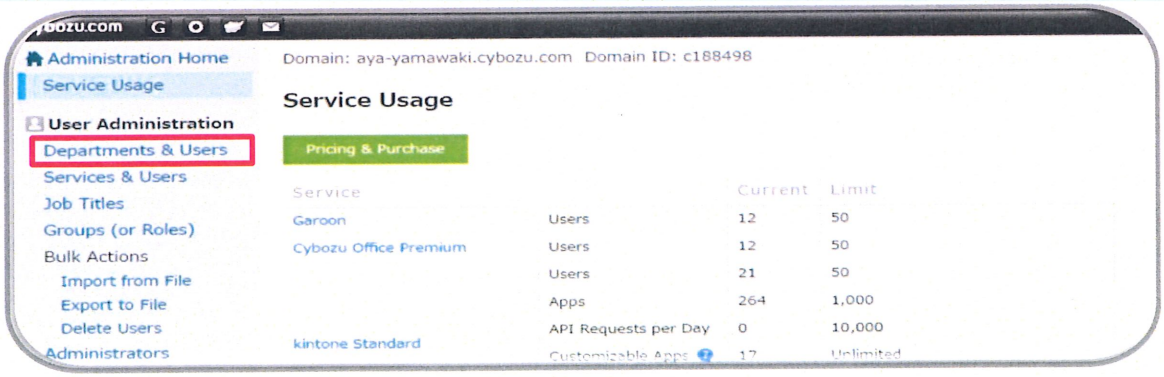
1. Open “cybozu.com common management”



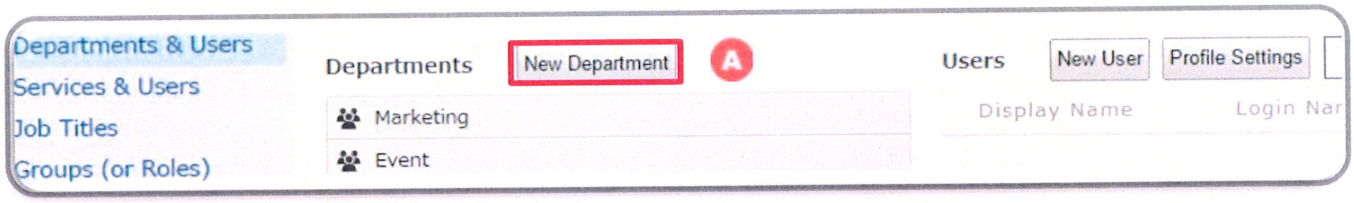
2. Add groups from the item “Groups/Users”

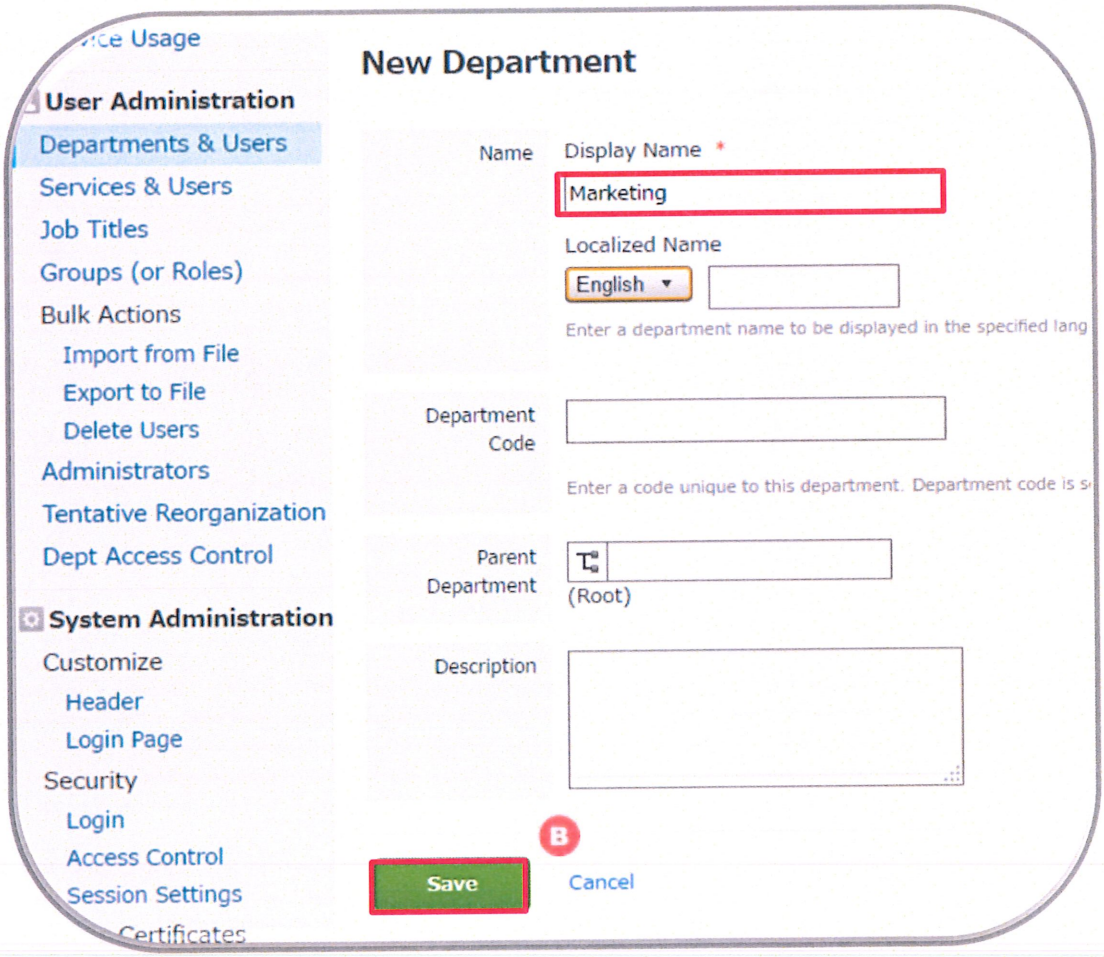
A menu will appear after clicking on the cogwheel icon in the upper right of the screen. Select “cybozu.com common management.”

When the “cybozu.com common management” appears, select [Groups/Users] from the menu on the left.



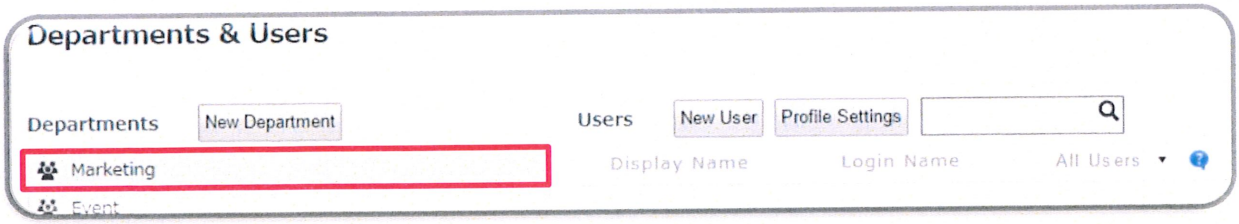
Click "Add group," (A) highlighted in red in the image below. Enter a group name in the "Group Name" section, and click (B) "Save."



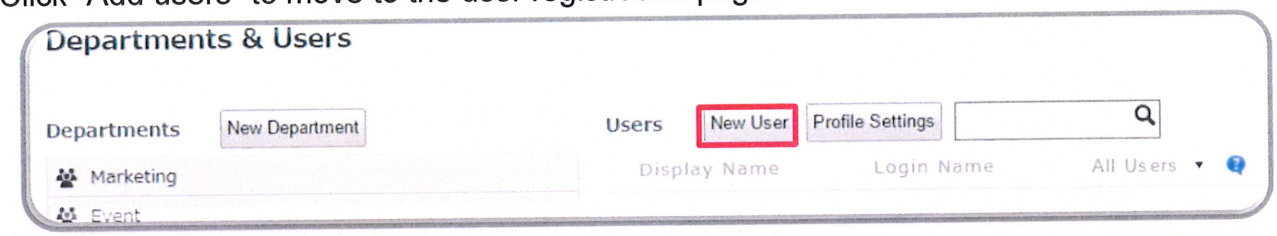


3. Add users from the item "Groups/Users"

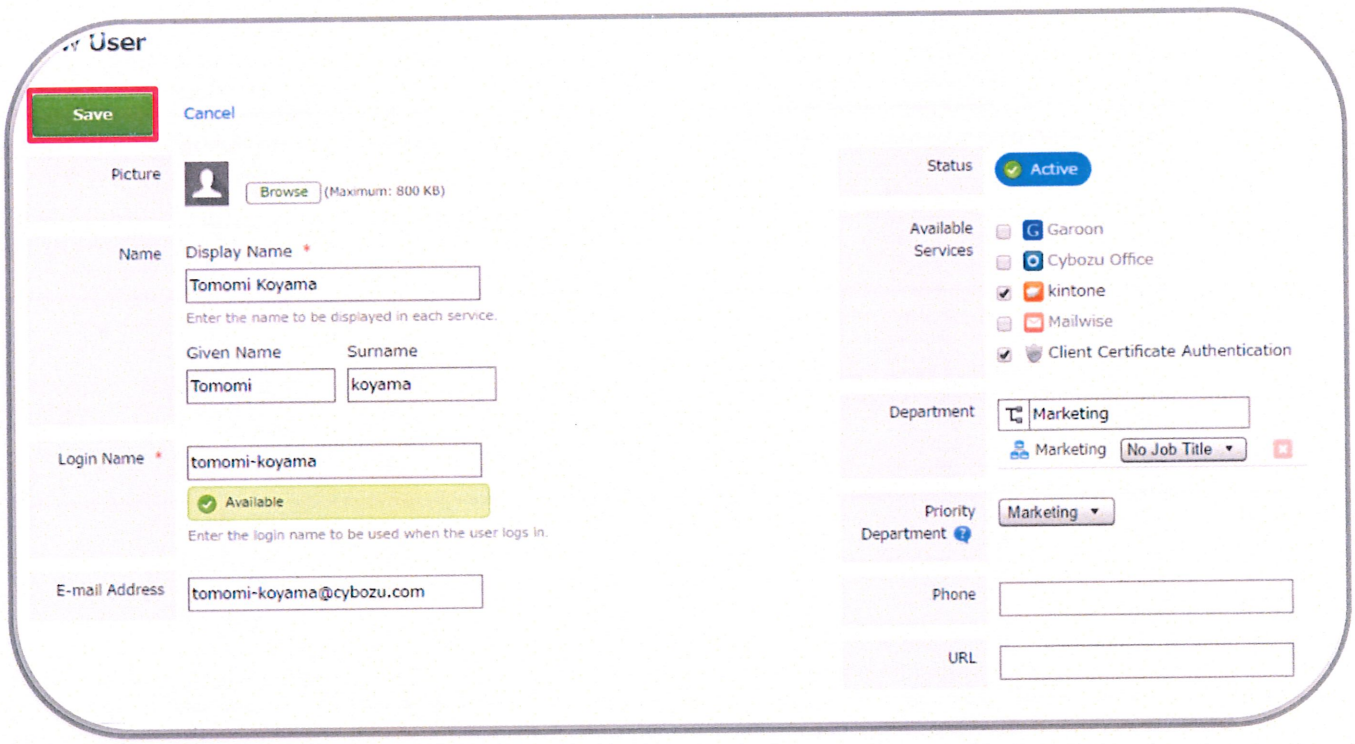
Click the group name created in step 2



Click “Add users” to move to the user registration page.



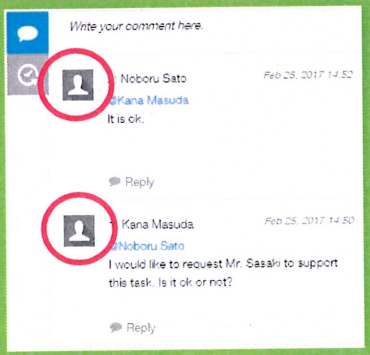
Set the necessary items and click “Save.”



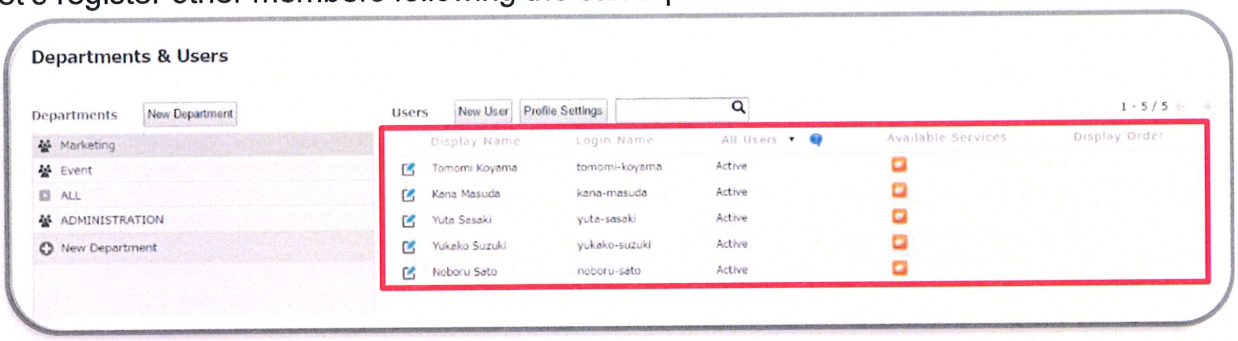
This concludes the user registration process.

Tips **The user can edit user images and information, such as contact information, at a later date.**

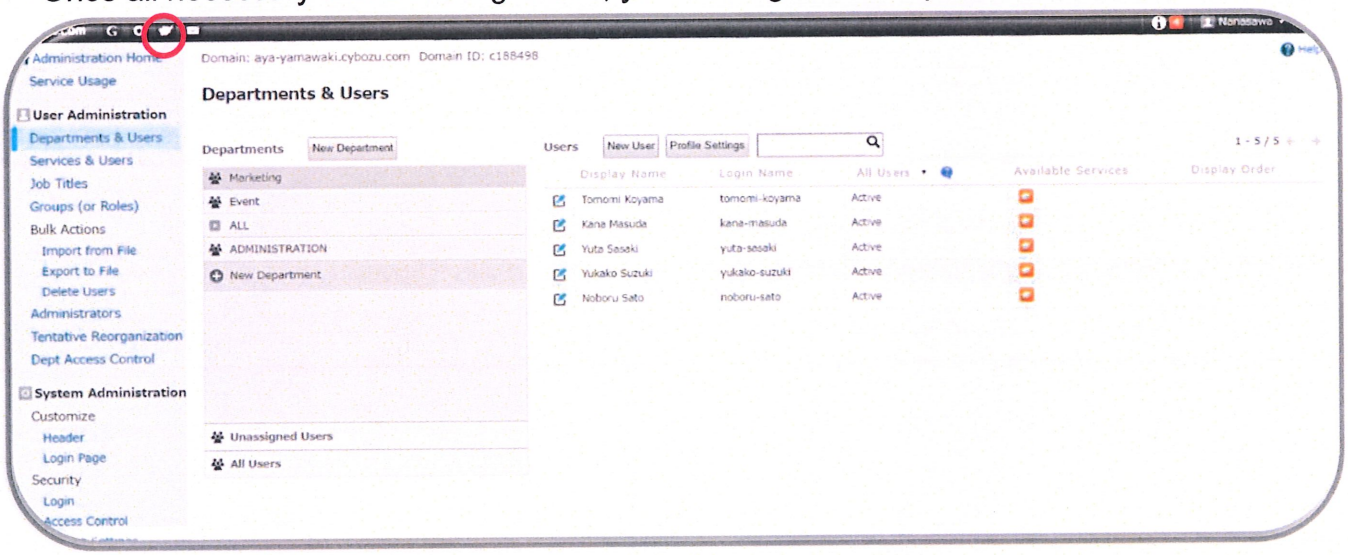
Users can change their icon image, displayed next to their name, as well as edit information such as contact information and birthdays. At the initial user registration stage, setting the required fields such as displayed name, login name, and password should suffice.



Let's register other members following the same process.



Once all necessary users are registered, your settings are complete.



Click the cloud icon on the top left and return to kintone's top page.

Use the app you created

Let's use the app we created with the users we added in the previous section.

Before that, we must determine the current tasks of all members of the marketing department and register them.



Suzuki



Sasaki Yuta

・Creating the kintone catalog
・Creating new novelties
・Drafting press releases

・Creating promotional posters

・Coverage of an example case from Tanaka Pharmaceuticals

・Planning and managing event exhibitions



Kana Masuda



・Creating guidebooks, such as the one for kintone ・
Implementing user questionnaire surveys

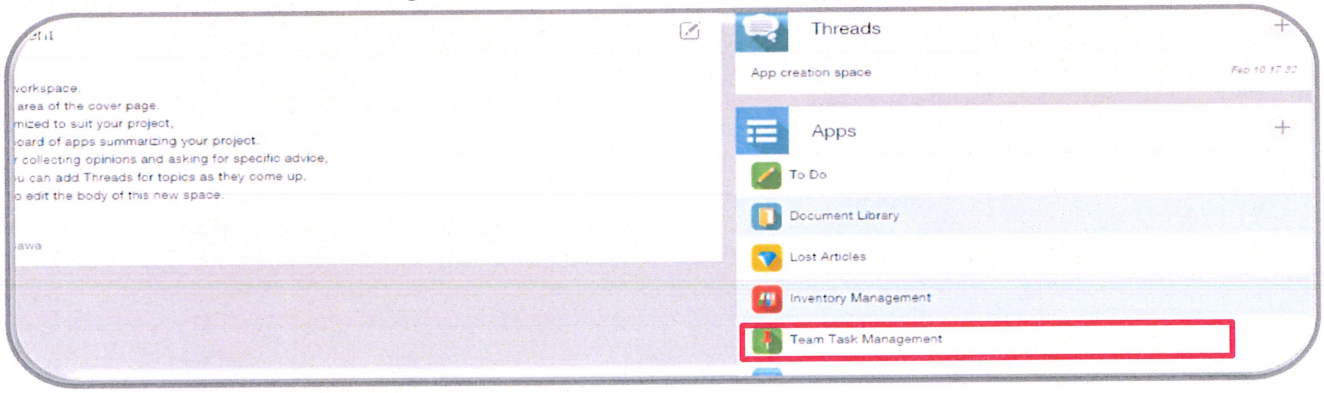
・Coverage of an example case from Yamamoto Inc.
・Web site renewal
・Creating flyer designs

Tomomi Koyama

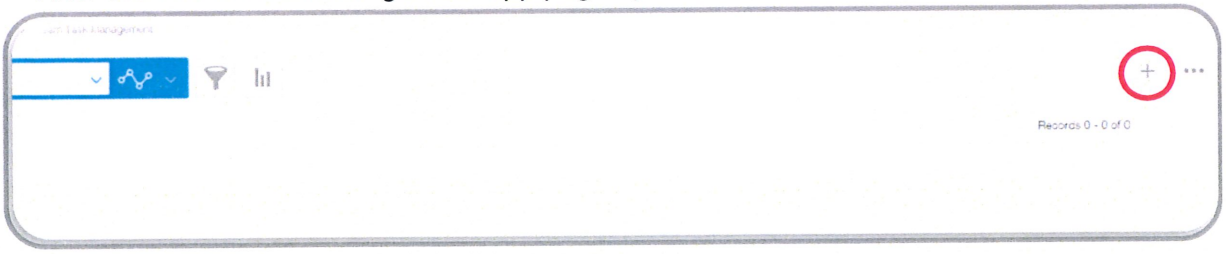
Yukako

1. How to register new records

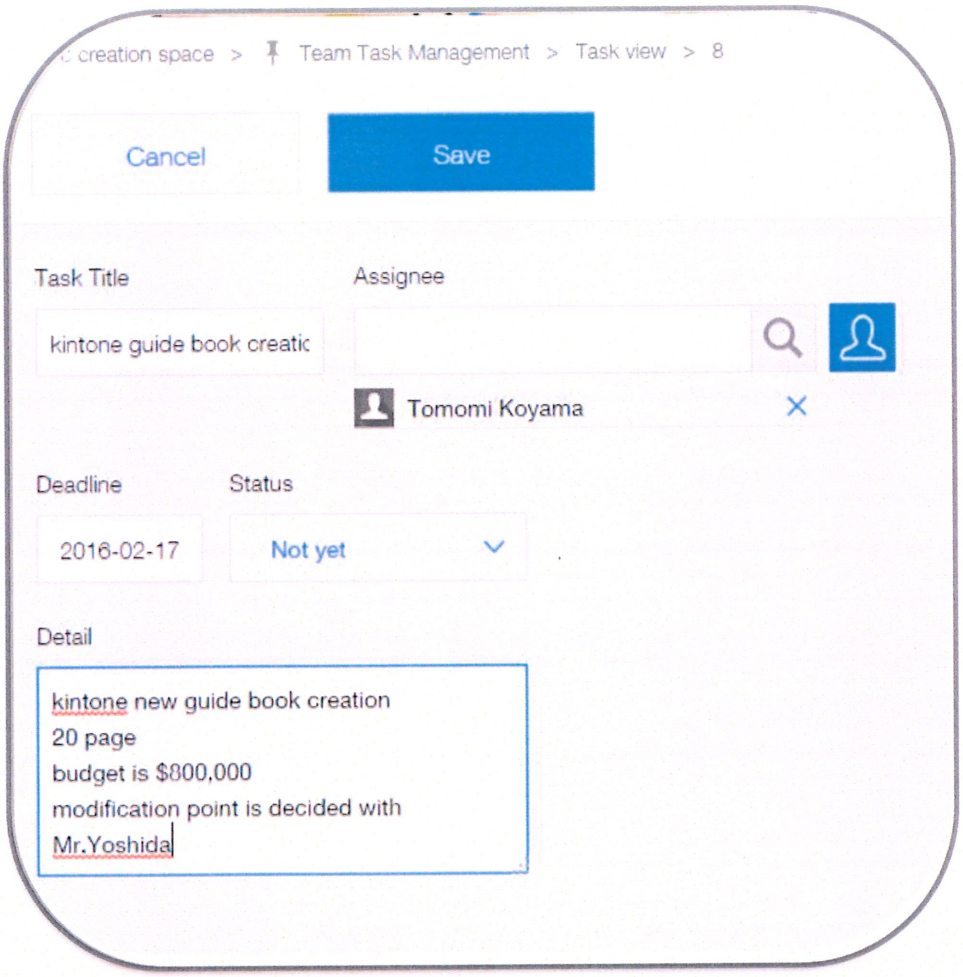
Click the "Team task management" icon on the bottom right of the kintone top page.



After the Team Task Management app page opens, click the + icon on the top right of the Screen



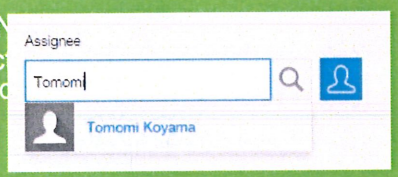
Enter the “Task title,” “Name of the person in charge,” Deadlines,” “Progress,” and “Detailed content”.

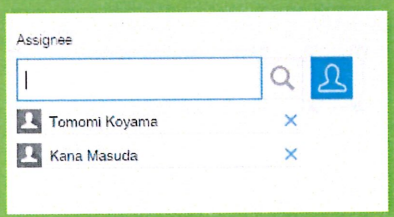


Tips

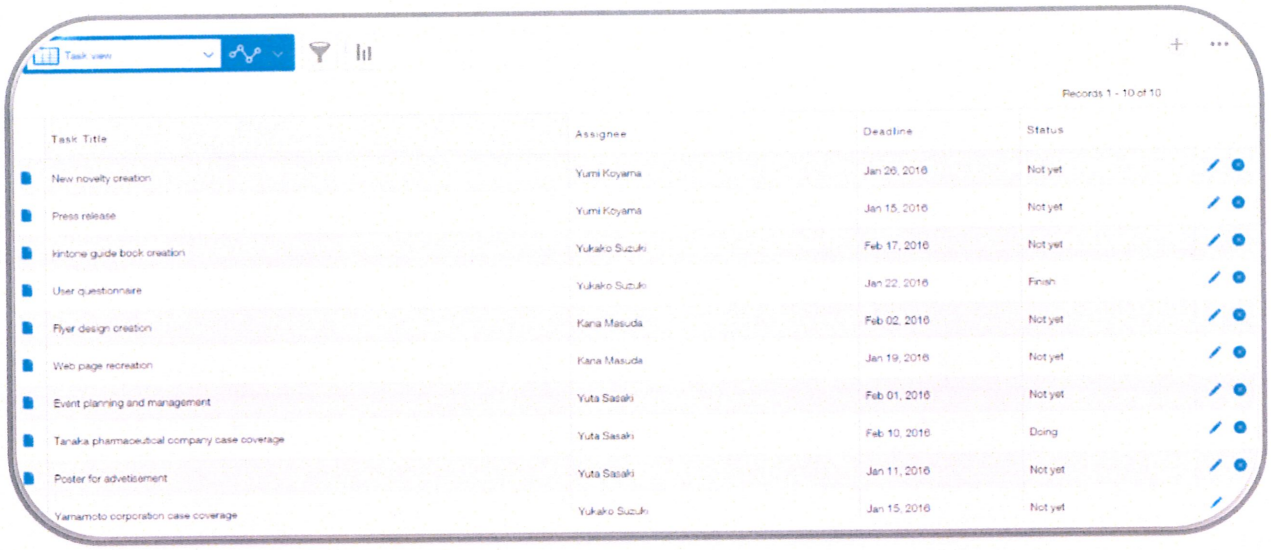
How to use the “Name of the person in charge” column (user selection

The user selection part is used for the “N
of the person in charge” column. User selec
parts can search and select users registered
kintone.



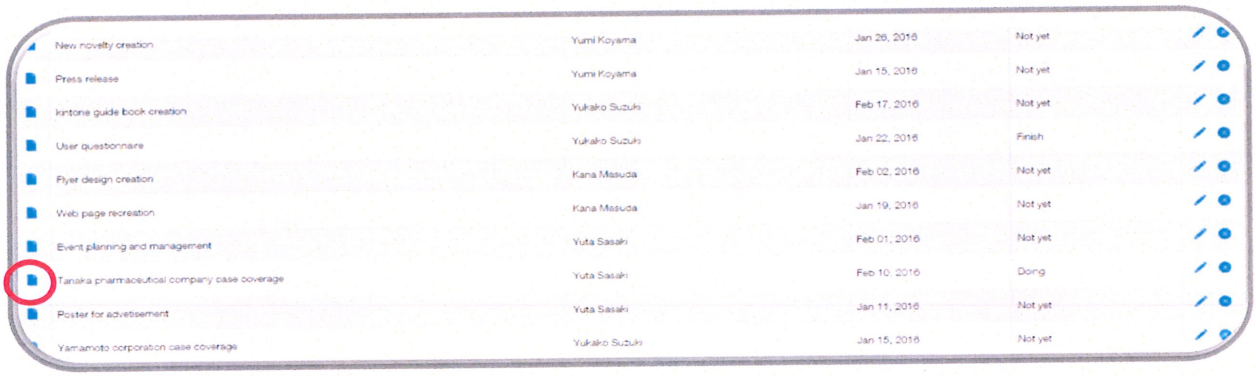


We will register other members' tasks similarly. This time, you have registered every task, but it may be best to have everyone register his or her own tasks.



2. How to edit and make changes registered content

If there have been changes to registered content, you will need to edit the records.
In this example, we will change "Not started" tasks to "Completed" in the "Progress" section.

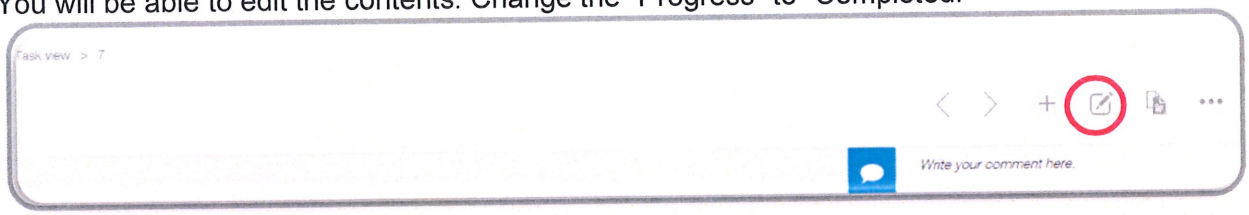


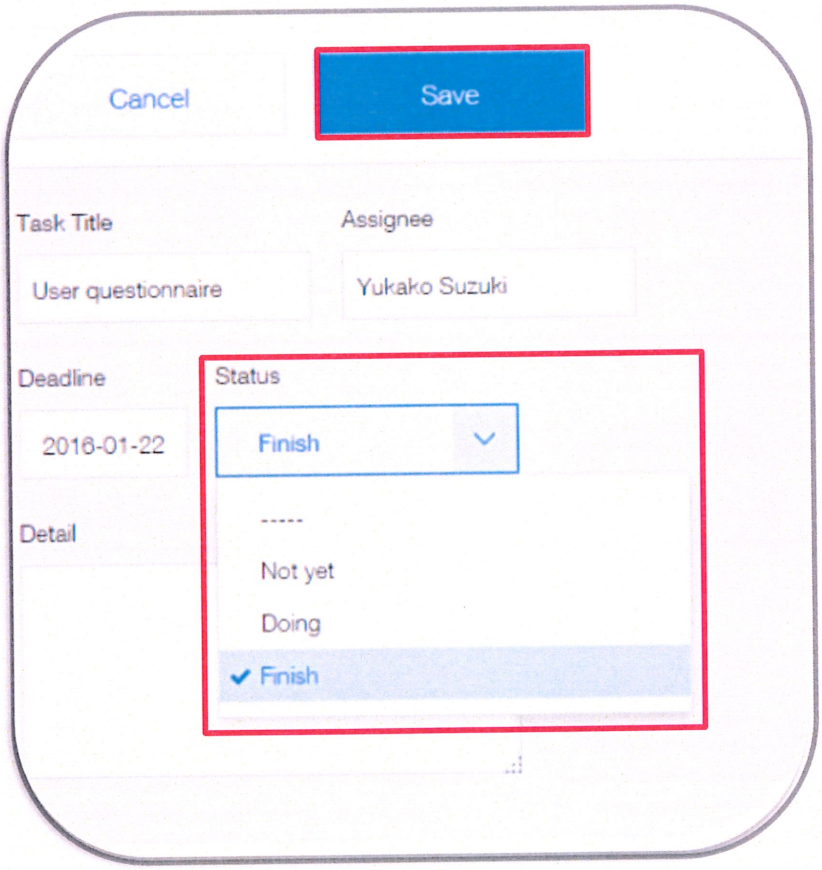
Here, we will change the "Progress" of Suzuki's task, "Implementing user questionnaire surveys."

Click the blue icon on the left to open the details screen.

Click the icon on the top right of the details screen.

You will be able to edit the contents. Change the “Progress” to “Completed.”



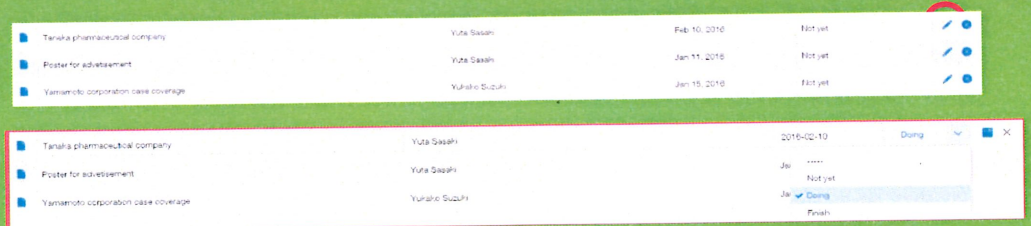


Click [Save]. When the record list screen is displayed, the tasks have been successfully updated.

Tips

You can directly edit and make changes to tasks from the list screen

By clicking on the icon on the right of each task in the list screen, you can directly edit and update items on the list.
*Some items cannot be edited from the list screen.



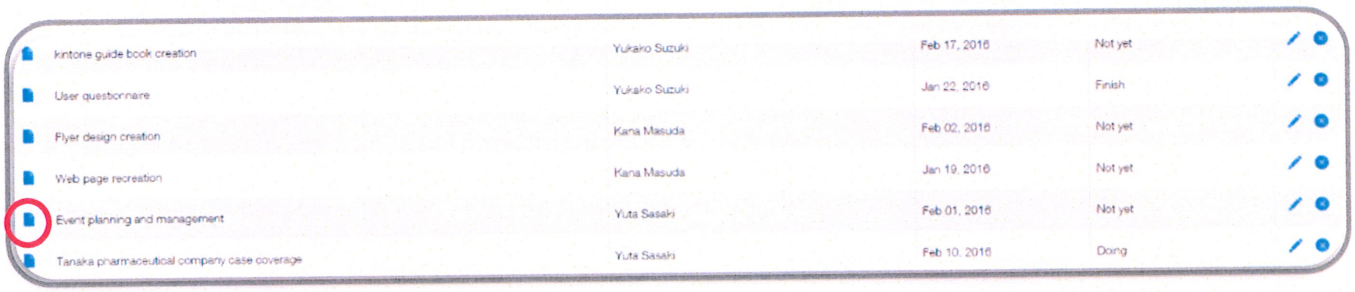
Comment functions

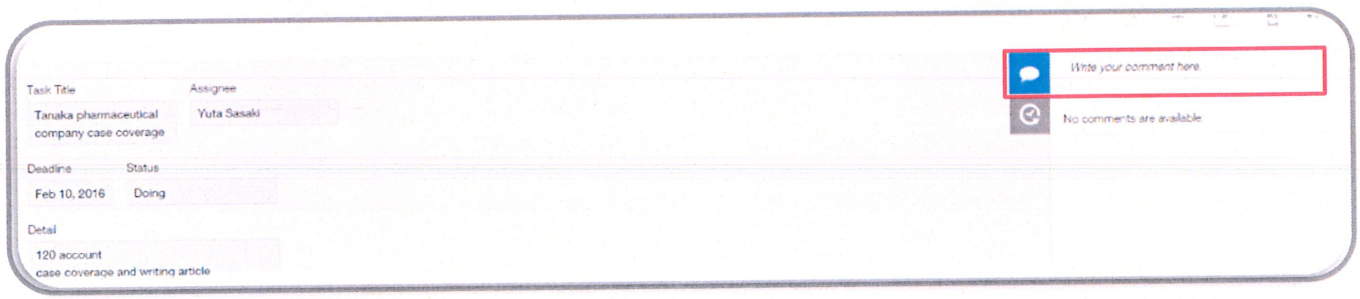


Procedure for writing comments in records

1. Open the details screen to display the comment field

Open the record list and click the blue icon on the left side to open the details screen. Then, click “Comment” on the right side of the details screen.



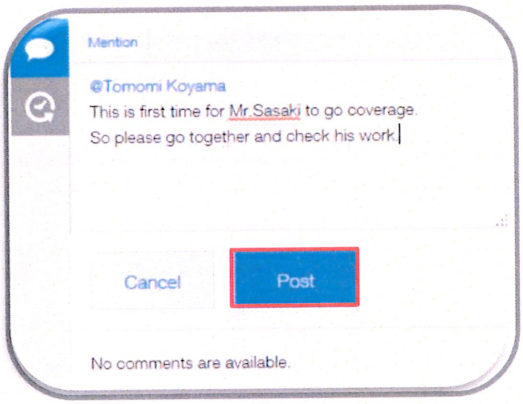


2. Write a comment in the comment field

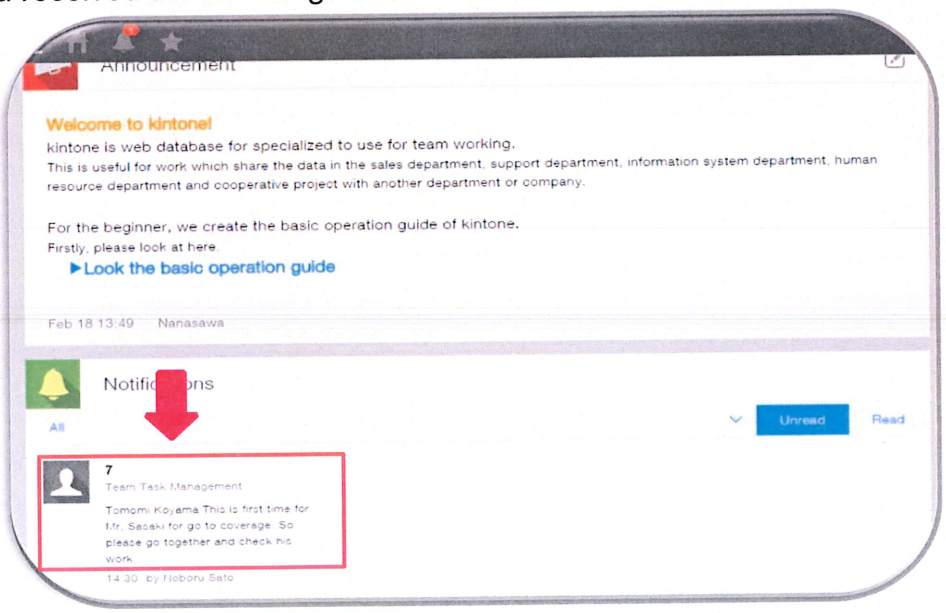


When you click "Select recipient," an @ mark will be displayed. Enter the name of the person to whom you want to leave a comment. When you type the person's name up to a certain point, a list of corresponding user names will appear. Click on the name you wish to leave a comment for.

Enter your comment, and click "Post."



You will be notified of comments addressed to you in the kintone portal. In this example, Koyama received the following notification.



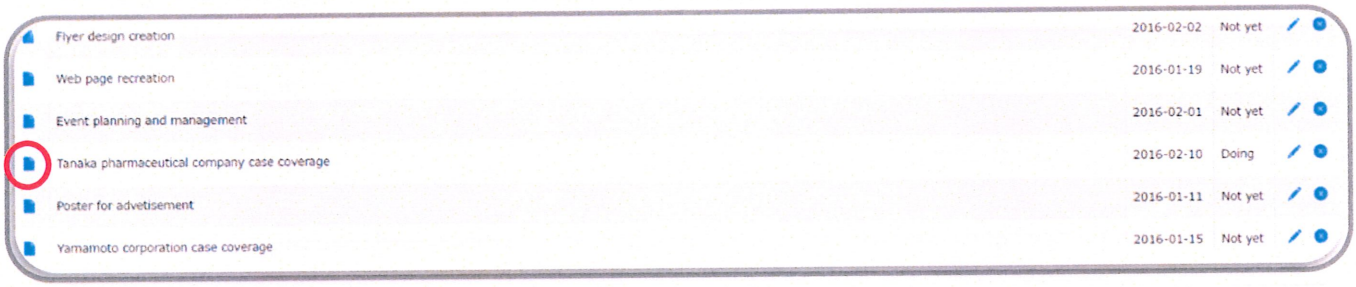
Revision history

kintone apps feature a “Revision history” function, which automatically keeps a record of who made what changes to what items. When sharing information on software such as Excel, it is easy to lose track of which file is the latest, or what changes have been made.
The revision history function not only prevents such situations, but also allows users to revert to older data, in case someone accidentally overwrites a file, preventing issues that often occur when sharing data.

Procedure for displaying revision history

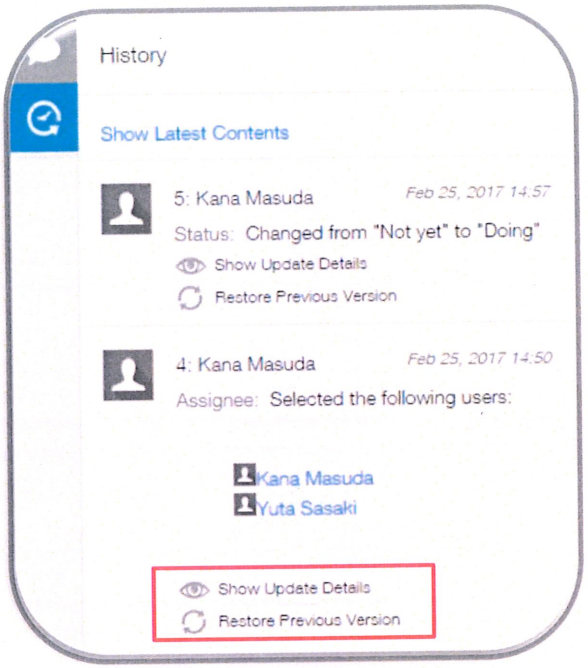
1. Open the details screen and display revision history

Open the record list screen and click the blue icon on the left side to open the details screen. Click the icon on the right side of the details screen.



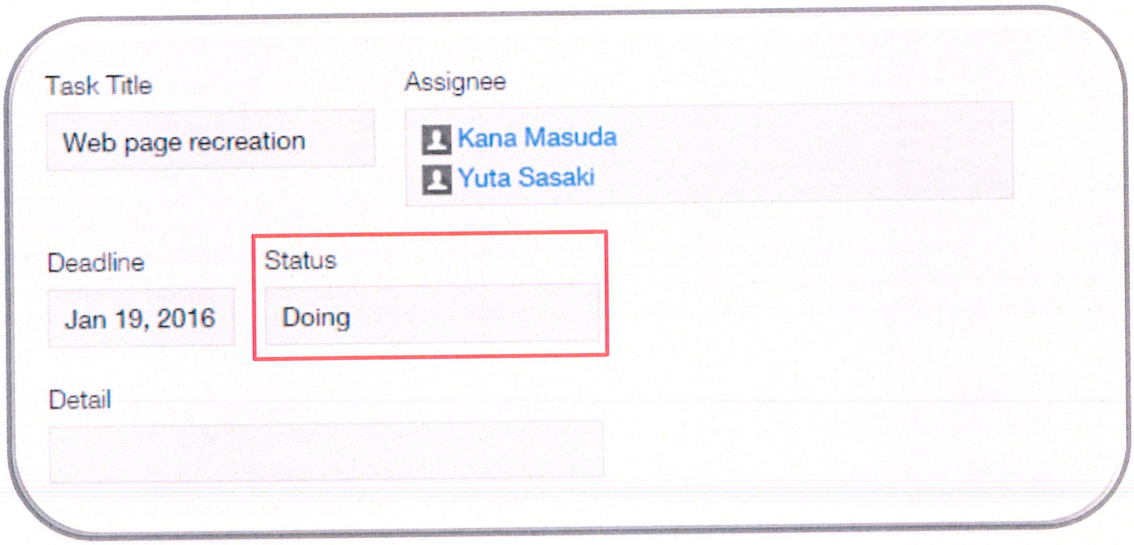


2. Check the revision history, and revert to an older version if necessary



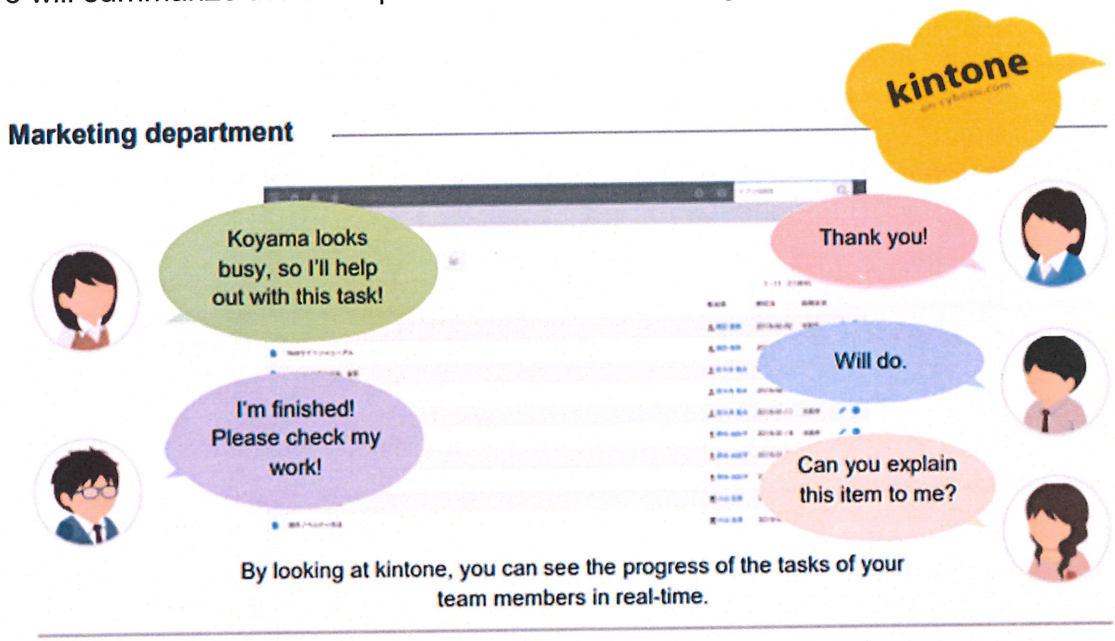
By clicking on the **"Show changes,"** highlighted red in the image to the left, the changed sections will be highlighted.

If you want to undo this change, click the **"Revert to the previous version"** Button below



Benefits of using kintone apps

The previous section covered the fundamental workflow for creating and using an app. Here, we will summarize the examples and benefits of using the app you created.



Improvement point 1 **You are now able to visualize the tasks of team members**

Until now, the team leader received reports and messages at meetings, but by registering with the app, it is now easier to see what tasks need to be taken care of, and which member has how many tasks.

Improvement point 2 **You are now able to prevent forgetting to carry out a task**

Tasks in our daily work that can be done quickly, but don't necessarily need to be taken care of right away, tending to be left for a later time. By registering the task with the app, you can prevent forgetting to carry out tasks.

Improvement point 3 **It's easier to communicate**

You can ask members to handle tasks by writing them down, as opposed to verbal communication. Not only can you prevent any miscommunications, but you can also communicate via kintone whenever you think of a new task, allowing for smoother communication within the team.



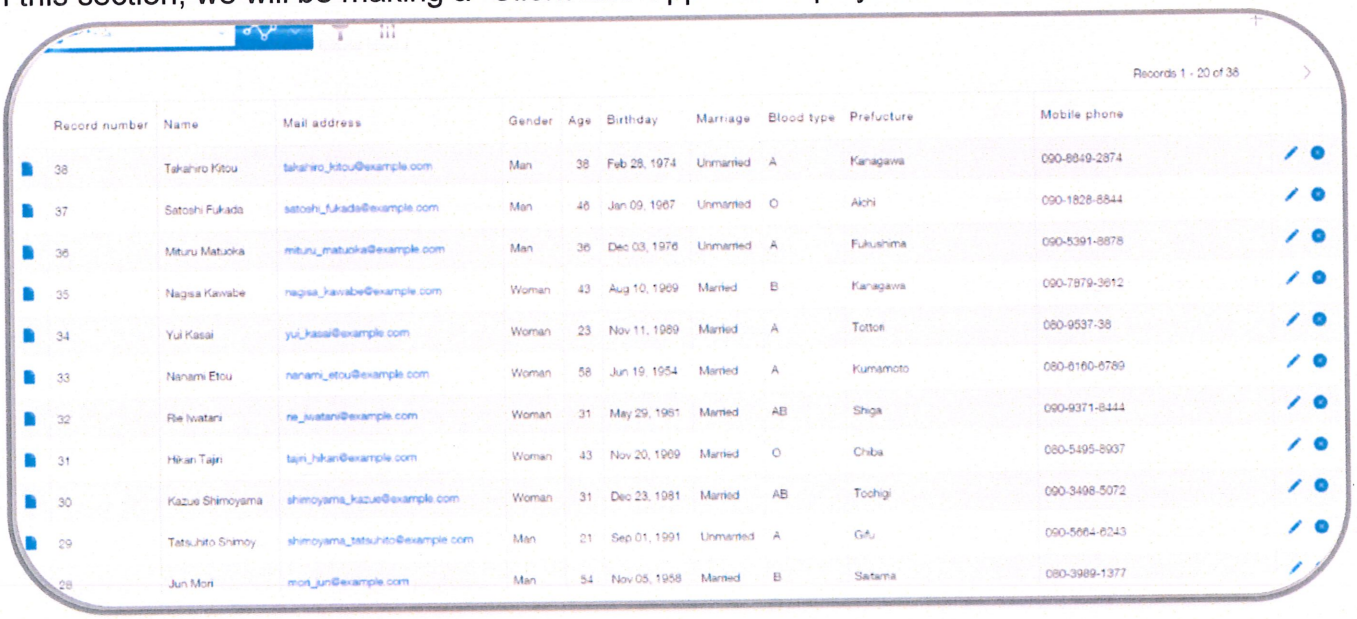
It's with an amazing service like kintone, you can resolve so many issues with an app that can be made in minutes!

Import Excel file and make an app

In addition to making an app from scratch by dragging and dropping, kintone users can import Excel files or use ready-made templates to create apps.

Our next app **Client list app**

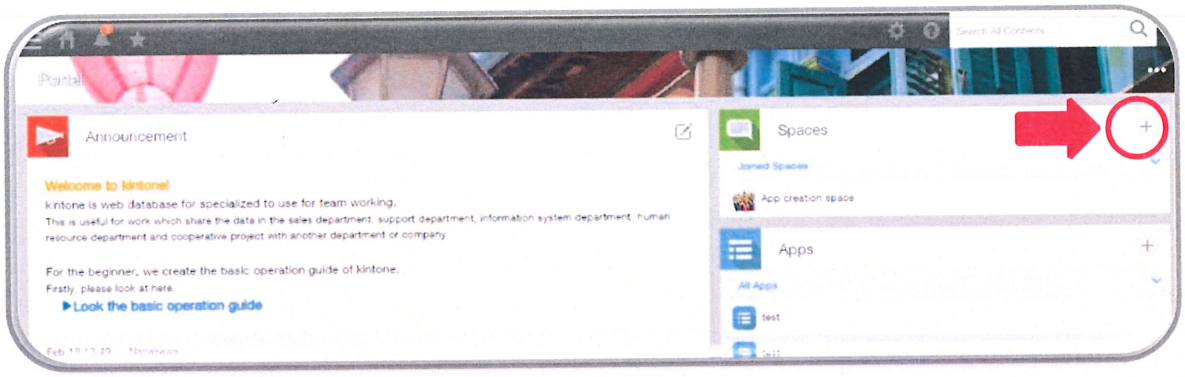
In this section, we will be making a "Client List" app that displays client information as a list.



Records 1 - 20 of 38

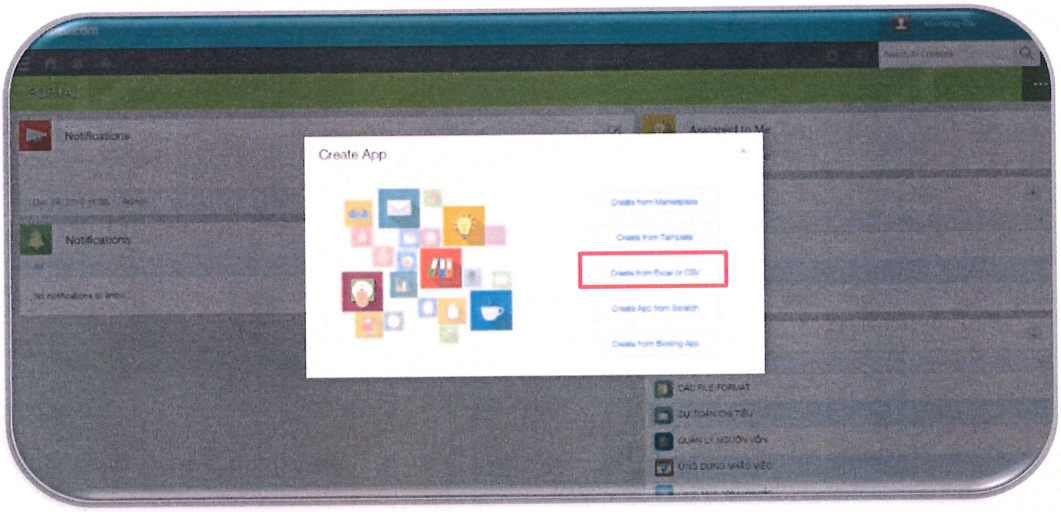
Record number	Name	Mail address	Gender	Age	Birthday	Marriage	Blood type	Prefecture	Mobile phone
38	Takahiro Kitou	takahiro_kitou@example.com	Man	38	Feb 28, 1974	Unmarried	A	Kanagawa	090-8849-2874
37	Satoshi Fukada	satoshi_fukada@example.com	Man	46	Jan 09, 1967	Unmarried	O	Aichi	090-1828-8844
36	Mituru Matuoka	mituru_matuoka@example.com	Man	36	Dec 03, 1976	Unmarried	A	Fukushima	090-5391-8878
35	Nagisa Kawabe	nagisa_kawabe@example.com	Woman	43	Aug 10, 1969	Married	B	Kanagawa	090-7879-3612
34	Yui Kasai	yui_kasai@example.com	Woman	23	Nov 11, 1989	Married	A	Tottori	080-9537-38
33	Nanami Etou	nanami_etou@example.com	Woman	58	Jun 19, 1954	Married	A	Kumamoto	080-6160-6789
32	Rie Iwatani	rie_iwatani@example.com	Woman	31	May 29, 1981	Married	AB	Shiga	090-9371-8444
31	Hikari Tajiri	tajiri_hikari@example.com	Woman	43	Nov 20, 1909	Married	O	Chiba	080-5495-8937
30	Kazue Shimoyama	shimoyama_kazue@example.com	Woman	31	Dec 23, 1981	Married	AB	Tochigi	090-3498-5072
29	Tatsuhito Shimoy	shimoyama_tatsuhito@example.com	Man	21	Sep 01, 1991	Unmarried	A	Gifu	090-5664-6243
28	Jun Mori	mori_jun@example.com	Man	54	Nov 05, 1958	Married	B	Saitama	080-3989-1377

1. **Click the "Create app" button, and move to the creation page**
   Click the + icon on the kintone portal page.



2. Select an app creation method

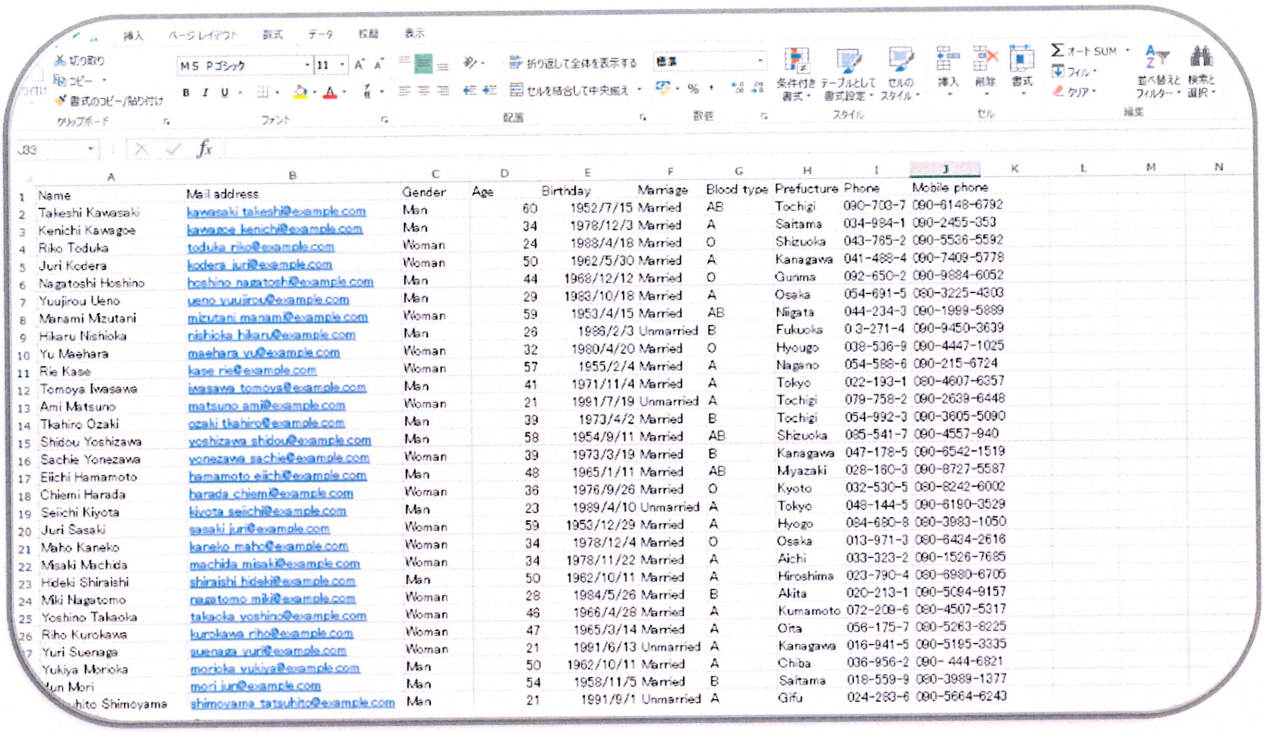
Here, we will select a method to create an app. In this example, we will select “Create from Excel/CSV,” located at the third from the top.



This time, we will be using the following Excel file to create an app.

Client names, gender, age, and other information is listed in this file.

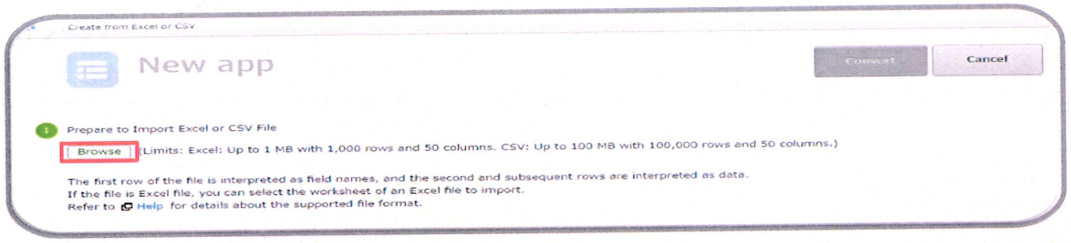
(In this example, we are using an Excel file, but you can also use CSV files.)



	A	B	C	D	E	F	G	H	I	J
1	Name	Mail address	Gender	Age	Birthday	Marriage	Blood type	Prefucture	Phone	Mobile phone
2	Takeshi Kawasaki	kawasaki takeshi@example.com	Man	60	1952/7/15	Married	AB	Tochigi	090-703-7	090-6148-6792
3	Kenichi Kawagoe	kawagoe kenichi@example.com	Man	34	1978/12/3	Married	A	Saitama	004-984-1	090-2455-353
4	Riko Toduka	toduka riko@example.com	Woman	24	1988/4/18	Married	O	Shizuoka	043-765-2	090-5536-5592
5	Juri Kodera	kodera juri@example.com	Woman	50	1962/5/30	Married	A	Kanagawa	041-488-4	090-7408-5778
6	Nagatoshi Hoshino	hoshino nagatoshi@example.com	Man	44	1968/12/12	Married	O	Gunma	092-650-2	090-9884-6052
7	Yuujirou Ueno	ueno yuujirou@example.com	Man	29	1983/10/18	Married	A	Osaka	054-691-5	080-3225-4303
8	Manami Mizutani	mizutani manami@example.com	Woman	59	1953/4/15	Married	AB	Niigata	044-234-3	090-1999-5889
9	Hikaru Nishioka	nishioka hikaru@example.com	Man	26	1988/2/3	Unmarried	B	Fukuoka	0 3-271-4	090-9450-3639
10	Yu Maehara	maehara yu@example.com	Woman	32	1980/4/20	Married	O	Hyougo	038-536-9	090-4447-1025
11	Rie Kase	kase rie@example.com	Woman	57	1955/2/4	Married	A	Nagano	054-588-6	090-215-6724
12	Tomoya Iwasawa	iwasawa tomoya@example.com	Man	41	1971/11/4	Married	A	Tokyo	022-193-1	080-4607-6357
13	Ami Matsuno	matsuno ami@example.com	Woman	21	1991/7/19	Unmarried	A	Tochigi	079-758-2	090-2638-6448
14	Tkahiro Ozaki	ozaki tkahiro@example.com	Man	39	1973/4/2	Married	B	Tochigi	054-992-3	090-3605-5090
15	Shidou Yoshizawa	yoshizawa shidou@example.com	Man	58	1954/9/11	Married	AB	Shizuoka	085-541-7	090-4557-940
16	Sachie Yonezawa	yonezawa sachie@example.com	Woman	39	1973/3/19	Married	B	Kanagawa	047-178-5	090-6542-1519
17	Eiichi Hamamoto	hamamoto eiichi@example.com	Man	48	1965/1/11	Married	AB	Miyazaki	028-180-3	090-8727-5587
18	Chiemi Harada	harada chiemi@example.com	Woman	36	1976/9/26	Married	O	Kyoto	032-530-5	080-8242-6002
19	Seiichi Kiyota	kiyota seiichi@example.com	Man	23	1989/4/10	Unmarried	A	Tokyo	048-144-5	090-6190-3529
20	Juri Sasaki	sasaki juri@example.com	Woman	59	1953/12/29	Married	A	Hyogo	084-680-8	080-3983-1050
21	Maho Kaneko	kaneko maho@example.com	Woman	34	1978/12/4	Married	O	Osaka	013-971-3	080-8434-2618
22	Misaki Machida	machida misaki@example.com	Woman	34	1978/11/22	Married	A	Aichi	033-323-2	090-1526-7685
23	Hideki Shiraishi	shiraishi hideki@example.com	Man	50	1962/10/11	Married	A	Hiroshima	023-790-4	090-6980-6705
24	Miki Nagatomo	nagatomo miki@example.com	Woman	28	1984/5/26	Married	B	Akita	020-213-1	090-5084-9157
25	Yoshino Takaoka	takaoka yoshino@example.com	Woman	46	1966/4/28	Married	A	Kumamoto	072-209-6	080-4507-5317
26	Riho Kurokawa	kurokawa riho@example.com	Woman	47	1965/3/14	Married	A	Oita	056-175-7	090-5263-8225
27	Yuri Suenaga	suenaga yuri@example.com	Woman	21	1991/6/13	Unmarried	A	Kanagawa	016-941-5	090-5185-3335
28	Yukiya Morioka	morioka yukiya@example.com	Man	50	1962/10/11	Married	A	Chiba	036-956-2	090- 444-6821
29	Jun Mori	mori jun@example.com	Man	54	1958/11/5	Married	B	Saitama	018-559-9	080-3989-1377
30	shito Shimoyama	shimoyama tatsuhito@example.com	Man	21	1991/9/1	Unmarried	A	Gifu	024-283-6	090-5664-6243

3. Click “File” to import an Excel file

When you click on the “File” button, a file selection screen will appear. Select the client information list file.

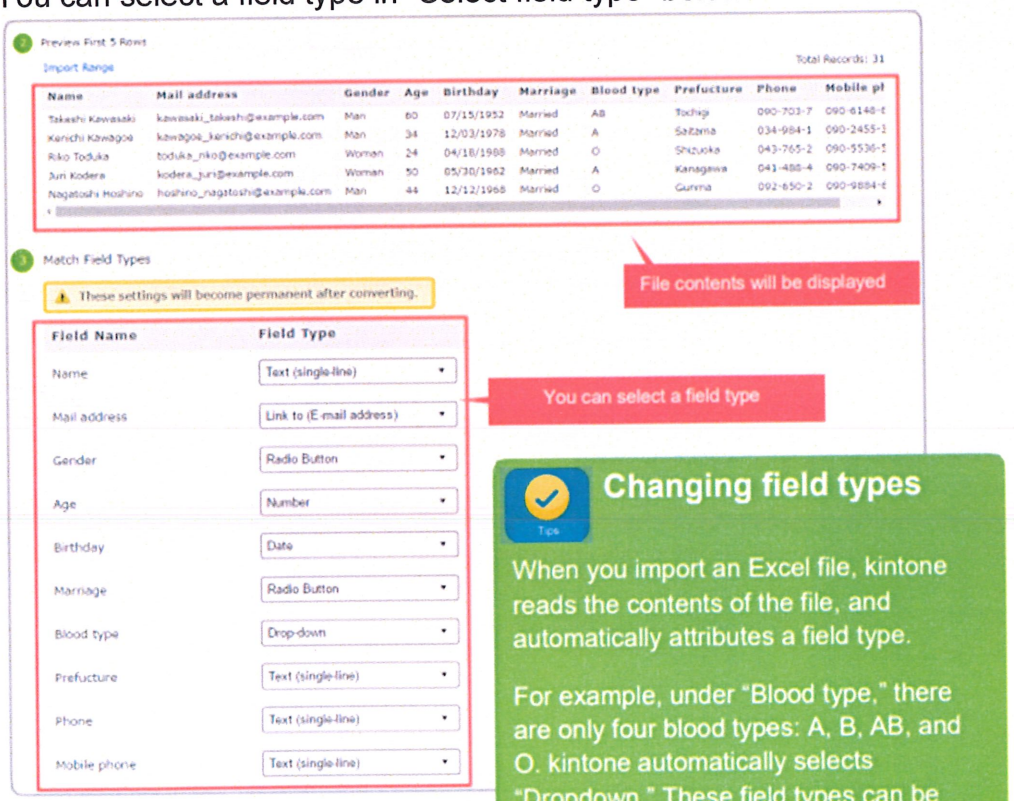


4. Check the contents of the imported file and the field type

A small section of the file is displayed under the “File contents” field.

The imported content should completely match the contents of the original Excel file.

You can select a field type in “Select field type” below.



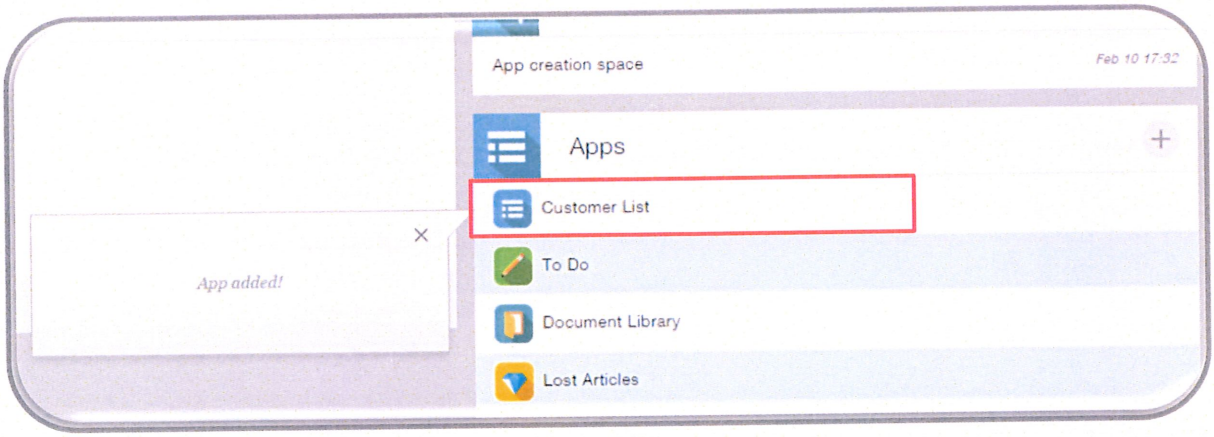
5. Click the "Create" button when you complete your settings

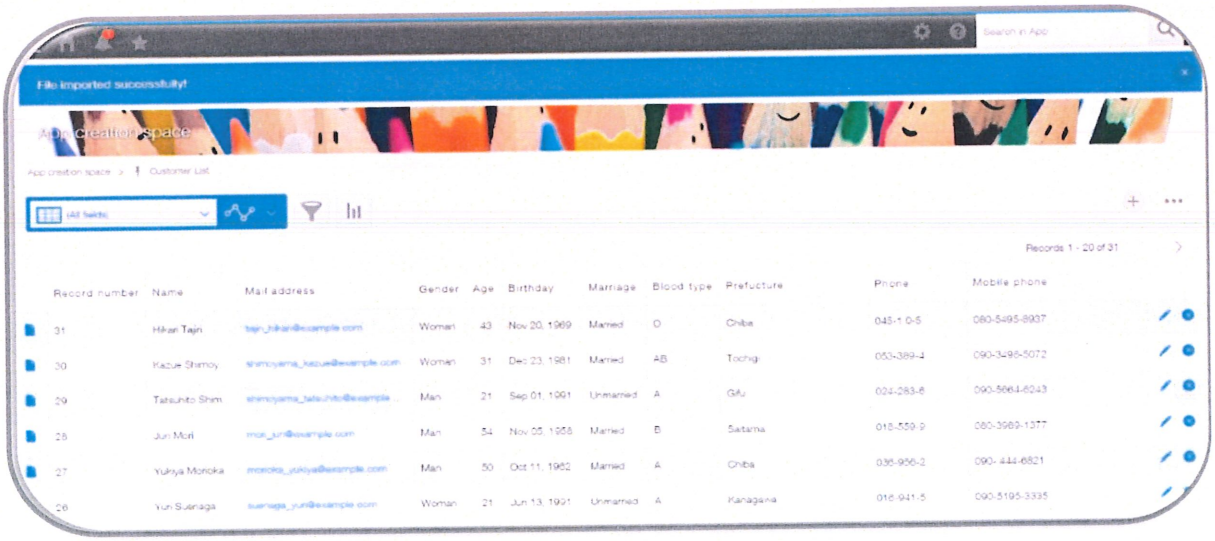
Once you have changed and set your settings, return to the top of the page and click [Create].



6. Finish creating an app from an Excel file

An icon for your newly created app will appear on the bottom right of the portal page. You have successfully created a kintone app using an imported Excel file.



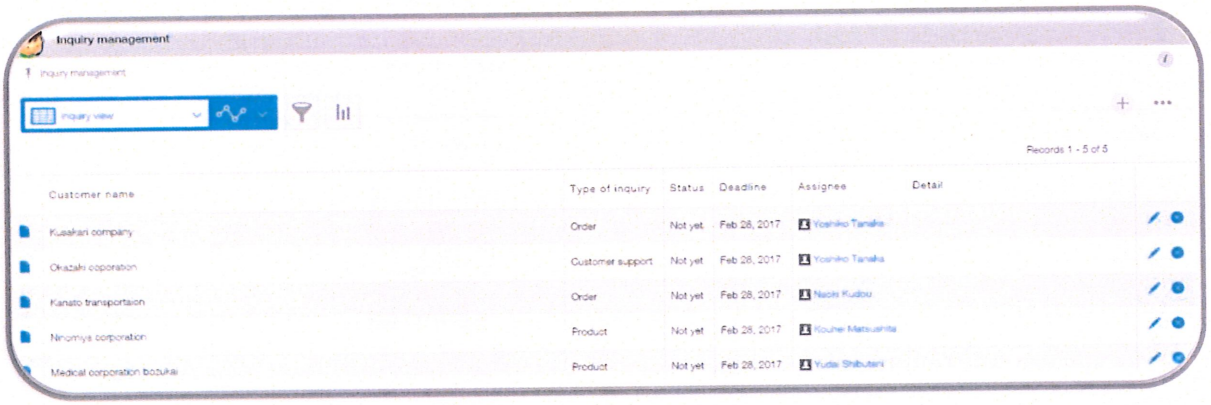


Adding from the app store

In addition to making an app from scratch by dragging and dropping, kintone users can import Excel files or use ready-made templates to create apps. In this section, we will show you how to create apps from templates available on the app store.

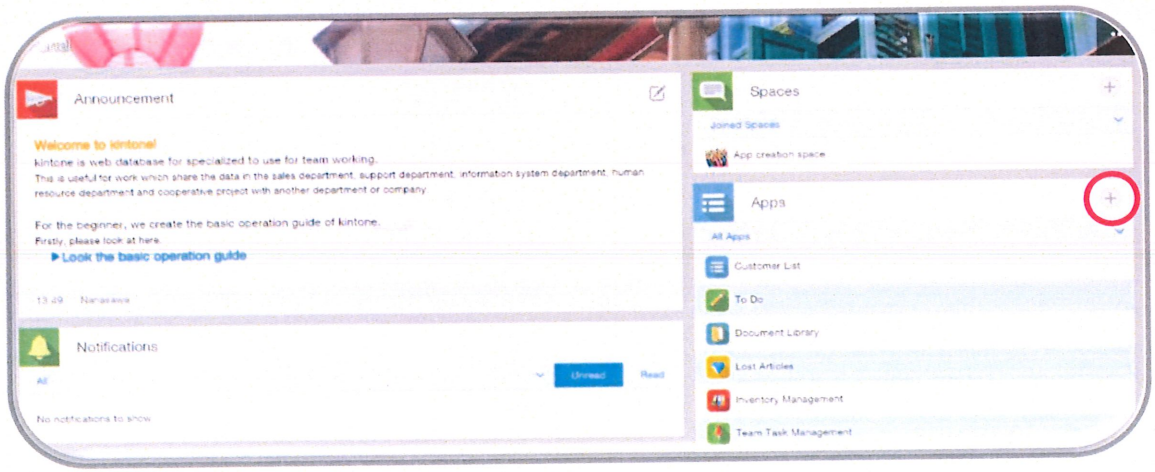
Our next app **Inquiry management app**

In addition to making an app from scratch by dragging and dropping, kintone users can import Excel files or use ready-made templates to create apps. In this section, we will show you how to create apps from templates available on the app store.



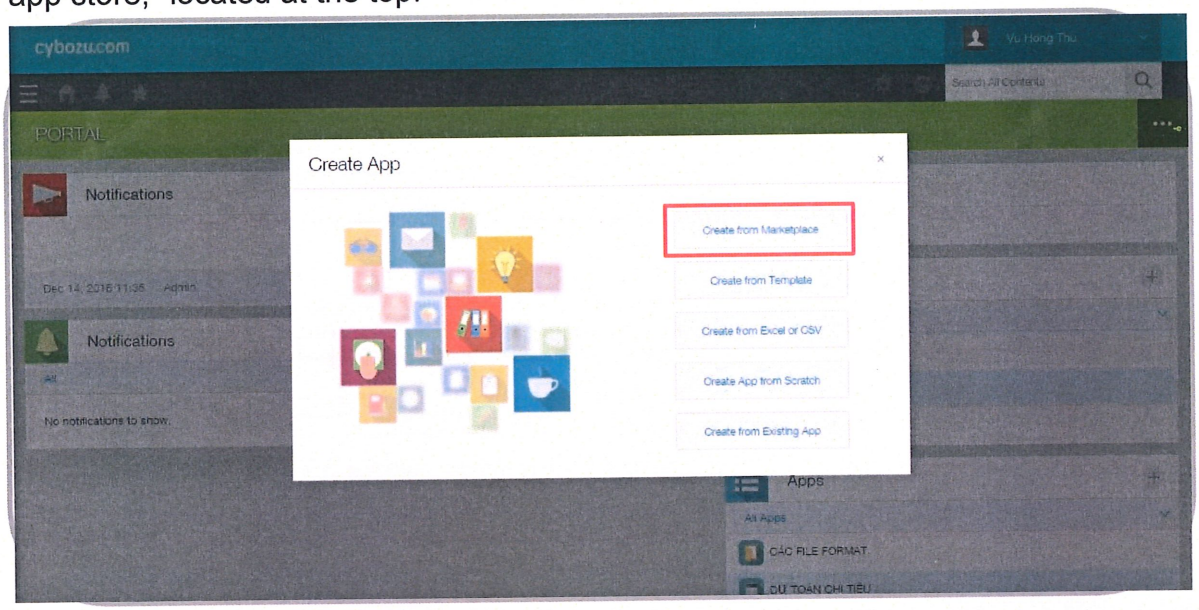
1. Click the "Create app" button, and move to the creation page

Click the + icon on the kintone portal page



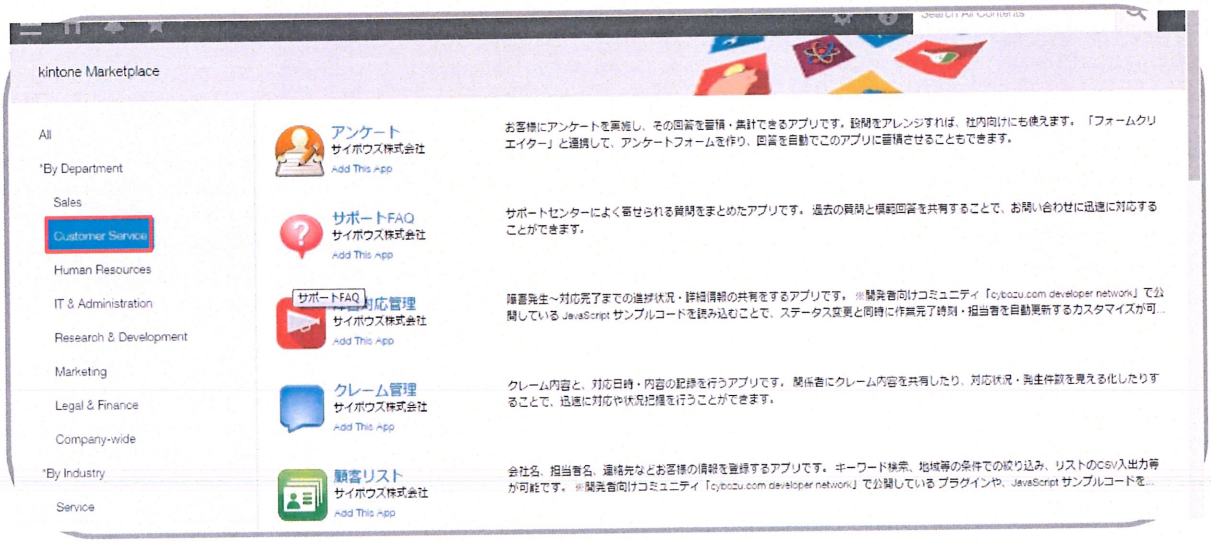
2. Select an app creation method

Here, we will select an app creation method. This time, we will select “Choose from the app store,” located at the top.



3. Select “Client services/support” from the app store category

The category located on the left side of the page shows recommended apps by department.



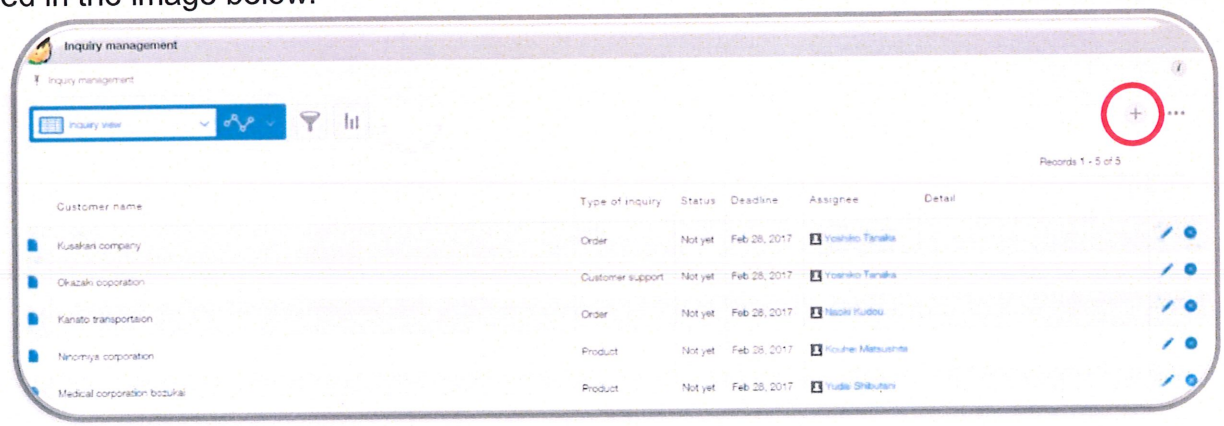
4. Click the “Add this app” button

When you find an app you want, click the “Add this app” button, located underneath the app title



5. Inquiry management app completed

You have successfully added an inquiry management app from the app store. The app will not have any data in it, so add new records from the + button, highlighted red in the image below.



Intermediate Level Section

～The freedom to customize for your task～

Make the most of kintone's useful features.

App customization ..... P32 ~ P35

Make a graph ..... P36 ~ P39

Other useful kintone features ..... Back cover



App customization

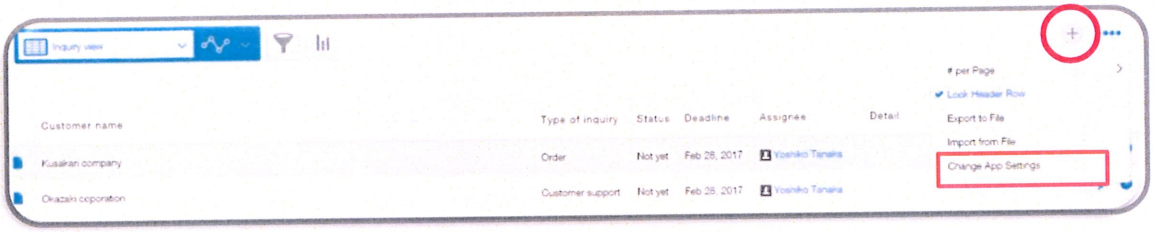
One of kintone's greatest unique features is that it allows anyone to easily create web apps and customize them. There are so many cases where as you use an app you created, you realize there are some forms you'd like to add. Since kintone lets you do everything from creation to customization without any programming skill, even if the app's creator transfers out or leaves their position, the app can be easily customized.

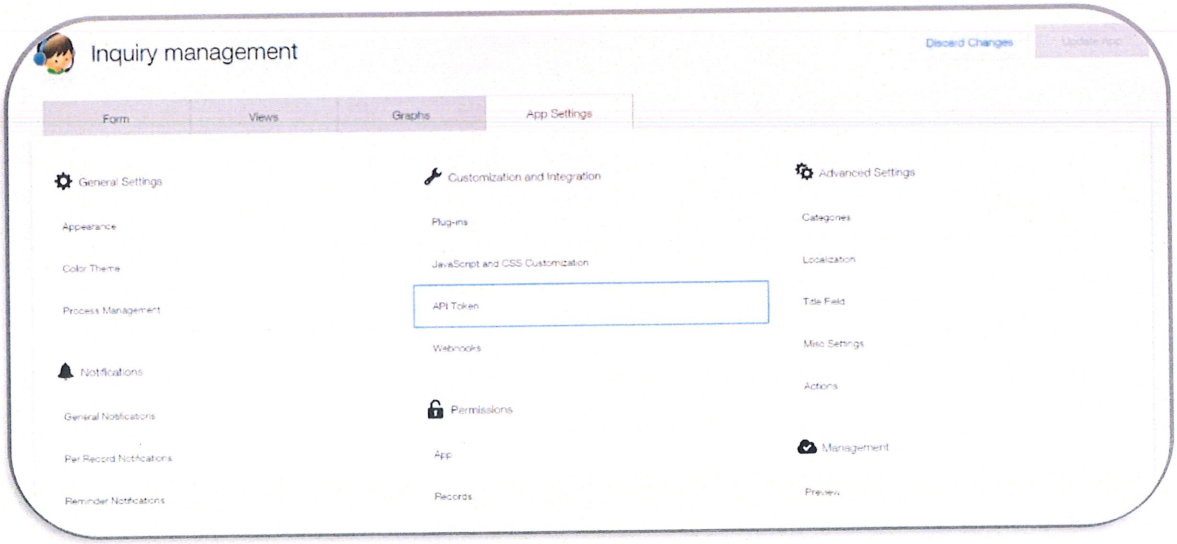
Basic customization (adding forms)

Let's start by introducing a basic customization method. This time, we'll try customizing the "inquiry management" app we downloaded from the app store on page 30.

1. Open the management page of the app

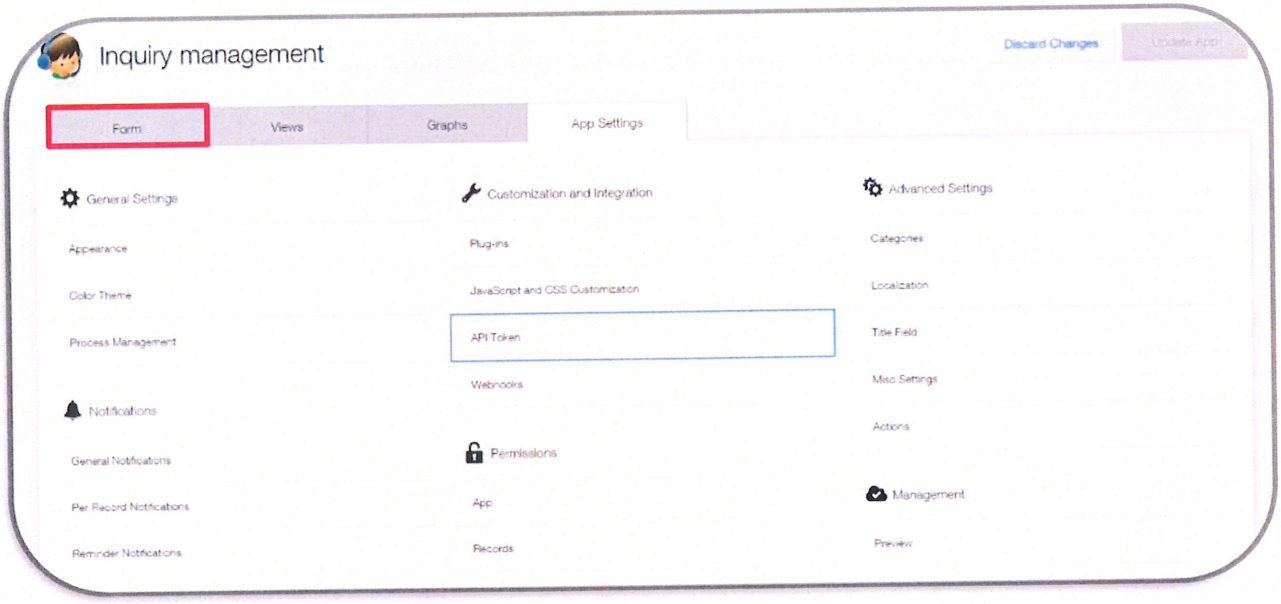
Open the "inquiry management" app, and click on the "..." mark on the upper right (circled in red below). Clicking here displays several menus, from which you'll select "change app settings." Doing this displays the management page for "inquiry management." (image 2). On this page, you can edit forms or add lists. You can even use the management page to change other settings such as adding graphs, assigning access permission, or setting notices.

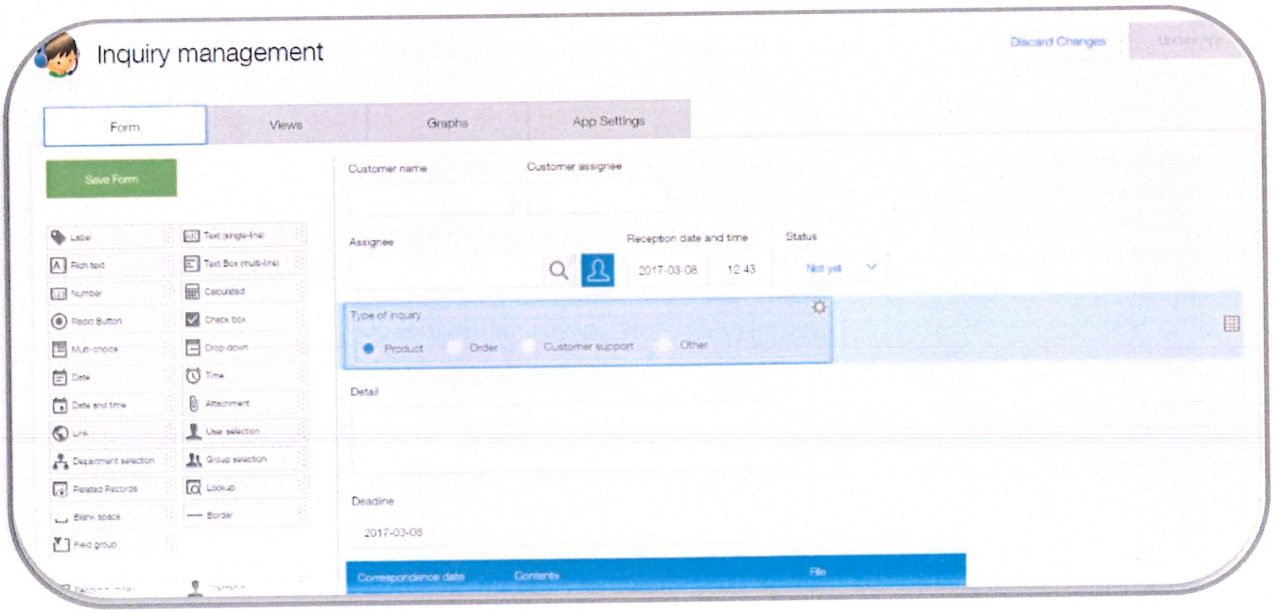




2. Select a form from the app's management page.

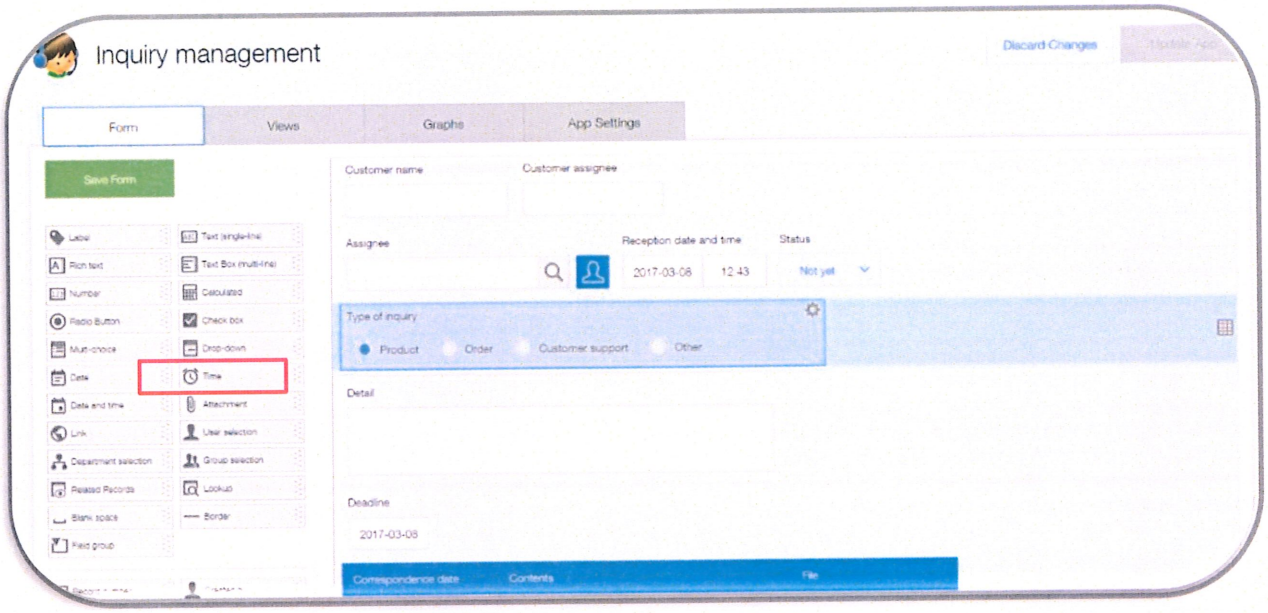
In this case, we'll edit a form.
By clicking the "form" tab highlighted in red below, the form edit page will be displayed. The methods for commands and settings are the same as for "Create an app from the beginning" (from page 5).



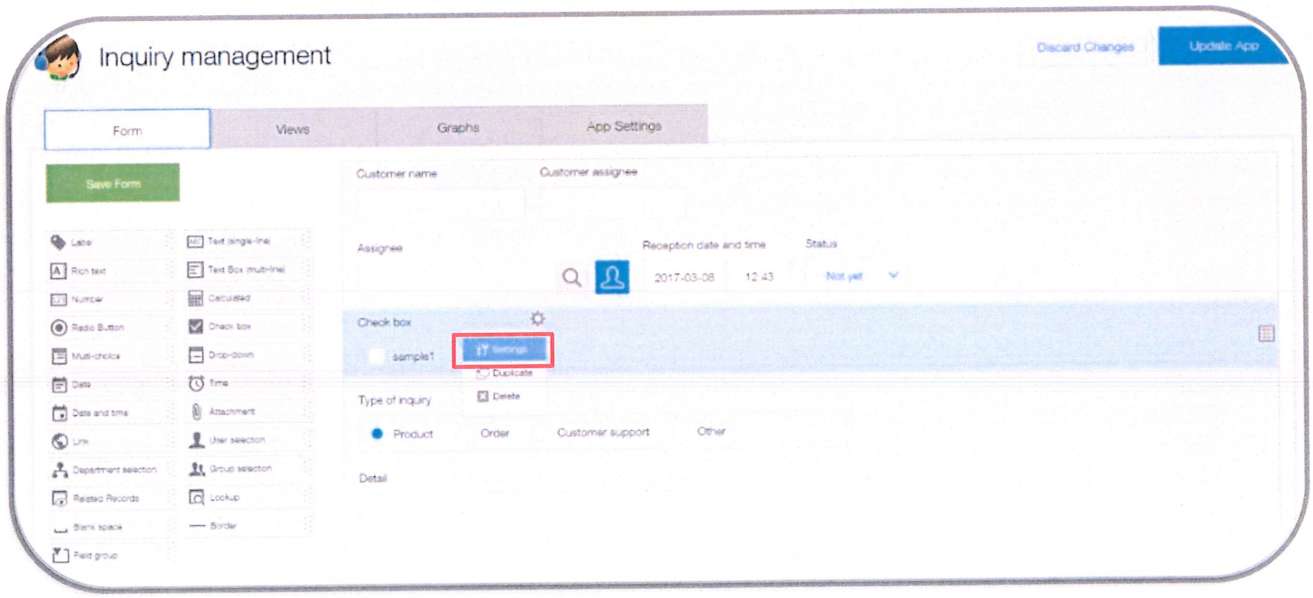


3. Edit (or add) a form.

Now, let's add the checkbox called "inquiry service." From the list of items on the left side, select Check box and drag it to the right.



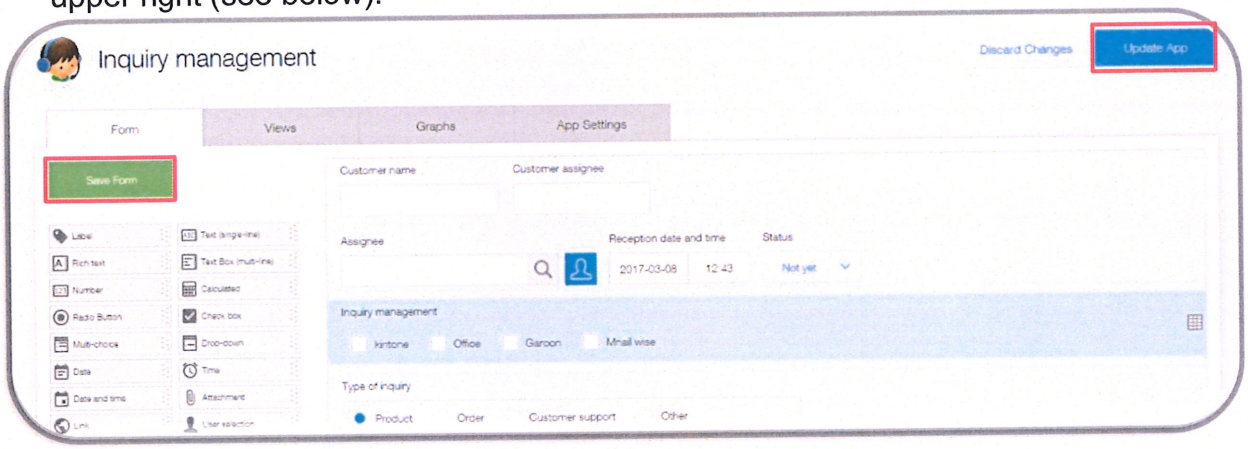
Placing the cursor on the ⚙ icon to the right of the checkbox displays the settings, so click on it.



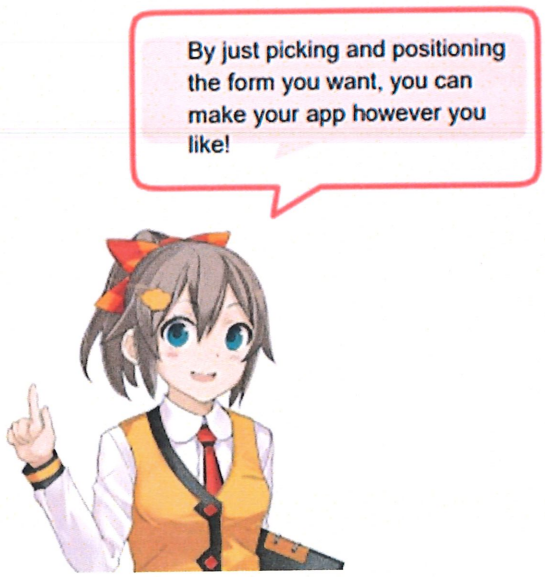


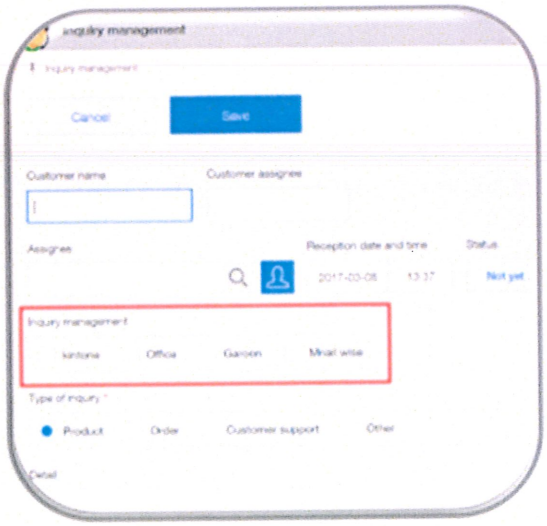
Input the field name, and then on the **"form and order"** column, enter the form of your choice, and click **"save."**

After clicking "**save form**" at the upper left of the form edit page, click "**update app**" at the upper right (see below).



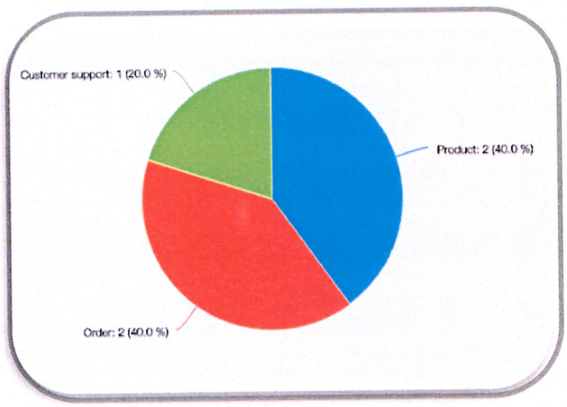
Clicking "update app" takes you back to the top page of the inquiry management app. Now, when you register a new record, the form you added (in this case, "inquiry service") will be included.





Make a graph

Apps made with kintone can be used not just for recording and storing information, but can also use the information to easily construct graphs and perform calculations. In this section, we'll explain how to make and utilize a graph.



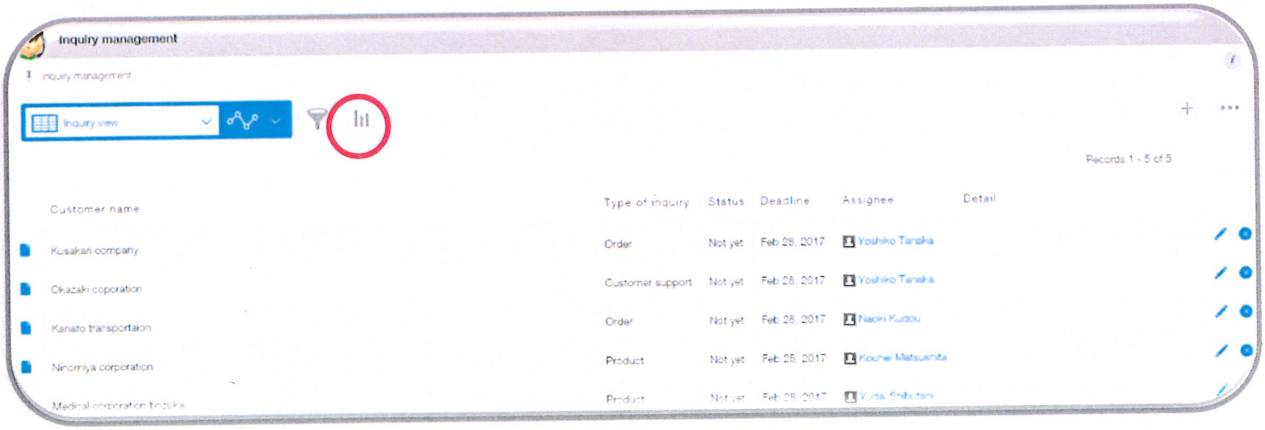


The "recommended graph" function lets you auto-generate a graph with one click.

There are two main methods to make a graph: setting the detailed calculation conditions manually, or analyze the registered data with kintone, displaying graphs for a variety of conditions automatically.
This feature to automatically generate a graph is called "recommended graph." We'll start by explaining how to set up recommended graph.

1. Open the app for which you'd like to make a graph.

Open an app made with kintone. In this case, we'll make a graph for the "**inquiry management**" app we constructed on page 31. Click on the [] mark shown in the image below.



2. Select the necessary graph from among the automatically generated graphs.
Graphs will be automatically generated for a variety of conditions.



When you find the graph you'd like to use, click on it.

This time, we'll use the **"record numbers (support conditions)"** pie graph.

The red space on the left side of the page below is the conditions for calculation of the graph. Changes to the calculation conditions are reflected in the preview on the right. If there's no particular need to change the calculation conditions, just click "**Apply.**"



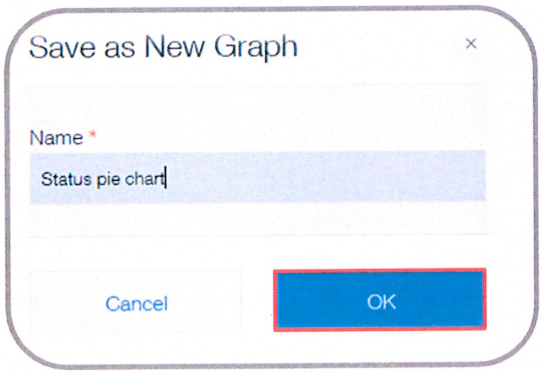
3. Save the graph

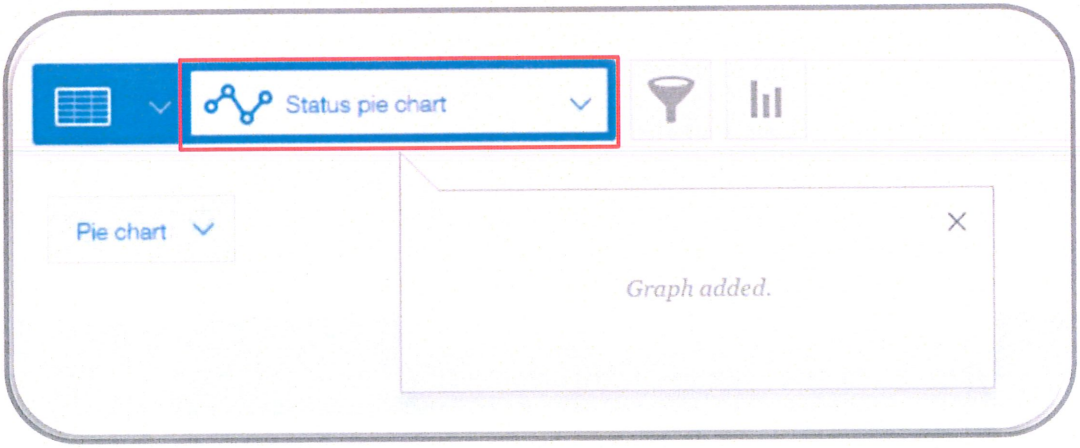
On the page for setting calculation conditions, clicking "**save**" on the lower right will save the graph calculated with those conditions. This feature is useful if you'd like to continually check the support conditions.



A dialog box is displayed, where you will input the optional graph name and click "**OK.**" This time, enter the name "**support conditions pie graph.**" When you do this, "support conditions pie graph" will be added to the pull-down "**graphs**" menu.

*If you downloaded the app from the app store, some graphs may be included with it from the start.

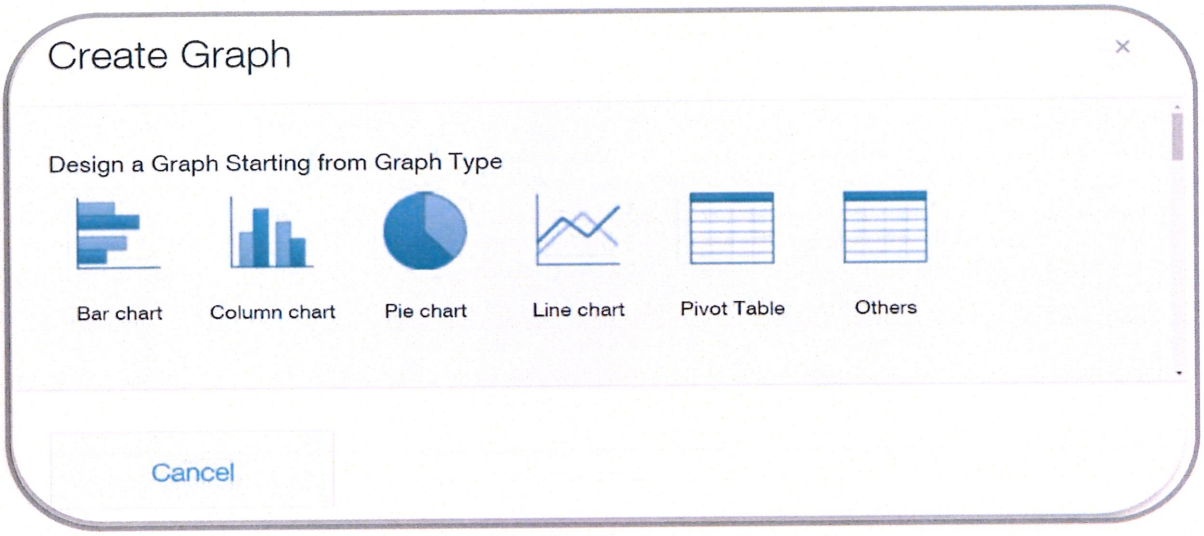




Next, we will explain how to set your own parameter to create a graph from scratch.

1. Select a graph type you want to create

First, Click the icon to display the graph creation screen.
select the type of graph you wish to create from “select graph type.”



This time, we will use a column chart to show unresolved inquiries per team member. Click “**column chart**” from the graph menu, and set the graph options.

Items that need to be categorized: The major item is set to “**Responsible personnel**,” with the conditions set to “**Status: Including one of the following: Unresolved**.” Doing so will enable you to visually grasp which staff member has how many unresolved cases. As you can see, you can quickly create any graph by setting the items and parameters.



Other useful functions in kintone

There are many more useful functions in kintone, which all can be extremely helpful in using several apps. This section shows a few examples of these functions.

Access rights

You can set detailed access rights such as per app, per record, or per field.

For example, you can flexibly set the access rights to meet your demands, such as setting the access rights so all employees can see client information, but the information is only editable by the sales department, or hide personal information, such as names and E-mail addresses, from partial users.

▼How to set access rights

https://help.cybozu.com/ja/k/user/app_rights.html

Lookup

If you set up the lookup function, you can acquire information in other apps and register them. For example, if you connect information from the client management app, such as company names, representative names, addresses, phone numbers, and E-mail addresses with the sales department's project management app, you can acquire and register the information straight from the client management app. Not only can you save the time required to re-enter all the information, you can also prevent errors.

▼ How to set up lookup

https://help.cybozu.com/ja/k/user/whats_lookup.html

Notifications

You can set up notifications to be sent to all users when records have been edited, or when comments have been given to records. Additionally, kintone apps also have a feature that sends a notification when records satisfy a specific condition. For example, you can set notifications to be sent out to users a day before deadlines as a reminder.

▼How to set notifications and reminders

https://help.cybozu.com/ja/k/user/notification.html

Process management

The process management function helps manage business processes so that they comply with business rules. You can set processes and person in charge per task on the app. Not only can you visualize individual task status, but also because the data will be shown as a graph, you can grasp the progress of all duties in real-time.

▼How to set up process management

https://help.cybozu.com/ja/k/user/process.html

For other details about using kintone, please check the user help.

ผู้อนุมัติ

ลงชื่อ วรวุฒิ เทพทัสดิน ฯ

(วรวุฒิ เทพทัสดิน ณ อยุธยา)

ผู้รับผิดชอบ

วันที่ 25/03/65

ลงชื่อ ธนิตร ธนวงศ์เกษม

(ธนิตร ธนวงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 25/03/65

ขั้นตอนการแจ้งปัญหาด้านระบบ

วัตถุประสงค์ เพื่อเป็นการบริการตอบสนองต่อผู้แจ้งปัญหาให้เป็นไปอย่างมีระบบ เป็นขั้นเป็นตอน และปรับปรุงเพื่อสร้างความพึงพอใจสูงสุดให้กับผู้แจ้ง รวมทั้งการติดตามงานก่อนและหลังการแก้ปัญหา โดยมีขั้นตอนดังนี้

ขั้นตอนการแจ้ง

1. ผู้แจ้งจะแจ้งปัญหาไม่ว่าจะเป็นการโทร/แชท/ผ่านระบบ มายัง IT Support
2. เจ้าหน้าที่ IT Support ผู้ดูแล รับทราบรายละเอียด แล้วบันทึกลงในระบบ IT Support แล้วดำเนินการ
   2.1. หากพิจารณาแล้ว สามารถแก้ไขได้ ก็ดำเนินการแก้ไข
   2.2. หากพิจารณาแล้ว ไม่สามารถแก้ไขได้ทันที หรือใช้เวลานาน จะส่งงานให้เจ้าหน้าที่ IT Support ไป Onsite หรือ Remote ไปช่วยแก้ไขปัญหา
3. เมื่อเจ้าหน้าที่ IT Support ทำหน้าที่แก้ปัญหา
   3.1. แก้ปัญหาไม่ได้ เพราะต้องใช้เวลา หรือต้องหาอุปกรณ์มาทดแทน ระบบก็ยังเปิดอยู่เพื่อให้เจ้าหน้าที่ IT Support ท่านอื่นมารับงานต่อได้
   3.2. แก้ปัญหาได้ ก็จะบันทึก และปิดเคส แจ้งไปยังผู้แจ้งด้วย

ขั้นตอนการวิเคราะห์ และปรับปรุงการบริการให้ได้ความพึงพอใจสูงสุด

1. เจ้าหน้าที่ IT Support นำข้อมูลที่ได้บันทึกไว้ในระบบ มาวิเคราะห์ทำเป็นกราฟ มาเสนอผู้บริหารและเจ้าหน้าที่ IT ทุกคน ร่วมกันวิเคราะห์ เสนอความคิดเห็น เพื่อปรับปรุงให้ปัญหาลดน้อยลง ในการประชุมประจำเดือน ซึ่งประกอบด้วยข้อมูลที่แบ่งได้ดังต่อไปนี้
   1.1. เป็นเรื่อง Hardware หรือ Software
      1.1.1. แบ่งเรื่อง Hardware ออกเป็นเรื่องย่อย ได้แก่ PC, Notebook, Tablet เป็นต้น
      1.1.2. แบ่งเรื่อง Software ออกเป็นเรื่อง Software ระบบ กับ Software ทั่วไป
   1.2. รายงานผลจำนวนครั้งที่แจ้งทั้งหมดเปรียบเทียบเป็นรายเดือนทุกเดือนตั้งแต่ มกราคม ถึง ธันวาคม
   1.3. รายงานจำนวนการแจ้งเป็นจำนวนครั้งในรายละเอียดที่เป็นเรื่องย่อยเรียงลำดับเรื่องมากมายังน้อย
      1.3.1. ให้ทำพิจารณาเรื่องที่แจ้งปัญหาสูง 3 อันดับแรก มาวิเคราะห์ แล้วหาแนวทางเพื่อปรับปรุงเพื่อทำให้เรื่องลดน้อยลง หรือ เพิ่มประสิทธิภาพมากยิ่งขึ้น
2. หัวหน้าฝ่ายหรือผู้บริหารระดับสูง ลงนามรับทราบในใบรายงานการแจ้งปัญหาของเจ้าหน้าที่ IT Support

ผู้อนุมัติ

ลงชื่อ ชัยพร ธนวงศ์เกษม

(ชัยพร ธนวงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 25/03/65

ลงชื่อ กร ธ

(น.ส กร ธรรมมาพณิชย์)

ผู้รับผิดชอบ

วันที่ 25/03/65

ขั้นตอนการคัดเลือกผู้ให้บริการภายนอก

วัตถุประสงค์ เพื่อเป็นการได้รับการบริการจากผู้ให้บริการที่มีคุณสมบัติได้ตามมาตรฐาน โดยอาศัยหลักการมีคุณภาพ และประสิทธิภาพ ให้เกิดความพึงพอใจสูงสุด เหมาะสมกับการลงทุนที่ได้ลงทุนไป โดยมีขั้นตอนดังนี้

ขั้นตอนการการคัดเลือกและเก็บประวัติผู้ขาย/ผู้รับจ้าง/ผู้ให้บริการ

1. กำหนดคุณสมบัติและคัดเลือกผู้ขาย/ผู้จ้าง/ผู้ให้บริการ
   1.1. กำหนดคุณสมบัติของงานแต่ละประเภทในรายละเอียดให้ชัดเจนครบถ้วน เช่น ต้องการบริษัทผู้ให้บริการเรื่อง Clouding System ควรกำหนดว่าบริษัทจำเป็นต้องมีคุณสมบัติอย่างไร มีประสบการณ์ในการทำงานอย่างไร เป็นเวลาเท่าไร มีฐานะทางการเงินอย่างไร เพื่อใช้เป็นกฎเกณฑ์ในการคัดเลือกผู้มีคุณสมบัติตามที่ต้องการ
   1.2. กำหนดกรอบวิธีการคัดเลือกผู้ขาย/ผู้จ้าง/ผู้ให้บริการที่มีคุณสมบัติตามต้องการ เพื่อสร้างเป็นทะเบียนรายชื่อผู้ขาย/ผู้จ้าง/ผู้ให้บริการ ที่มีคุณสมบัติเหมาะสมและได้การยอมรับแล้ว
2. ประเมินผลงานผู้ขาย/ผู้จ้าง/ผู้ให้บริการ
   2.1. การประเมินผลงานผู้ขาย/ผู้จ้าง/ผู้ให้บริการ เพื่อให้มั่นใจว่าจะได้รับสินค้าและการบริการที่ดี มีคุณภาพอย่างต่อเนื่อง และจะมีการปรับปรุงฐานข้อมูล ผู้ขาย/ผู้จ้าง/ผู้ให้บริการ ที่ทันสมัยอยู่เสมอ

ขั้นตอนการดำเนินการจัดซื้อจัดจ้าง

1. การจัดทำ TOR (Term Of Reference) และขออนุมัติ
   1.1. กระบวนการจัดทำ TOR และขออนุมัติเป็นกระบวนการเพื่อแสดงขั้นตอนตั้งแต่การกำหนดผู้เกี่ยวข้อง หรือการขออนุมัติแต่งตั้งคณะกรรมการร่างเอกสาร TOR
   1.2. การจัดทำเอกสารข้อกำหนดคุณสมบัติขั้นต่ำ (Term Of Reference)
   1.3. การตรวจสอบความถูกต้องของเอกสาร
   1.4. การแจ้งผลการอนุมัติให้ผู้เกี่ยวข้องในการจัดซื้อ/จัดจ้าง/เช่าในแต่ละครั้งทราบ
2. การคัดเลือกและทำสัญญา
   2.1. กระบวนการคัดเลือก และทำสัญญาเป็นกระบวนการหลังจากที่ได้ร่างข้อกำหนดคุณสมบัติ (TOR) และ/หรือ Specification แล้ว โดยมีหลักเกณฑ์หลักๆ ดังนี้
      2.1.1. พิจารณาความมีชื่อเสียงบริษัทหรือหน่วยงานหรือเจ้าหน้าที่

2.1.2. ประสบการณ์การทำงาน หรือ หน่วยงานอ้างอิง

2.1.3. Certification หรือ ใบรับรองแสดงถึงความเป็นมืออาชีพ

2.1.4. ระยะเวลาที่ประกอบอาชีพ หรือ ทำงานมา

2.1.5. เป็นต้น

2.2. สำหรับการจัดซื้อจัดจ้างและได้รับการอนุมัติให้จัดซื้อจัดจ้างเรียบร้อยแล้ว จะเข้าสู่กระบวนการคัดเลือกผู้ขาย/ผู้จ้าง/ผู้ให้บริการจนถึงทำสัญญาจ้าง

2.3. บริษัทจะทำการเลือกจาก ผู้ขาย/ผู้จ้าง/ผู้ให้บริการไม่ต่ำกว่า 2 รายเสมอ

2.4. หากคุณสมบัติขั้นต่ำผ่านทั้ง 2 ราย จะทำการคัดเลือกจากราคาที่ต่ำกว่า

3. การตรวจรับงาน

3.1. กระบวนการตรวจรับเป็นกระบวนการจากเมื่อผู้ขาย/ผู้จ้าง/ผู้ให้บริการ ได้ส่งมอบสินค้าหรือบริการเรียบร้อยแล้ว จะต้องมีขั้นตอนการตรวจรับงานเพื่อให้ได้รับงานที่ถูกต้องและตรงกับ TOR

3.2. มีการทดลอง ทดสอบในกรณีที่เป็นอุปกรณ์ เครื่องใช้คอมพิวเตอร์ต่างๆ

3.3. นำไปใช้จริง

ผู้อนุมัติ

ลงชื่อ วรวุฒิ เทพทัสดิน ฯ

(วรวุฒิ เทพทัสดิน ณ อยุธยา)

ผู้รับผิดชอบ

วันที่ 25 มี.ค 65

ลงชื่อ ธนิตร อนวงศ์เกษม

(ธนิตร อนวงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 25 มี.ค. 65

ขั้นตอนการสำรองข้อมูลและกู้คืนระบบ DBC (Dynamics 365 Business Central)

วัตถุประสงค์ เพื่อให้การบริการระบบสารสนเทศเป็นไปอย่างต่อเนื่อง จึงกำหนดให้ฝ่ายสารสนเทศต้องมีการทดสอบการสำรองข้อมูลของระบบ DBC ใน Cloud Storage สามารถนำขึ้นใช้งานได้จริง ในกรณีที่มีระบบปฏิบัติการหลักล้มเหลว

ข้อกำหนดการสำรองข้อมูล

- สำหรับสถานที่การ Backup จะอยู่ที่ Data Center ของ Microsoft ซึ่งจะถูกเก็บไว้ในส่วนของ Data Center ซึ่งจะมีการกระจายเก็บสำรองข้อมูลระหว่าง Server ด้วยเช่นกัน
  รายละเอียดเพิ่มเติมเกี่ยวกับการทำ Backup ที่ Microsoft แจ้งไว้ จะเป็นไปตาม Link ด้านล่างนี้
  https://docs.microsoft.com/en-us/azure/azure-sql/database/automated-backups-overview?tabs=single-database
- การ Backup จะอยู่ในเงื่อนไขการให้บริการ รายละเอียดเพิ่มเติมตาม Link ด้านล่างนี้
  https://docs.microsoft.com/en-us/dynamics365/business-central/compliance/compliance-service-compliance#service-terms
- ความถี่ด้านการ Backup ต่างๆ ที่แตกต่างกัน เช่น Full backup จะทำงานทุกๆ 1 Week, Differential backups ทำงานทุกๆ 12-24 ชั่วโมง และ Transaction log backups ทำงานทุกๆ 5 - 10 นาที
  รายละเอียดเพิ่มเติม ตาม Link ด้านล่างนี้
  https://docs.microsoft.com/en-us/azure/azure-sql/database/automated-backups-overview?tabs=single-database#what-is-a-database-backup

การสำรองข้อมูล กำหนดให้มีการสำรองข้อมูลของระบบงาน DBC โดยมีการสำรองข้อมูล ดังนี้

1. ระบบ Backup จะทำงานอัตโนมัติ เพื่อป้องกันข้อมูลสูญหาย โดยสามารถ Restore ย้อนหลังได้สูงสุด 28 วัน โดยมีรายละเอียดข้อมูลเพิ่มเติมจาก Link ด้านล่างนี้

   https://docs.microsoft.com/en-us/dynamics365/business-central/dev-itpro/faq#how-often-are-production-databases-backed-up

2. ระบบ Backup จะไม่มี Process บอกว่า Backup สถานะสำเร็จหรือไม่ เนื่องจากเป็นระบบคล้ายกับ Versioning ที่จะถูก Backup ทุกครั้งที่มีการเปลี่ยนแปลงข้อมูล และถูกจัดการโดย Microsoft เป็นหลักเท่านั้น ตาม Link การอธิบายในข้อที่ 1

3. หากต้องการ Backup ข้อมูลย้อนหลังมากกว่า 28 วัน จะต้องใช้วิธีการ Export backup จากระบบ และนำไปเก็บไว้ในเครื่องอื่น หรือเปิดใช้งานผ่าน Azure storage account โดยสามารถดูคู่มือเพิ่มเติมได้ตาม Link ด้านล่างนี้ครับ
   https://docs.microsoft.com/en-us/dynamics365/business-central/dev-itpro/administration/tenant-admin-center-database-export#creating-the-database-export

การกู้คืนข้อมูล กำหนดให้มีการสำรองข้อมูลของระบบงาน DBC โดยมีการกู้คืนข้อมูล ดังนี้

1. การ restore ดูรายละเอียดขั้นตอนการทำทดสอบตามคลิป Video นี้
   https://ubizsolution0-my.sharepoint.com/:v:/g/personal/ubizdemo1_ubizsolution_com/EcPQLvZ0AdNCuIzpU-IOPkQBfJ3QsoWDErYIrcwyA8J8ng?e=KOcwCT

ตัวอย่างการทดสอบและผลการทดสอบ

IT-Procedure-033
(BDC Testing).docx

ผู้อนุมัติ

ลงชื่อ เณ็ฐธิดา สิงห์คง

(น.ส. เณ็ฐธิดา สิงห์คง)

ผู้รับผิดชอบ

วันที่ 25 มี.ค 65

ลงชื่อ ธนภร ธนวงศ์เกษม

(ธนภร ธนวงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

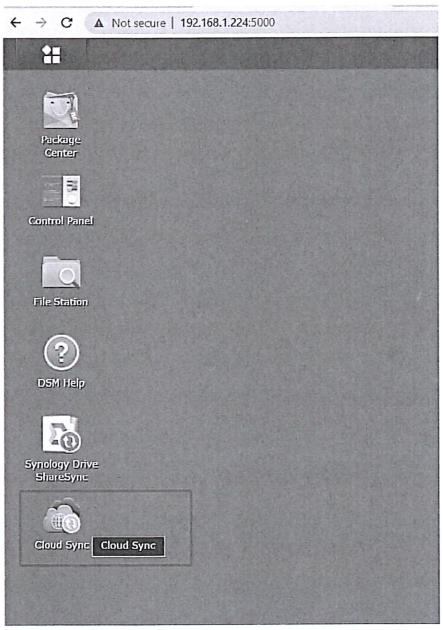
วันที่ 25 มี.ค. 65

ขั้นตอนการสำรองข้อมูลและกู้คืน NAS

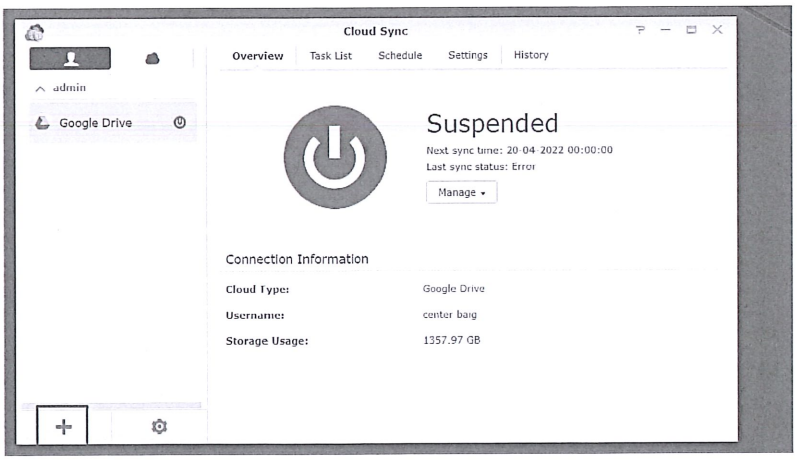
วัตถุประสงค์ เพื่อให้การบริการระบบสารสนเทศเป็นไปอย่างต่อเนื่อง จึงกำหนดให้ฝ่ายสารสนเทศต้องมีการทดสอบการสำรองข้อมูลใน NAS ที่สำรองไว้ใน Cloud Storage สามารถนำขึ้นใช้งานได้จริง ในกรณีที่มีระบบปฏิบัติการหลักล้มเหลว

วิธี Backup NAS

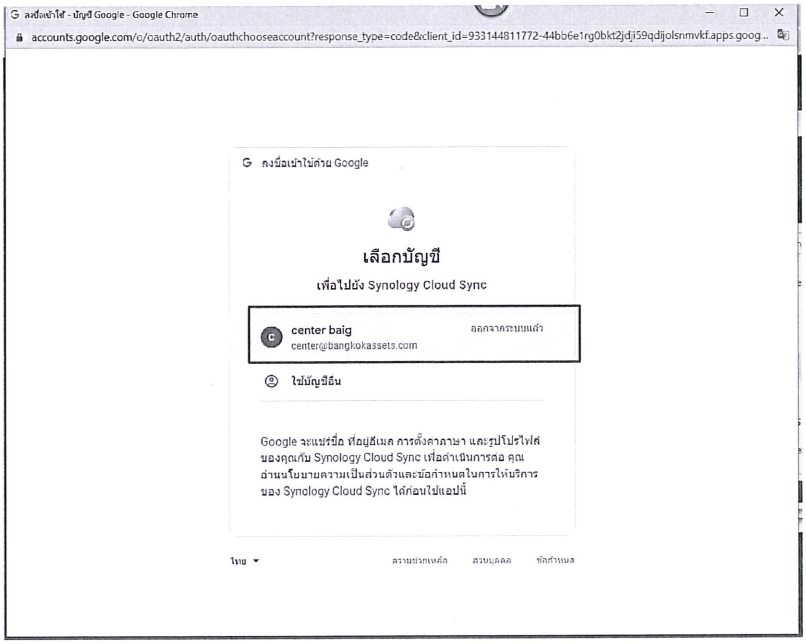
1. เปิด Browser พิมพ์ 192.168.10.224:5000
2. ไปที่ Cloud Sync



3. กดเครื่องหมาย + เพื่อเพิ่มการเชื่อมต่อไปยัง Cloud ที่ต้องการ



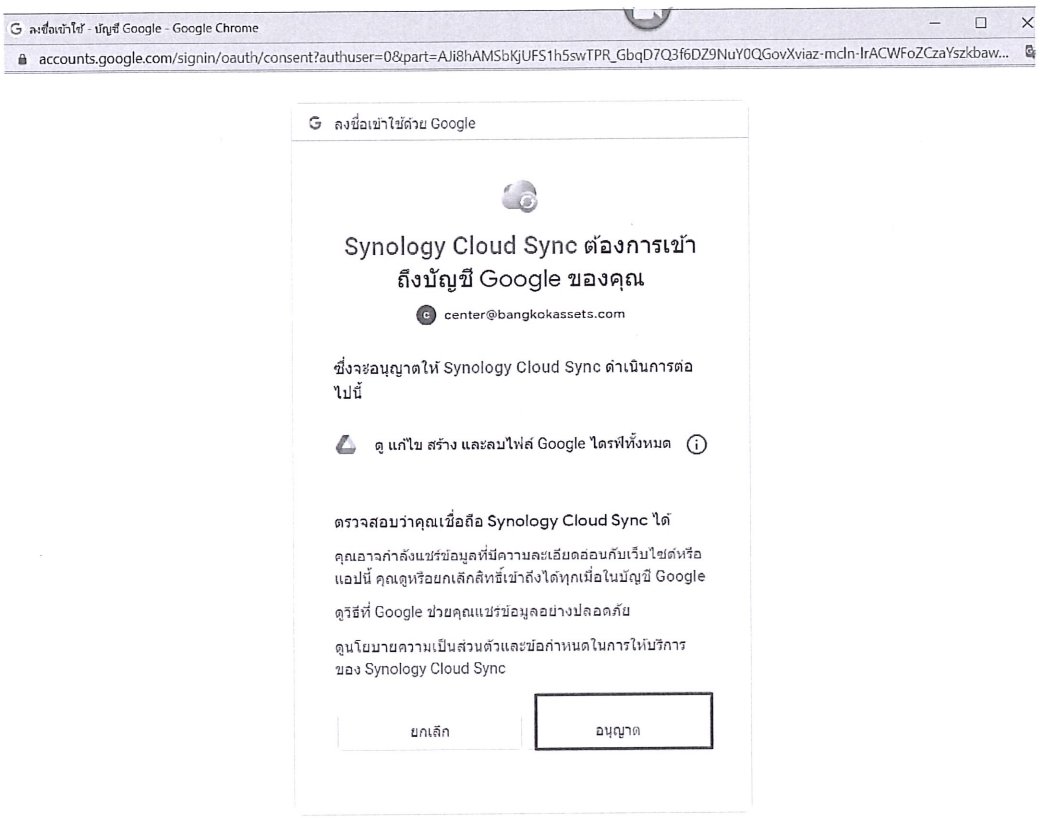
4. กรอก EMAIL เพื่อ login เข้าระบบ Cloud



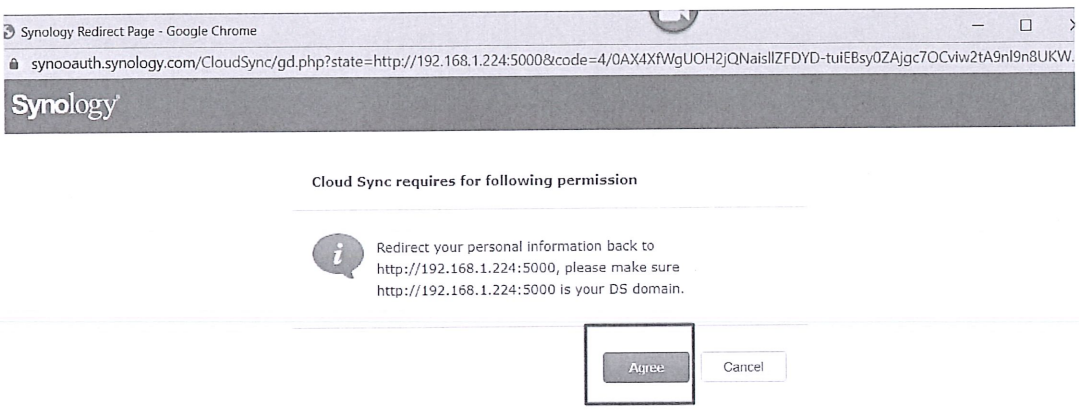
5. กรอก รหัสผ่านเพื่อ login



6. จะมีหน้าต่างแจ้งขออนุมัติการ Sync ระหว่าง NAS กับ CLOUD



7. จะมีหน้าต่างแจ้งเตือน ให้พิจารณาข้อมูลการ Sync

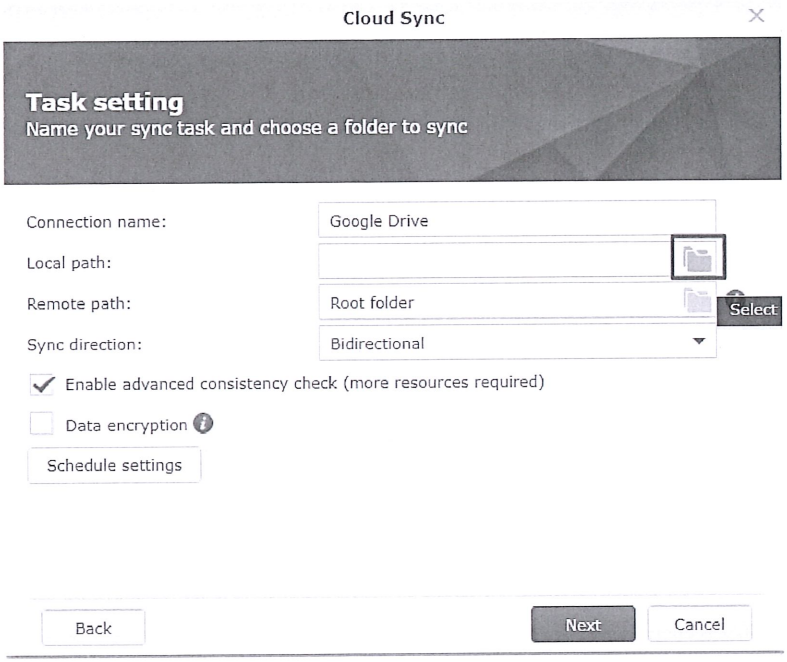


8. Connection Name คือ การตั้งชื่อ Connection

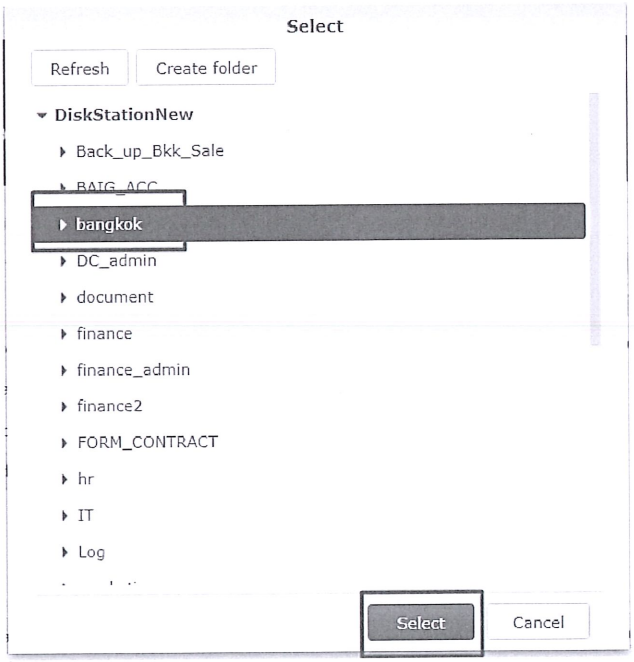
   Local path คือ Path ของ Source (ต้นทาง)

   Remote path คือ Path ของ Destination (ปลายทาง)

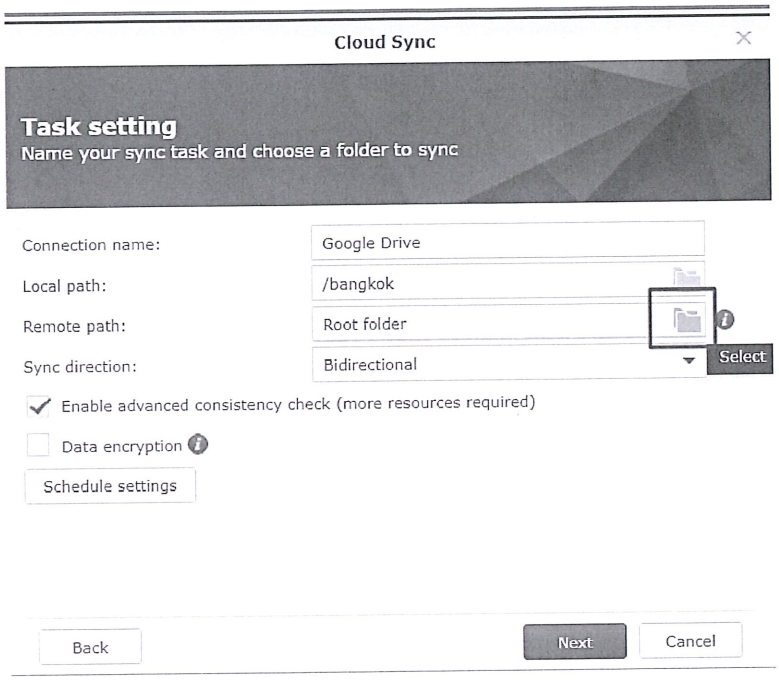
   Sync direction คือ รูปแบบการ Sync



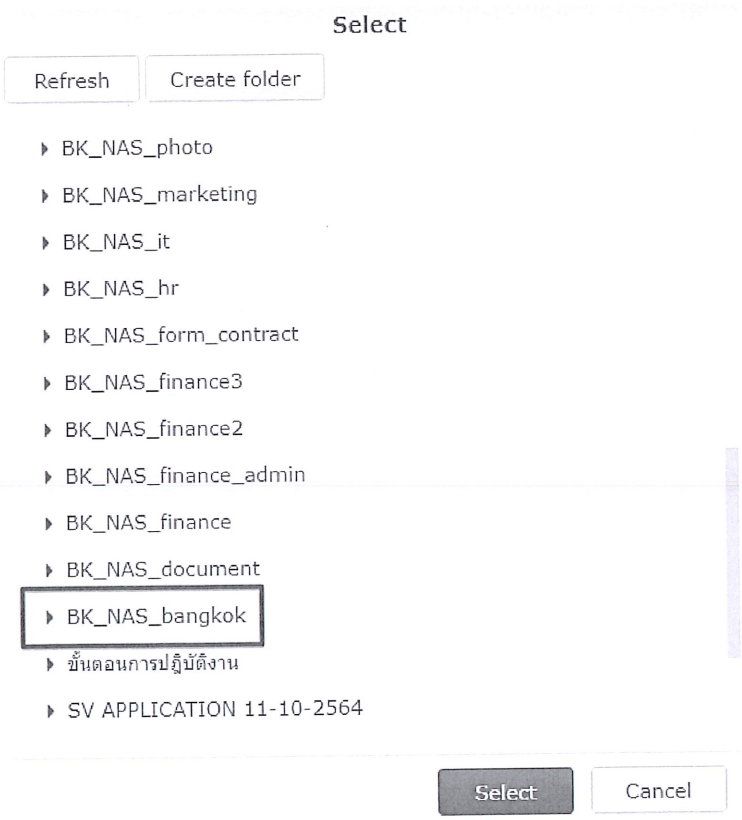
9. เลือก folder ต้นทาง



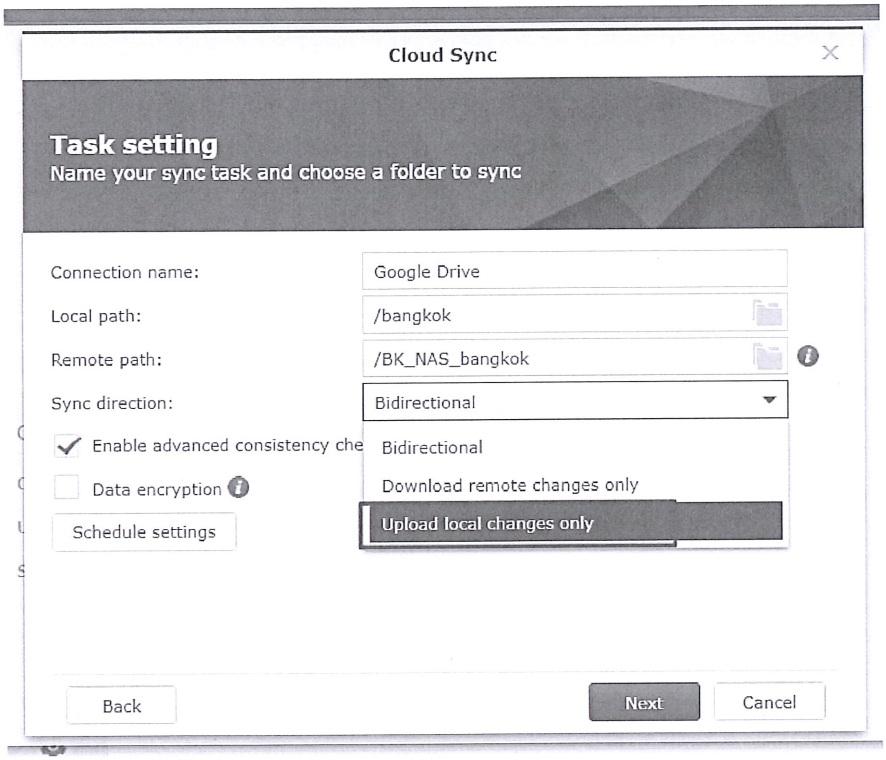
10. เลือก folder ปลายทาง



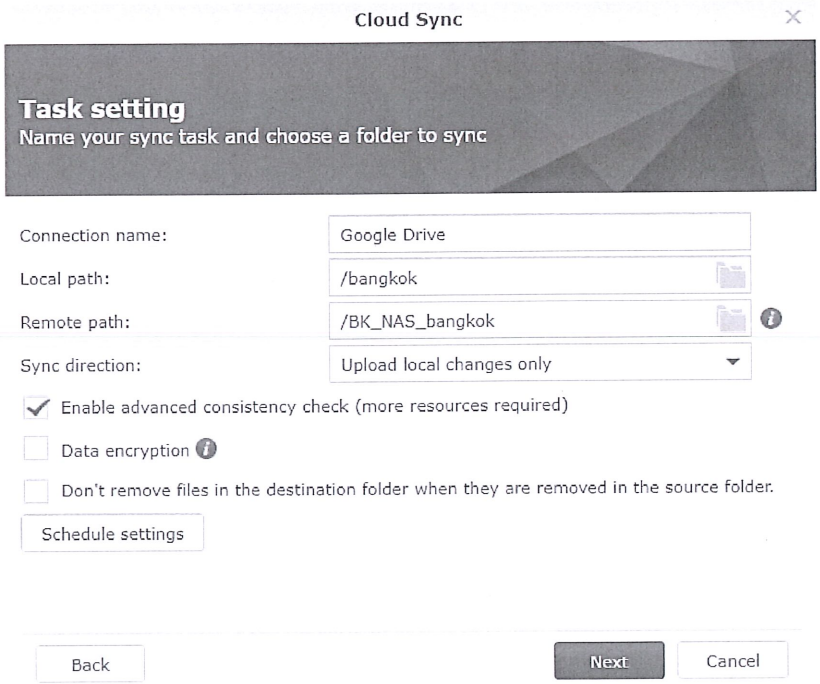
11. เลือก ชื่อ folder ปลายทาง (ถูกสร้างเอาไว้แล้วบน cloud)



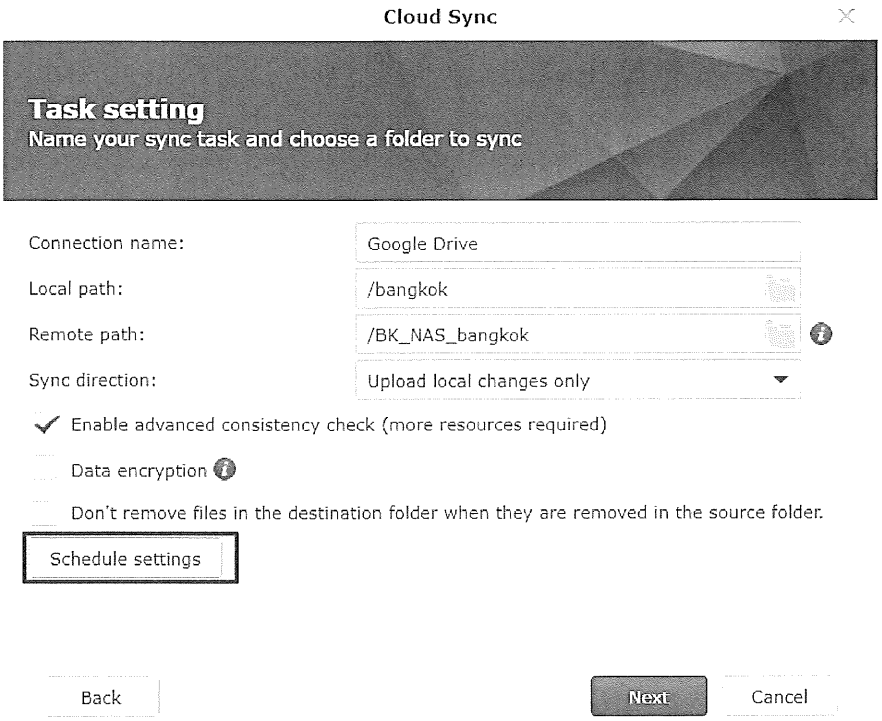
12. เลือก Upload local changes only



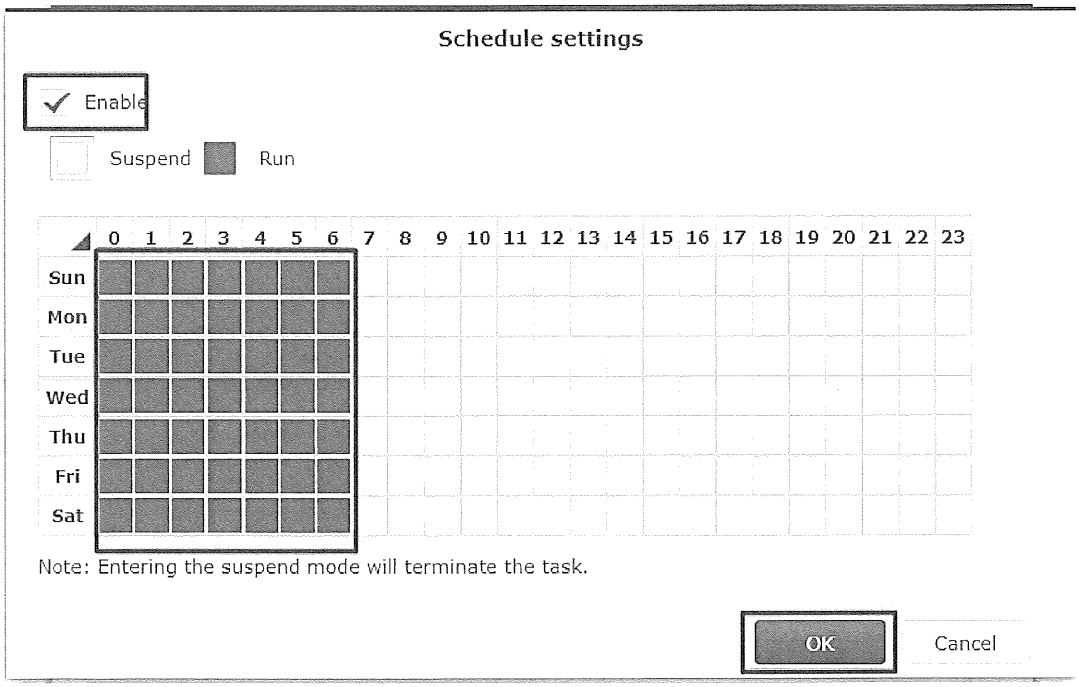
13. ทบทวนการตั้งค่า 4 จุด ได้แก่ Connection name , Local path , Remote path , Sync direction



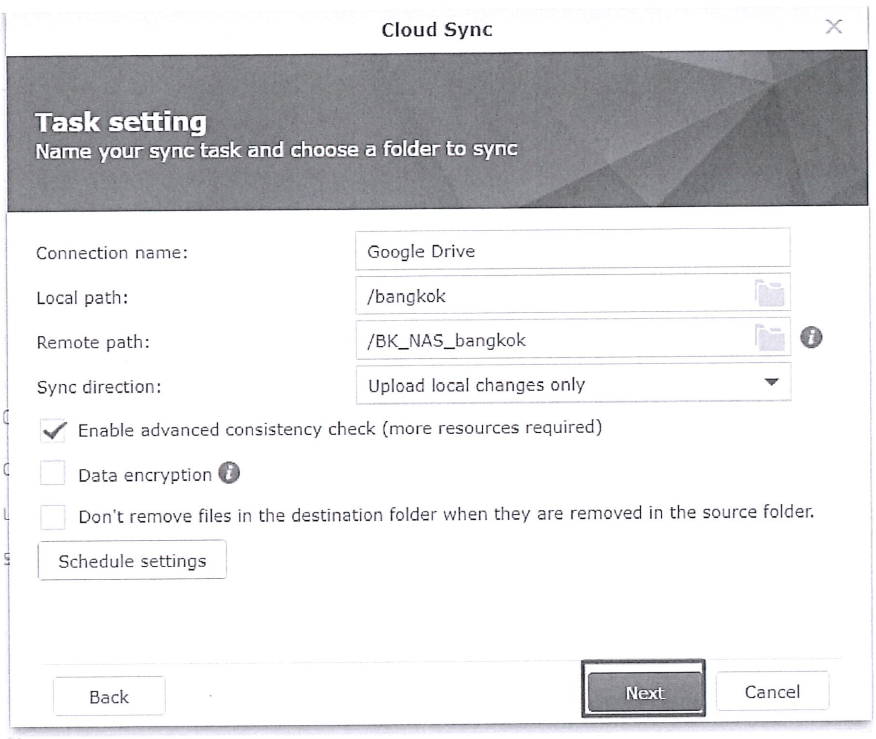
14. กดที่ปุ่ม Schedule setting เพื่อ เลือกการตั้งเวลา ในการ Sync



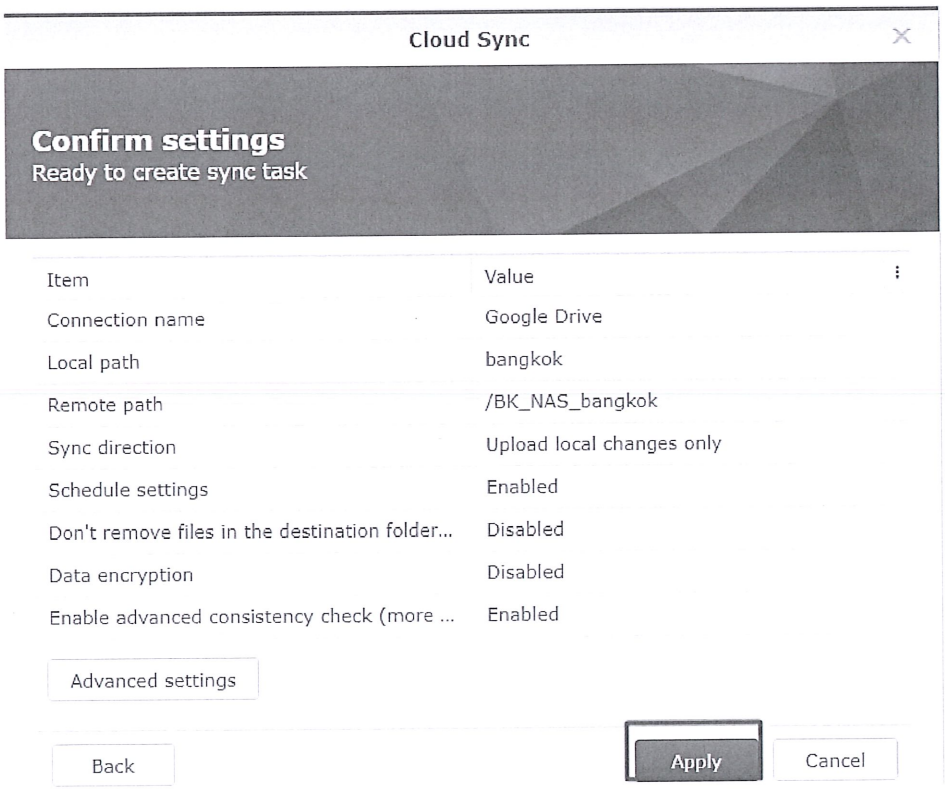
15. กดตั้งเวลาตามภาพด้านล่าง



16. เมื่อตั้งเวลาเสร็จแล้วให้กด Next

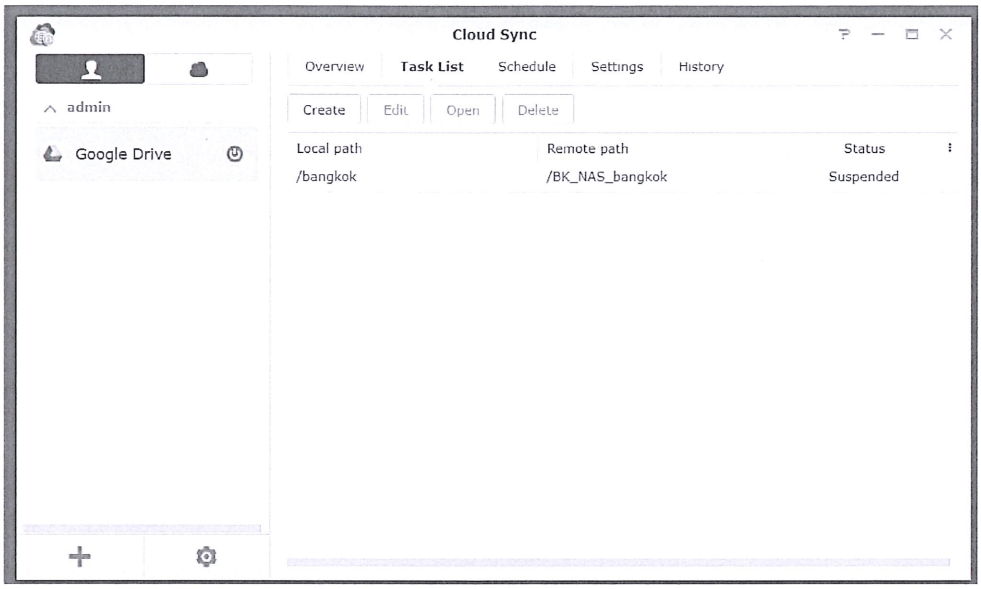


17. กด Apply



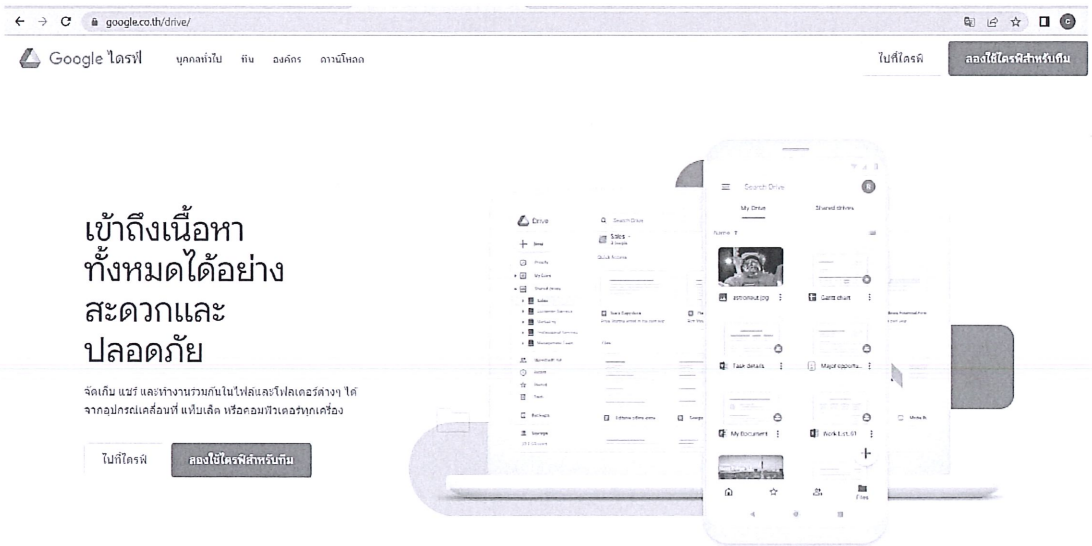
18. NAS จะทำกเลือก Upload local changes only

19. การ Sync ตามภาพ



การ Restore ดังนี้

1. Login เข้า https://www.google.co.th/drive/

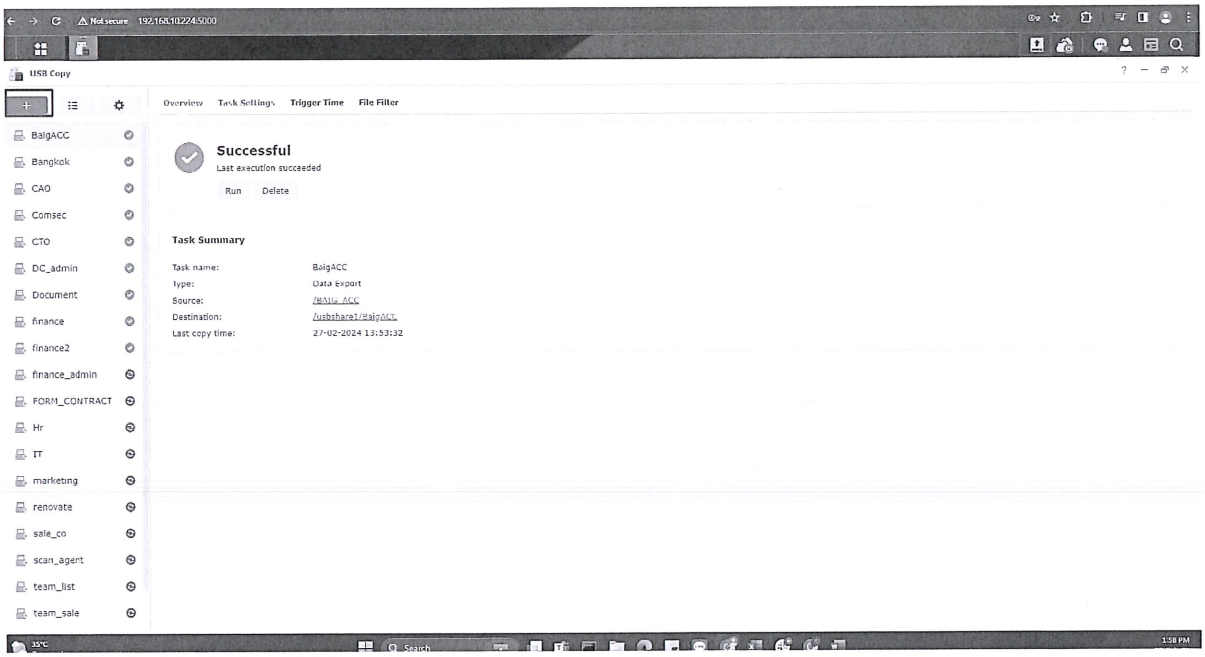


2. กด Download file ที่อยู่ใน folder บน Cloud นำกลับมาไว้ที่ NAS

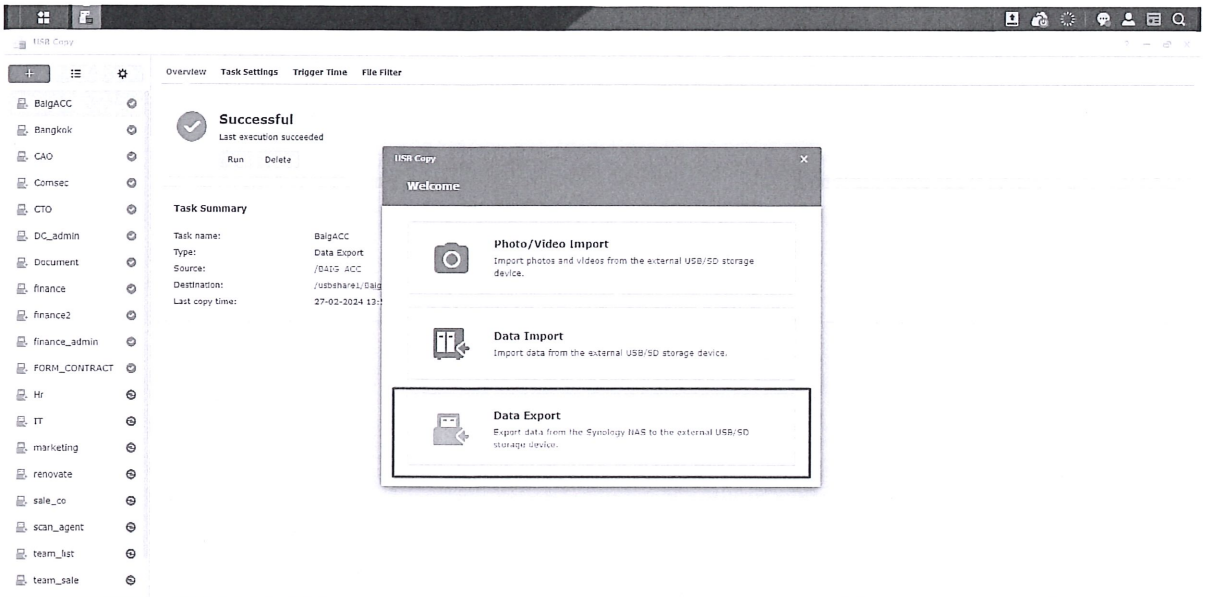


<u>การ Backup ด้วย External HDD โดยใช้โปรแกรม USB COPY</u>

1.เข้าหน้า USB COPY กดรูป + เพื่อเพิ่ม Task โปรแกรมนี้จะใช้ได้ก็ต่อเมื่อมีการเชื่อมต่อระหว่าง Nas กับ External HDD แล้วเท่านั้น



2.เลือก Data Export



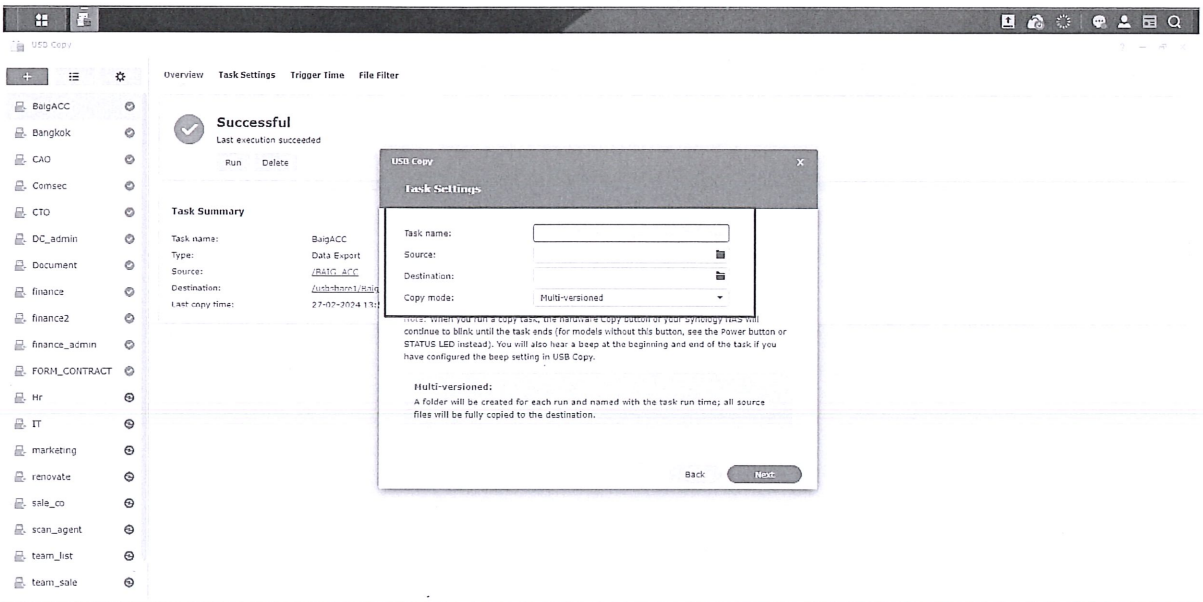
3. กรอกรายละเอียดดังนี้

Task name : ให้ใส่ชื่อที่เราต้องการลง

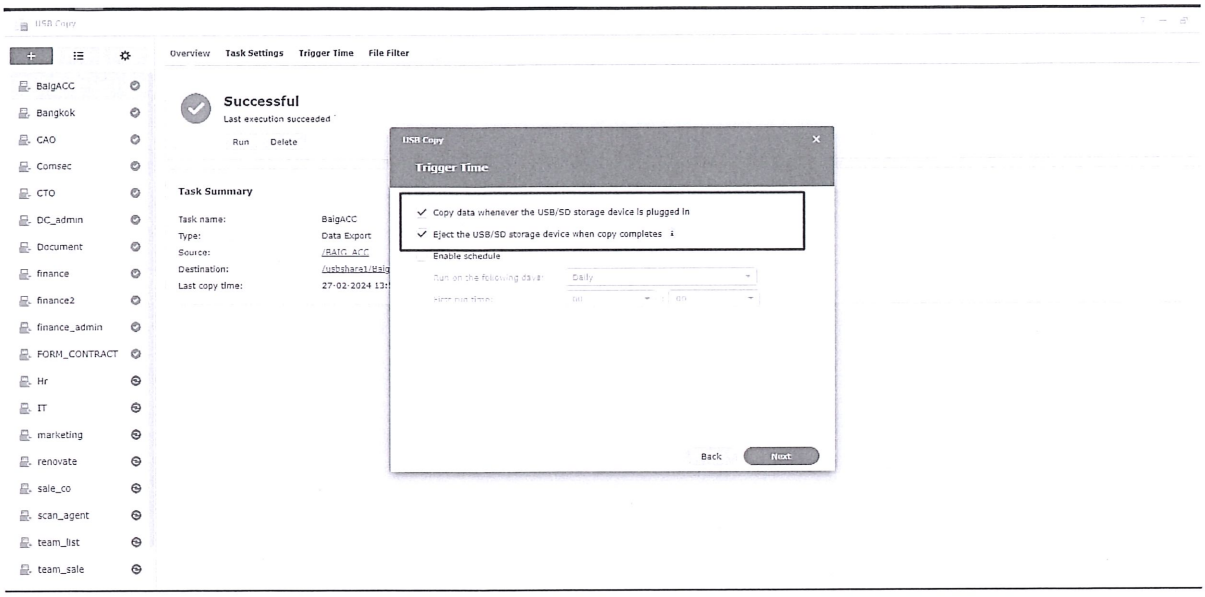
Source : เลือก โฟลเดอร์ใน Nas ที่เราต้องการ Copy

Destination : เลือกปลายทางที่ต้องการเก็บ

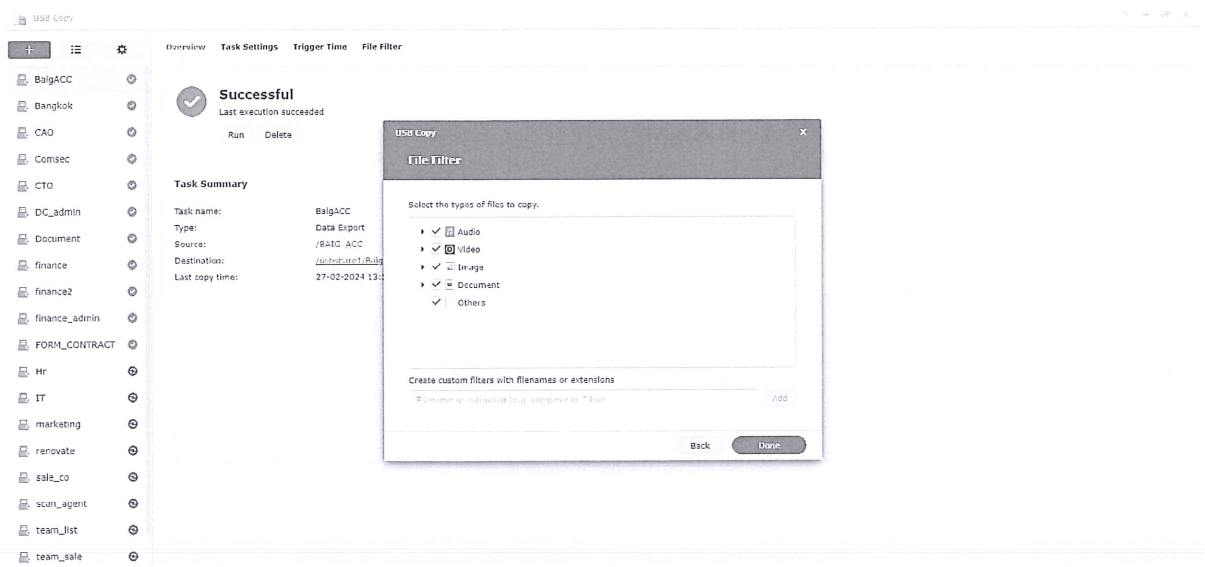
Copy Mode : เลือก Mirroring จากนั้นกด Next ระบบจะขึ้น Pop up แจ้งเตือน กดYes



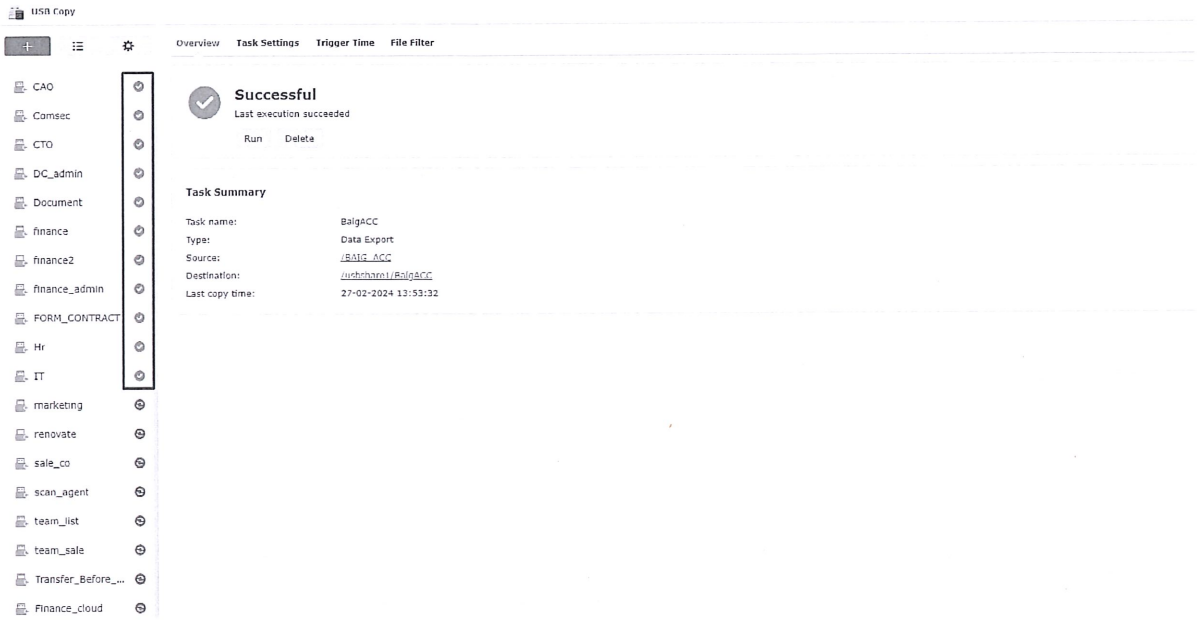
4.กดเลือก 2 ช่องบนตามภาพ เพื่อให้ทุกครั้งที่มีการเสียบ External ให้ทำ Backup ทันที และหาก Backup เสร็จแล้ว ให้ทำการ Reject External ออกจาก nas



5.เลือกประเภทไฟล์ที่ต้องการ Backup เช่นให้ Backup แค่เอกสาร จากนั้นกด Done



6.หากไฟล์ไหน Backup เสร็จแล้วจะมีสถานะ เครื่องหมายถูก ขึ้นบริเวณขวามือของชื่อ โฟลเดอร์ตามรูป



ประวัติการการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	30 มีนาคม 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา
2	1.1	1.ปรับปรุงแก้ไข IP 2.เพิ่ม Backup USB COPY	1 มีนาคม 2567	วีรพล วุฒิเสมานานนท์

ลงชื่อ วีรพล .

(วีรพล วุฒิเสมานานนท์)

ผู้รับผิดชอบ

วันที่ 1 มีนาคม 2567

ผู้อนุมัติ

ลงชื่อ ชนิดา ชนวงศ์เกษม

(ชนิดา ชนวงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

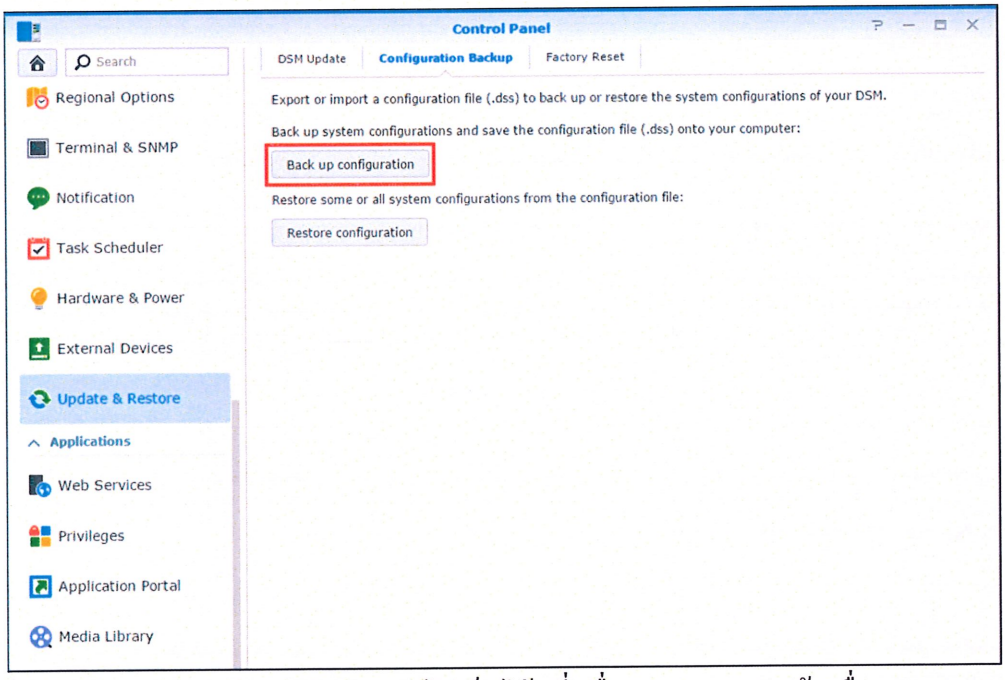
วันที่ 1 มี.ค. 2567

ขั้นตอนการติดตั้งค่าระบบการสำรองข้อมูลใน NAS

วัตถุประสงค์ เพื่อเป็นมาตรฐานในการตั้งค่าในการสำรองข้อมูลใน NAS

การตั้งค่าสำหรับ Backup (Backup Configuration)

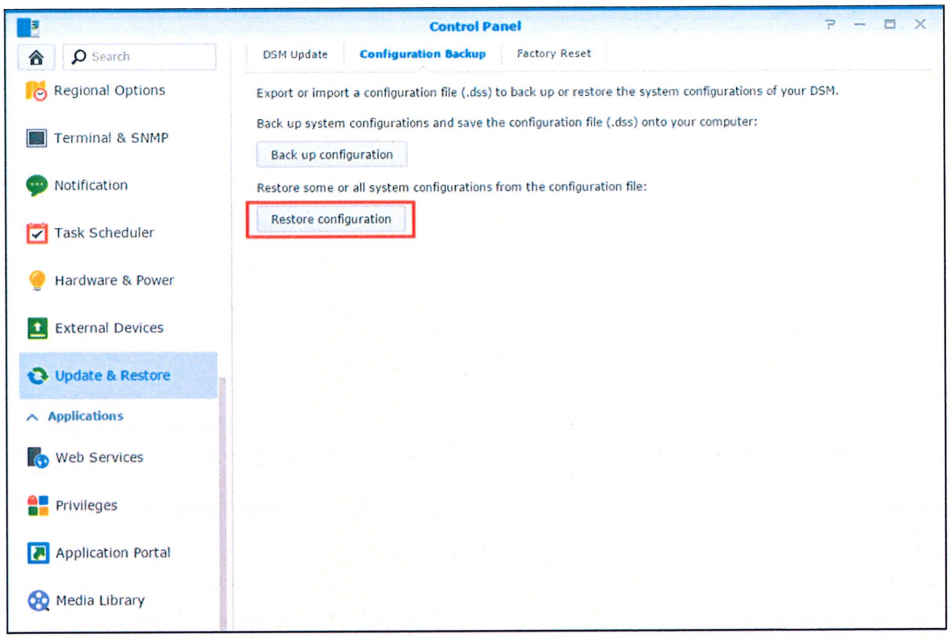
1. ไปที่ Control Panel > Update & Restore เพื่อ backup system configurations นามสกุล (.dss) ไปยัง Computer ตัวอย่าง เช่น users, groups, shared folders, and services.
2. คลิก Back up configuration.



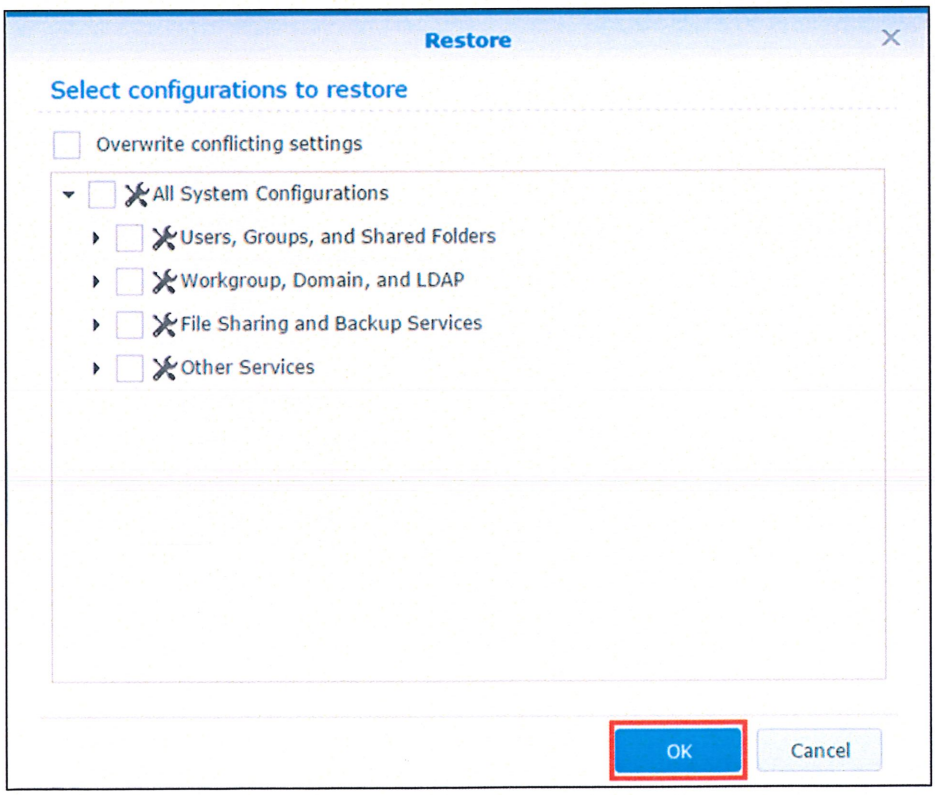
3. ไฟล์ configuration file จะ download ไปเก็บไว้ ที่เครื่อง Computer ด้วยชื่อ Synology Product Name]_[Created Date].dss)

การตั้งค่าสำหรับ Restore (Restore Configuration)

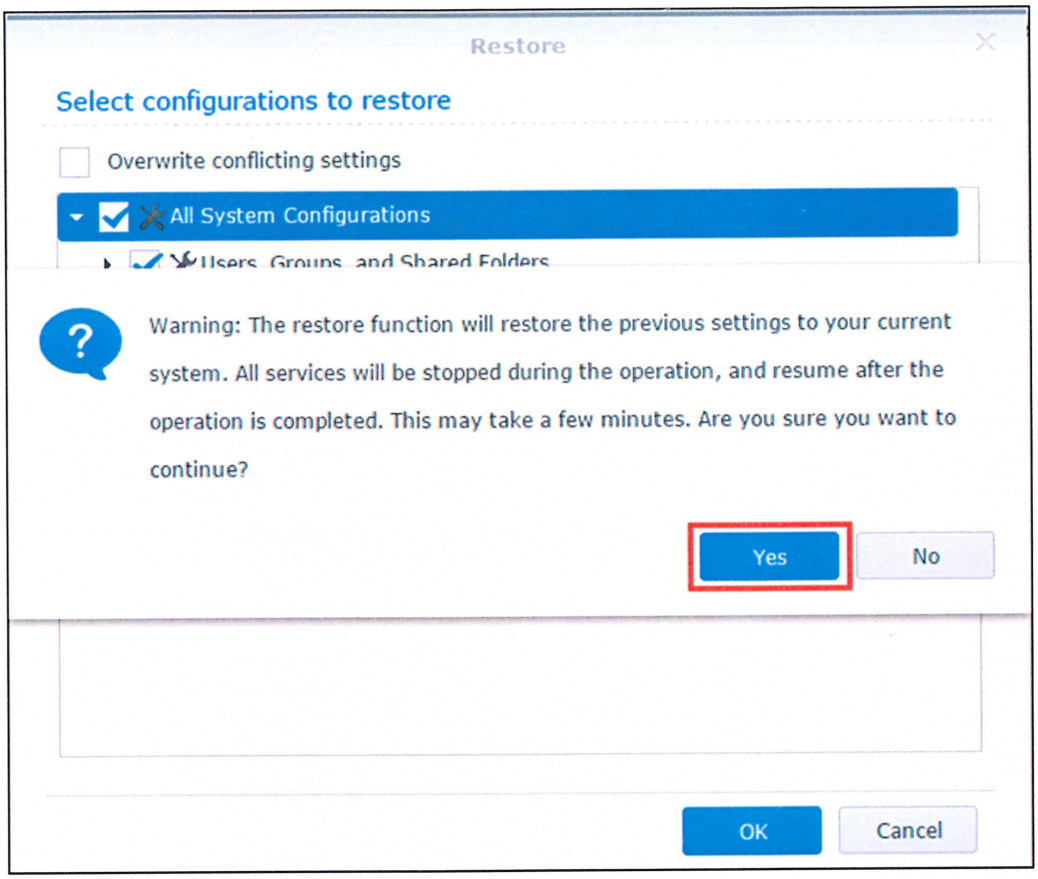
1. คลิก Restore configuration



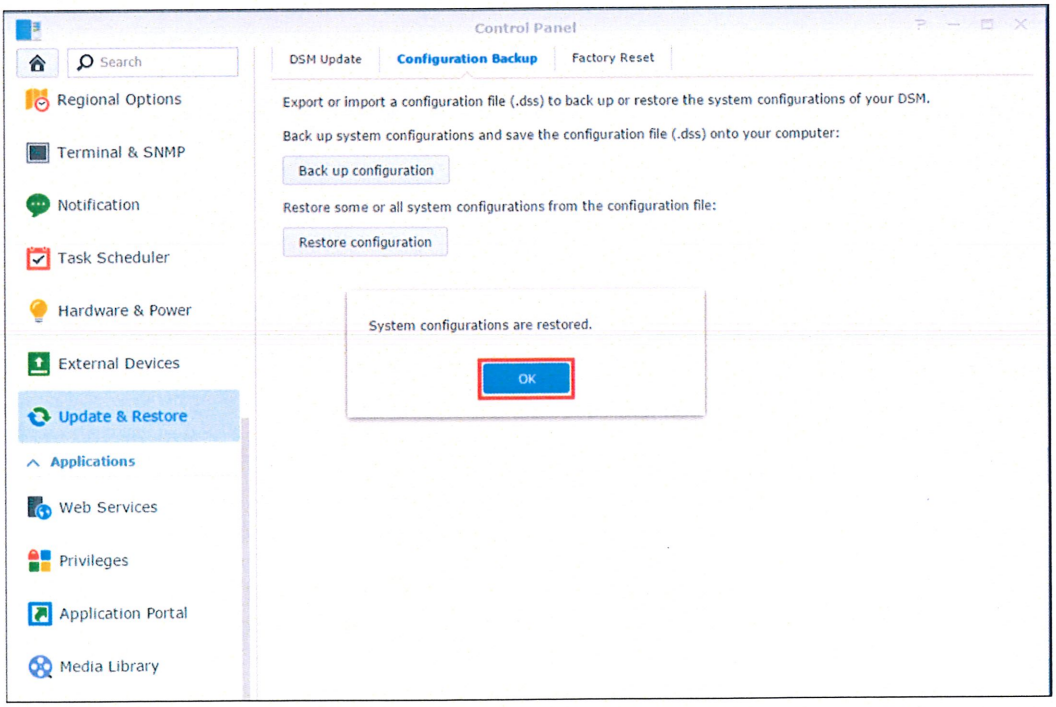
2. คลิก Browse and select the configuration file ซึ่งเก็บอยู่บนเครื่อง Computer
3. คลิก checkboxes ของ configurations ที่ต้องการจะ restore และคลิก OK. จะเป็นการ restore ทับ conflicting settings กับการตั้งค่า settings ดังต่อไปนี้ users, groups, shared folders, and services.



4. ปรากฏหน้าต่างที่มีข้อความเตือน. คลิก Yes to continue.



5. หลังจาก Restore เรียบร้อยแล้ว, คลิก OK to finish.



ผู้อนุมัติ

ลงชื่อ ชนิดา ชนงศ์เกษม

(ชนิดา ชนงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 25/03/65

ลงชื่อ วรวุฒิ เทพหัสดิน ณ อยุธยา

(วรวุฒิ เทพหัสดิน ณ อยุธยา)

ผู้รับผิดชอบ

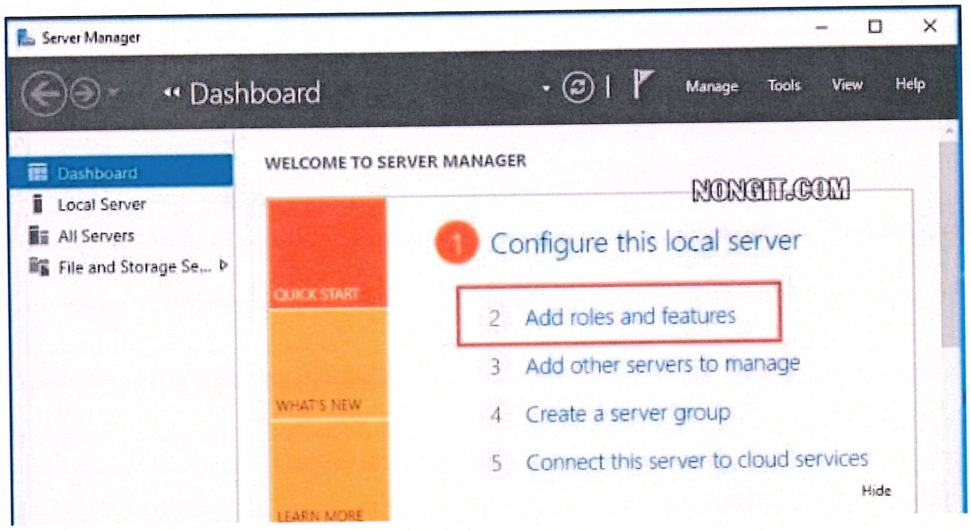
วันที่ 25/03/65

ขั้นตอนการติดตั้ง Domain Controller

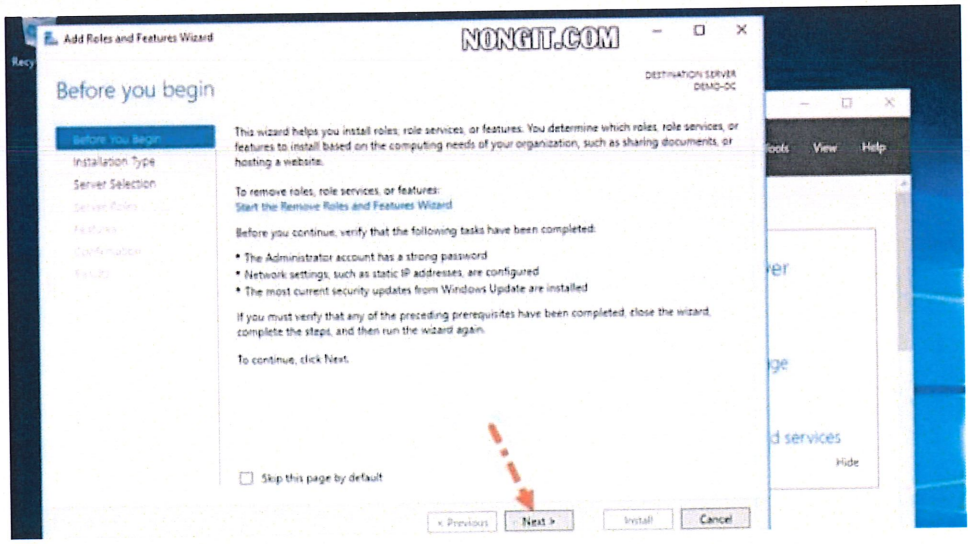
วัตถุประสงค์ เพื่อเป็นมาตรฐานในการตั้งDomain Controller (Active Directory) ภายในบริษัท

วิธีติดตั้ง Domain Controller (Active Directory) ใน Windows Server 2016

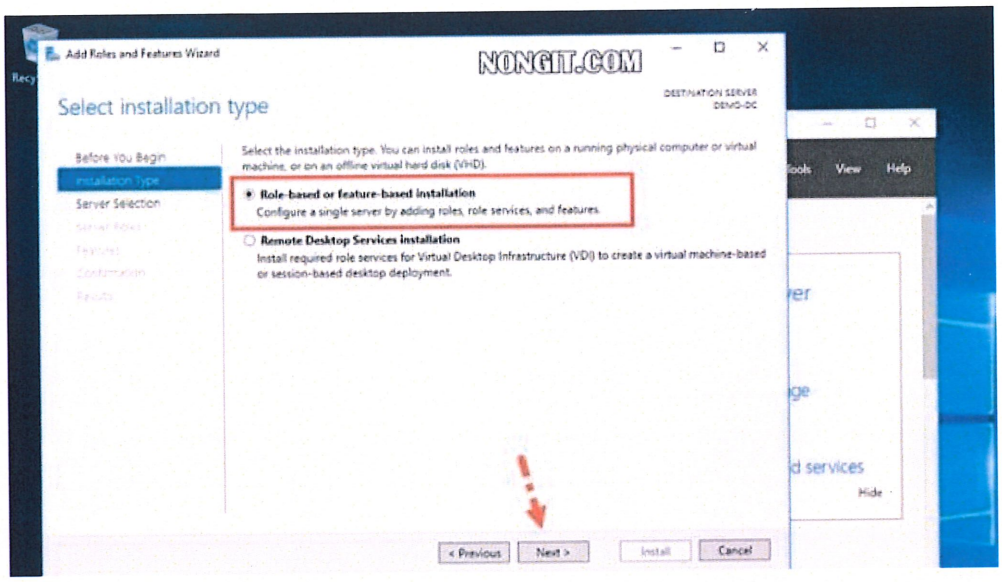
1. ทำการกำหนด IP Address และกำหนดชื่อ Server name ให้เรียบร้อย
   1.1. IP Address คือ 192.168.100.74
   1.2. Server name คือ Bangkok-Asset
2. เครื่อง Server ที่จะทำการติดตั้ง AD Server ต้องทำการเชื่อมต่อ network ไว้ก่อน
3. ที่หน้าต่างของ Server Manager ให้ท่านคลิก Add roles and features



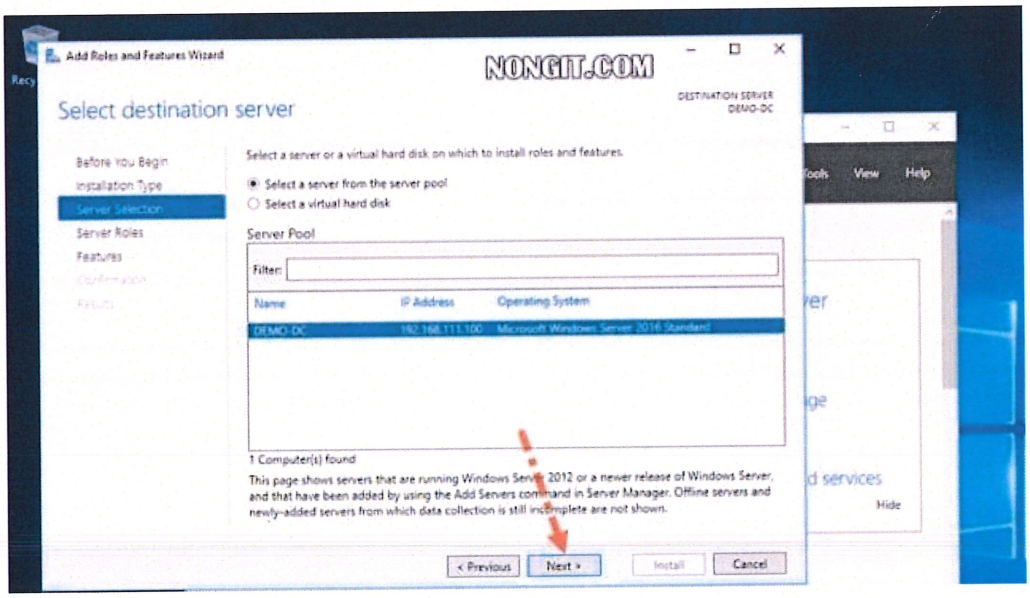
4. คลิกปุ่ม Next



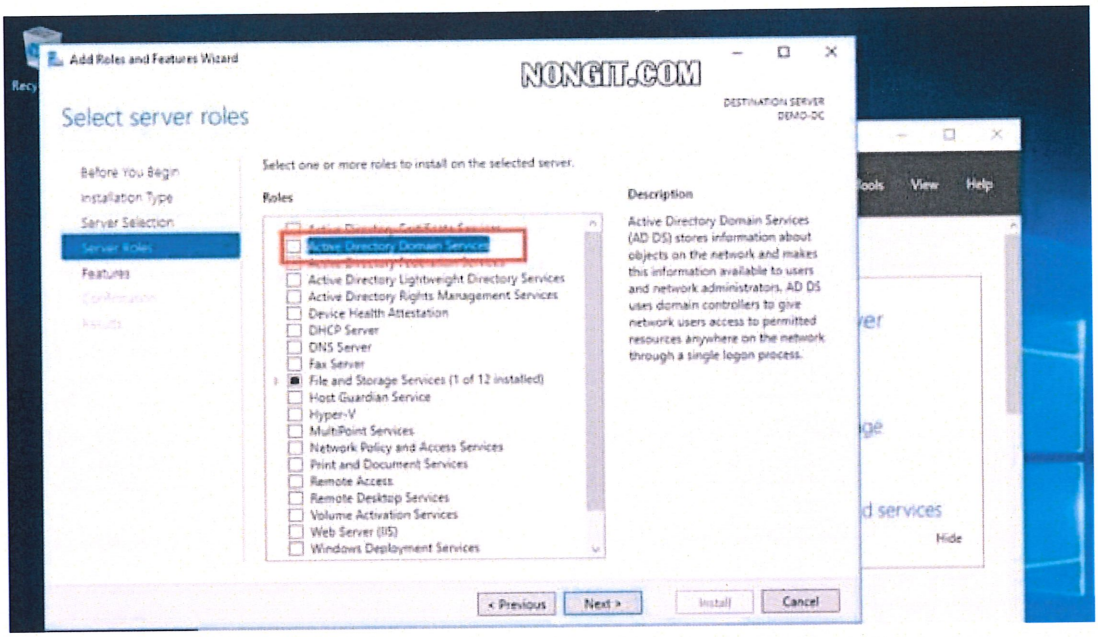
5. คลิกปุ่ม Next ต่อไป



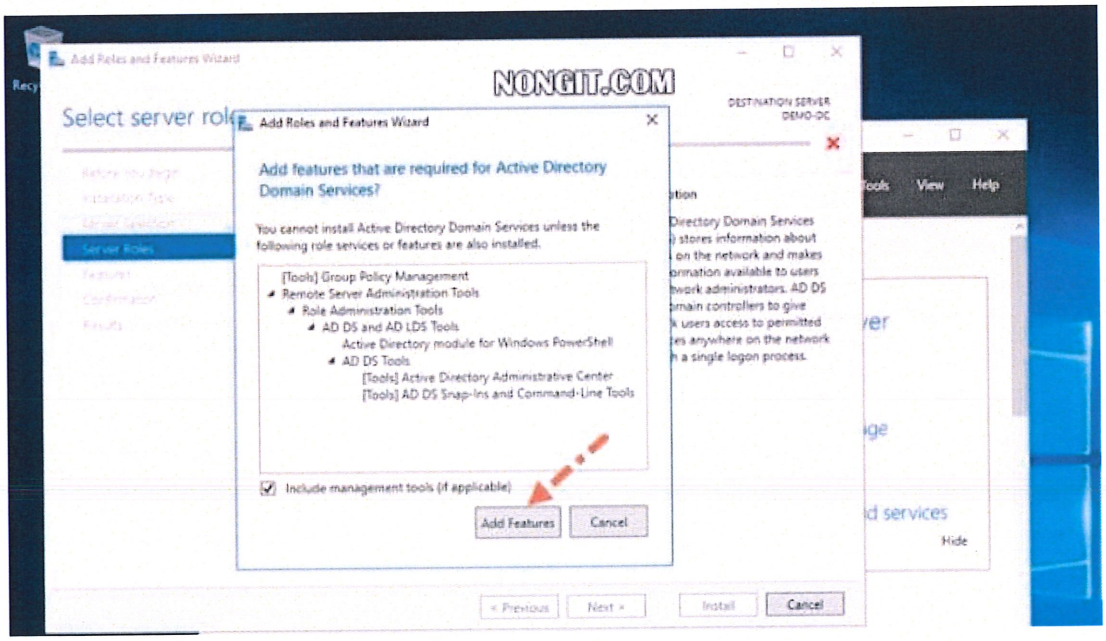
6. เลือกเครื่อง Server ที่จะลง AD จากนั้นคลิก Next



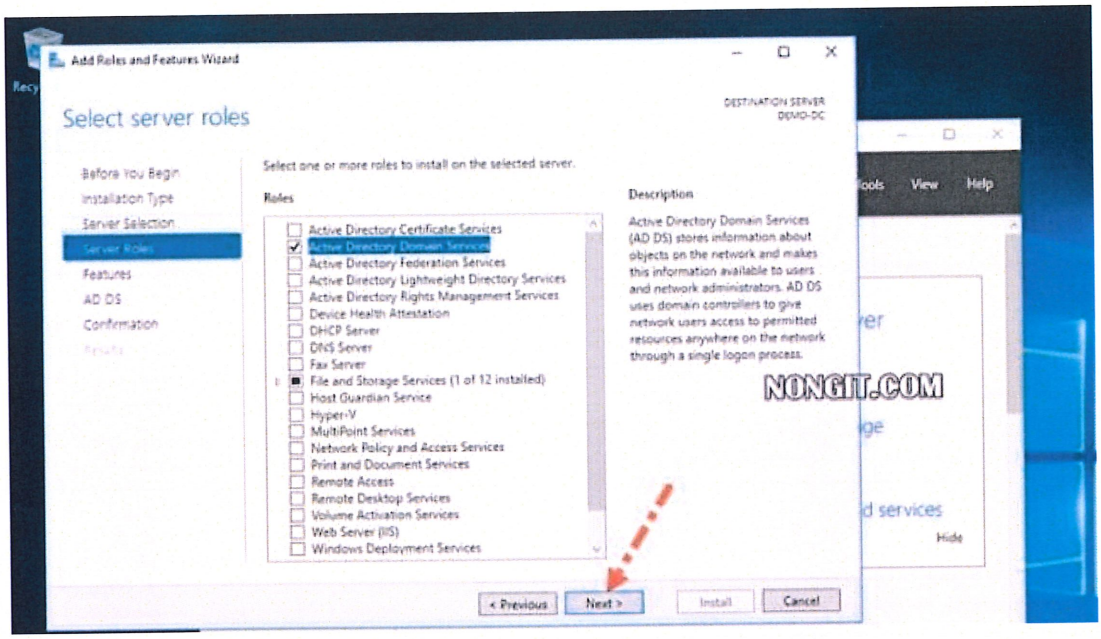
7. หน้านี้ให้เลือก (/) Active Directory Domain Services ที่อยู่ในช่อง Roles



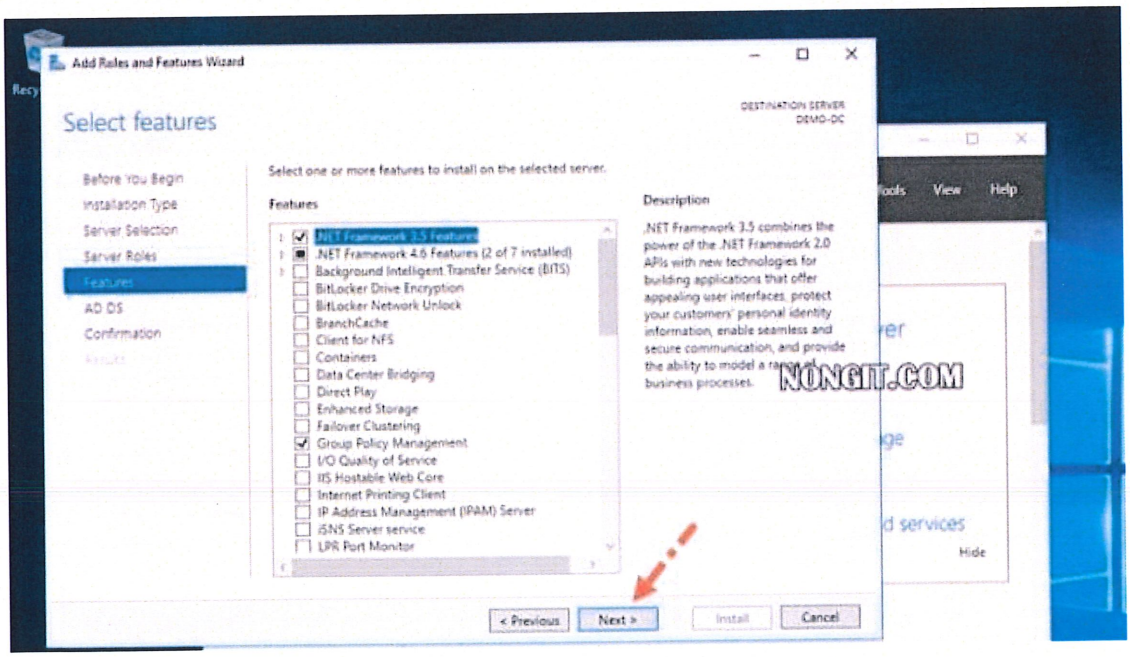
8. จากนั้นจะมีหน้าต่างแจ้งรายการ Feature ที่ Service ต้องการ ให้คลิก Add Feature



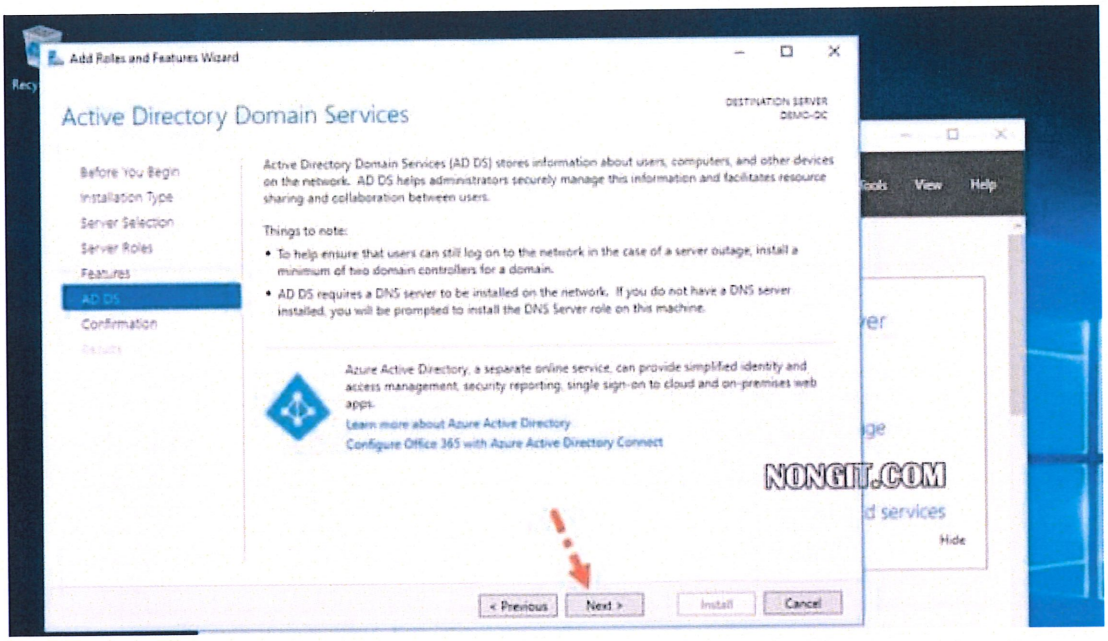
9. คลิกปุ่ม Next



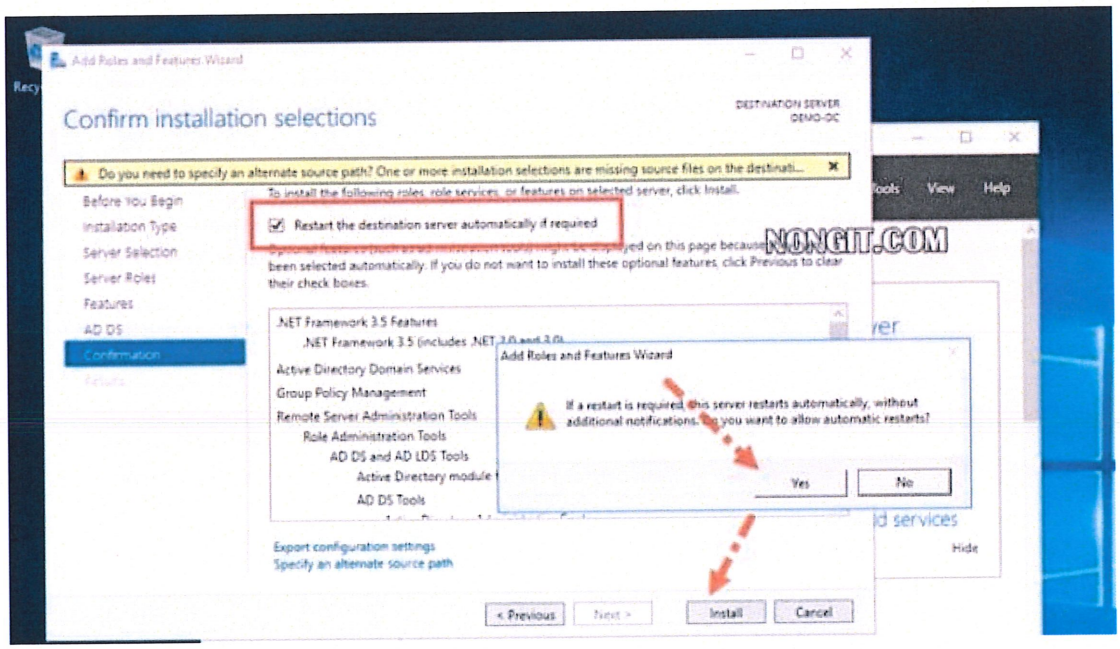
10. หน้านี้จะให้เลือก Feature อื่นๆ หากไม่เพิ่มอะไรก็คลิก Next (แนะนำให้ติดตั้ง .Net 3.5 ไว้ด้วย)



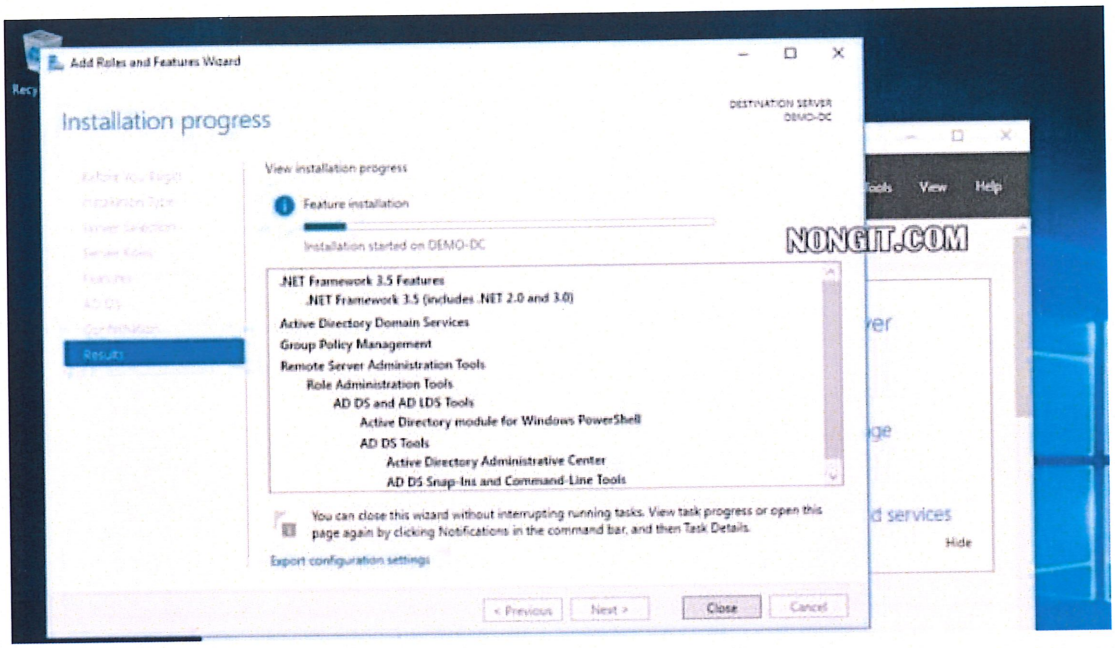
11. คลิกปุ่ม Next



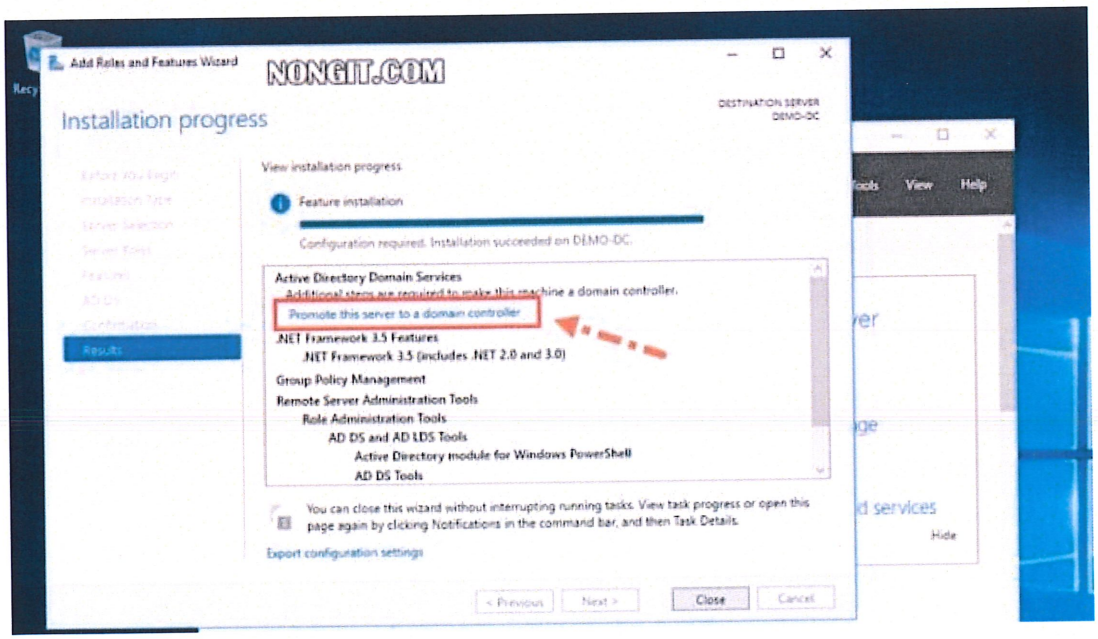
12. มาถึงหน้านี้จะให้มีการตรวจสอบรายการต่างที่เลือกไว้ เพื่อ Confirm ว่าจะติดตั้งรายการนี้ทั้งหมด เมื่อดูแล้วไม่ต้องการแก้ไขอะไรก็ให้เลือก (/) Restart the destination server automatically แล้วคลิก Yes ตามด้วยคลิกปุ่ม Install



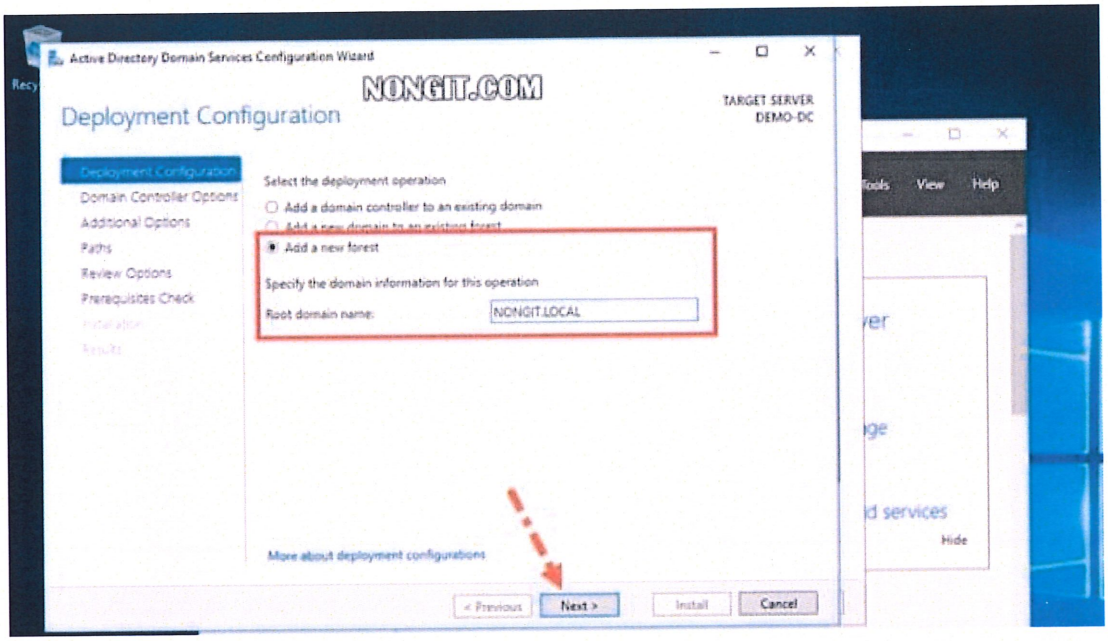
13. รอให้ระบบทำการติดตั้ง Roles



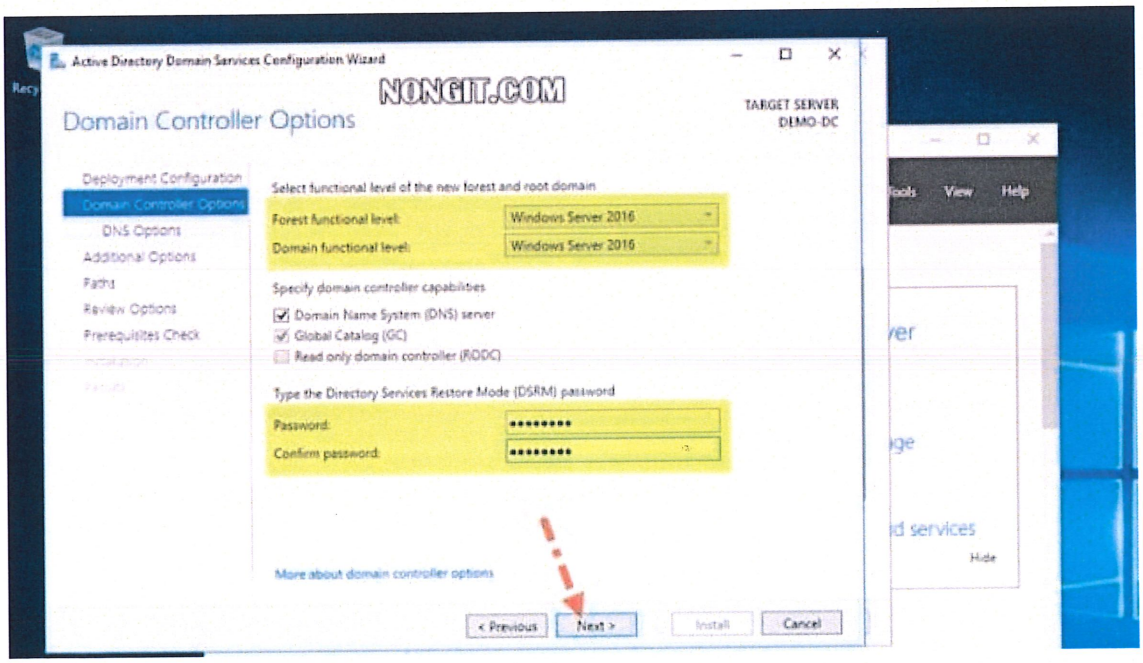
14. เมื่อติดตั้งเสร็จ จะแสดง Link ชื่อว่า Promote this server to a domain controller ให้คลิกเพื่อทำการ “Promote AD server 2016”



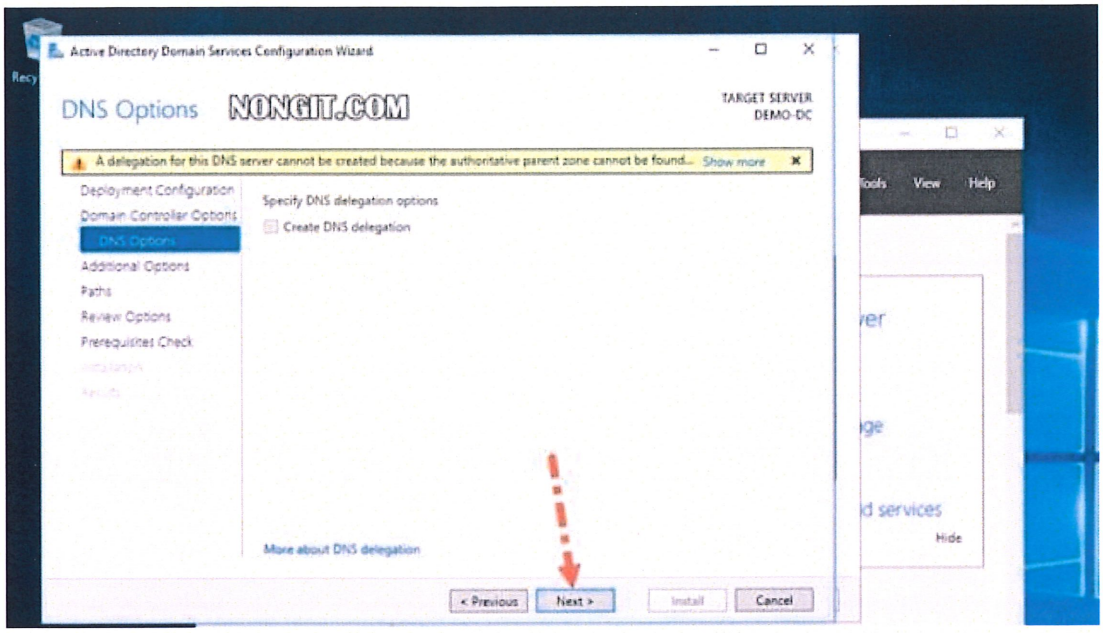
15. การสร้าง Domain ใหม่ จะต้องเลือก Add a new forest และกำหนดชื่อ Root Domain name: ตามที่ต้องการ (กำหนดเป็น BANGKOK.LOCAL) เมื่อกำหนดเสร็จก็คลิกปุ่ม Next



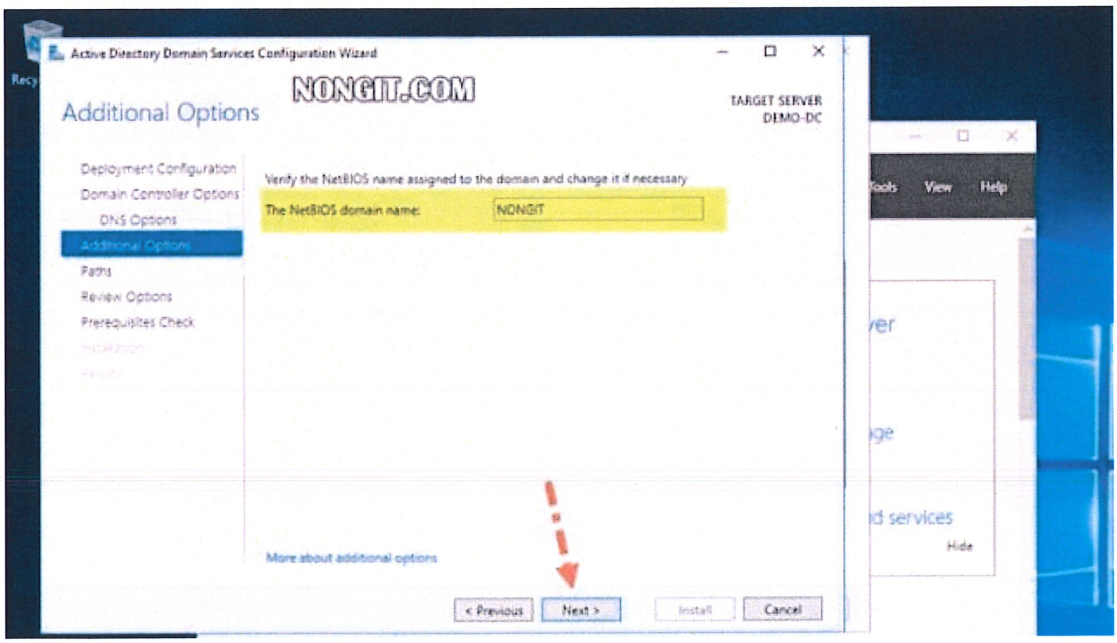
16. เลือกส่วนของ Forest และ Domain functional Level โดยหากมี Domain Server ที่อยู่ในระบบเครื่องเดียวก็เลือกเป็น Windows Server 2016 ทั้ง 2 และให้กำหนด Password สำหรับ Administrator ให้เรียบร้อยแล้วก็คลิกปุ่ม Next



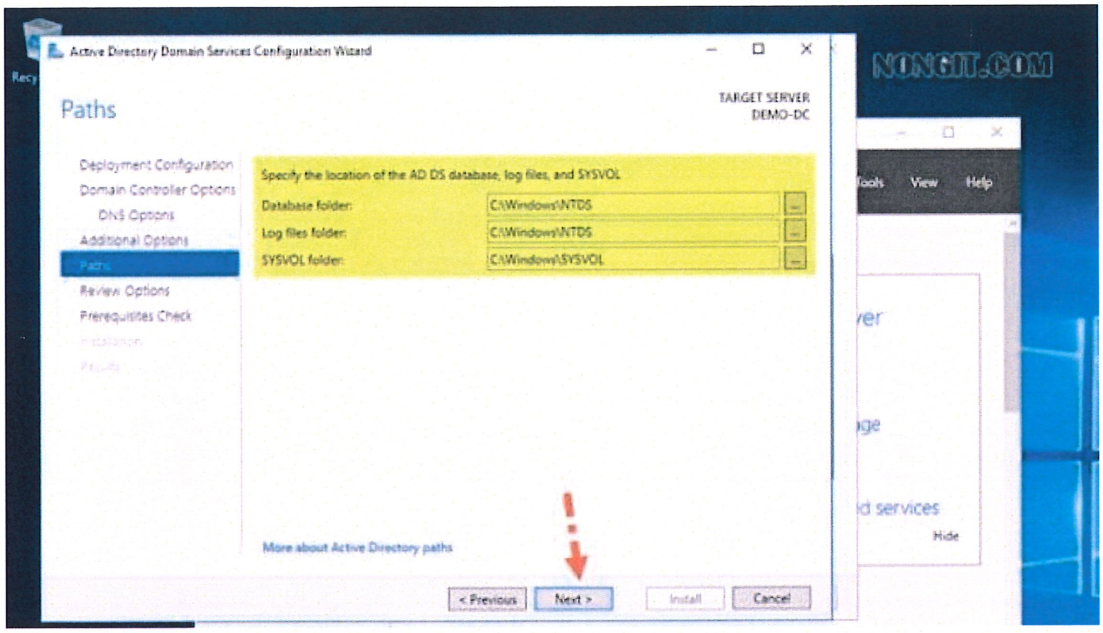
17. คลิกปุ่ม Next



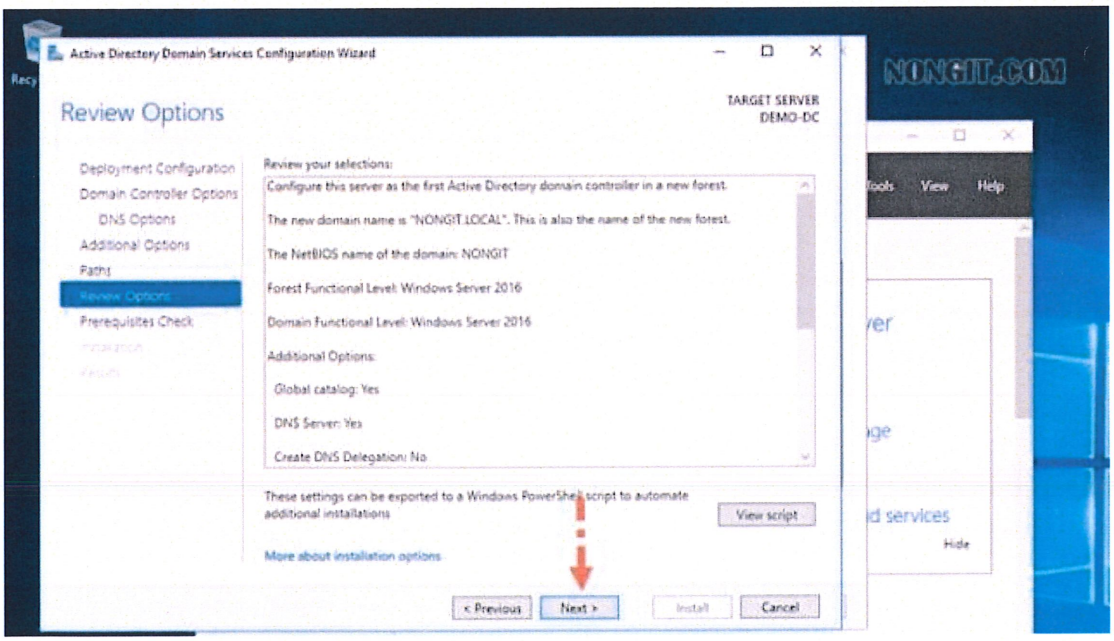
18. หน้านี้จะแสดง NetBIOS Domain Name คลิกปุ่ม Next ต่อไป



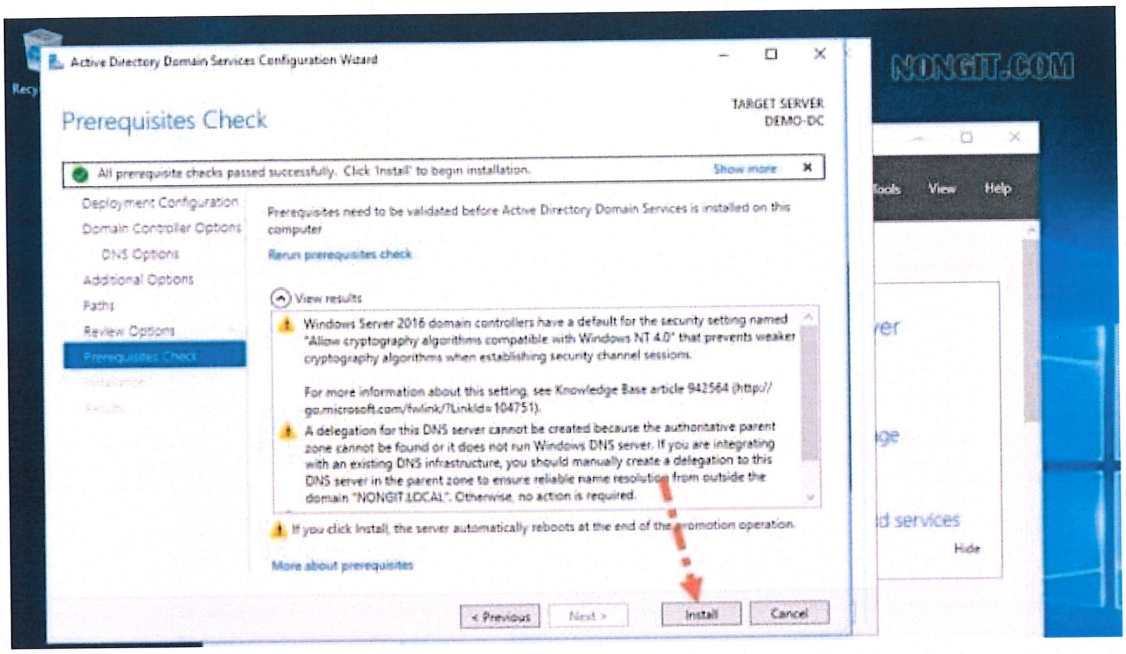
19. หน้านี้จะแสดง Path สำหรับ AD DS ของ Database Logs file และ Sysvol ให้คลิกปุ่ม Next



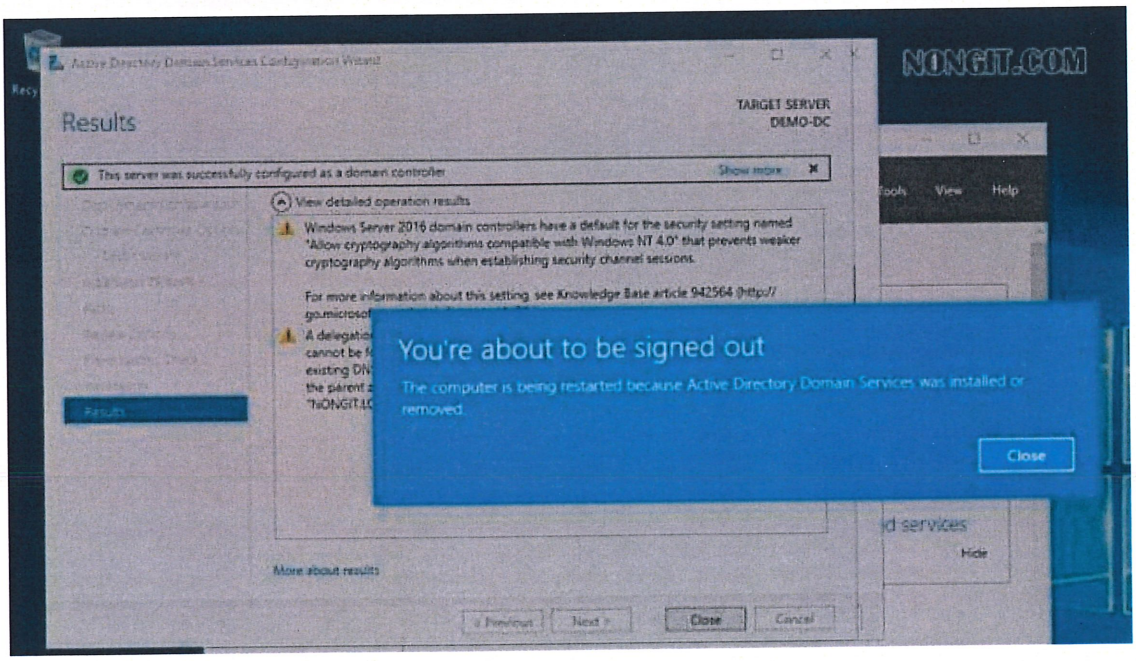
20. ที่หน้าต่าง Review Options จะแสดงค่า config ทุกขั้นตอนที่เลือกกำหนด คลิกปุ่ม Next



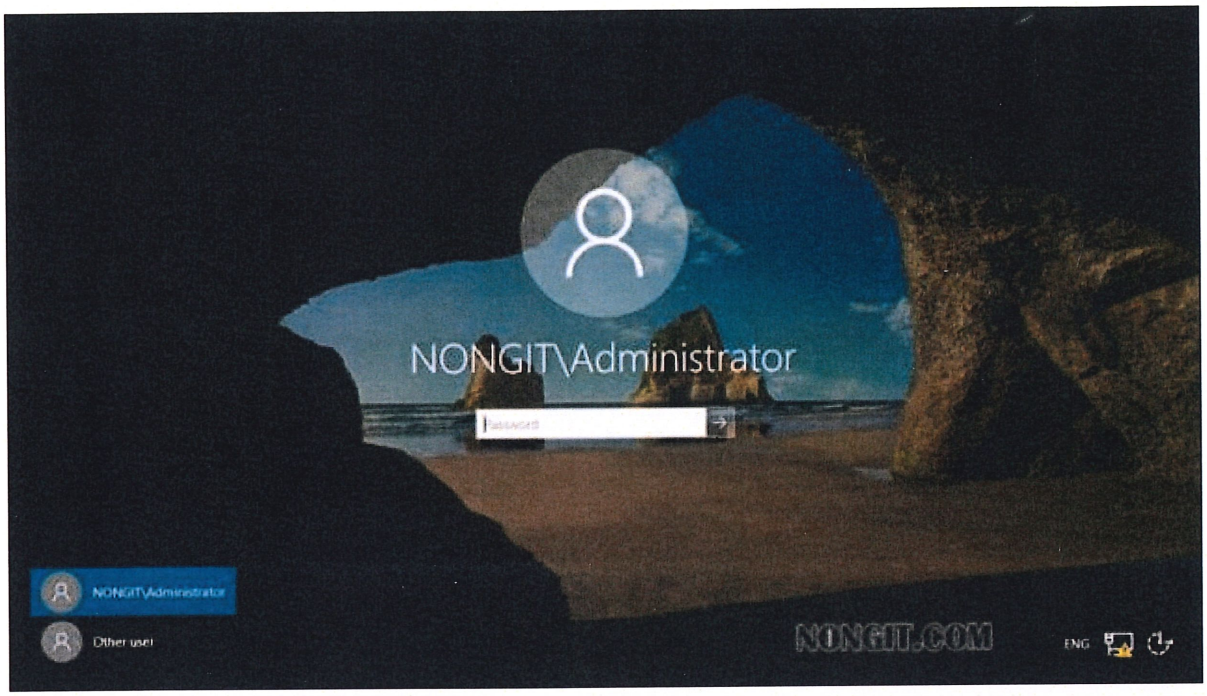
21. คลิกปุ่ม install



22. รอระบบทำการติดตั้ง Domain Controller เมื่อติดตั้งเสร็จจะ Restart เครื่อง 1 รอบ



23. เมื่อเครื่อง Restart เสร็จ ก็ให้ Sign in ด้วย Domain\Administrator



ลงชื่อ วรวุฒิ เทพทัสดิน ฯ

(วรวุฒิ เทพทัสดิน ณ อยุธยา)

ผู้รับผิดชอบ

วันที่ 25 มี.ค 65

ผู้อนุมัติ

ลงชื่อ ธนิศร ธนวงศ์เกษม

(ธนิศร ธนวงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

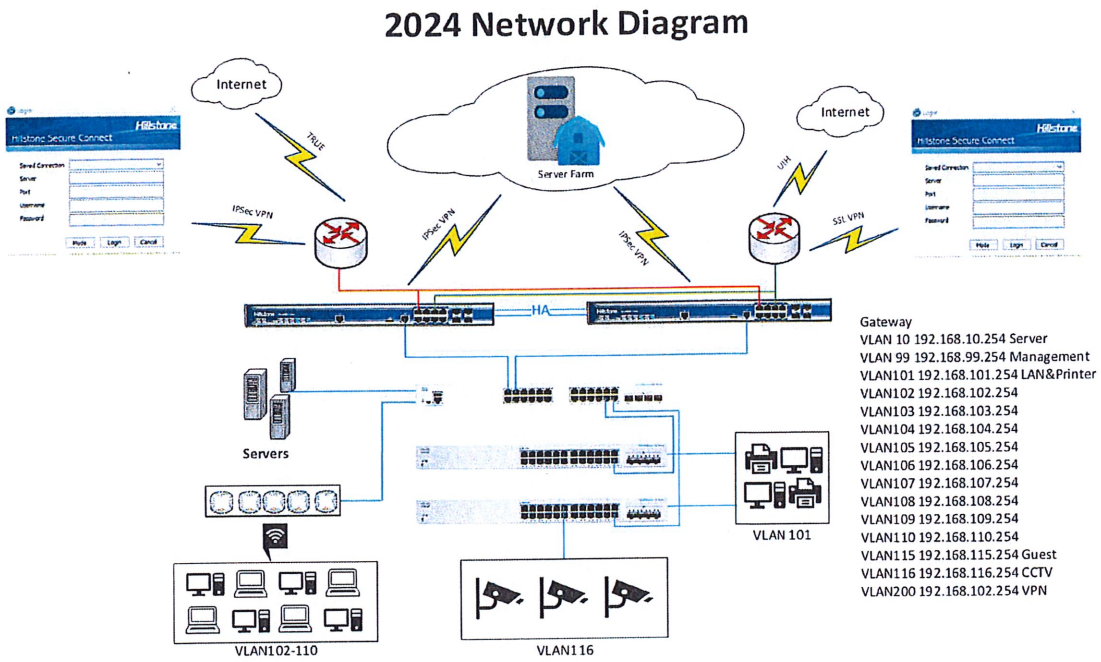
วันที่ 25 มี.ค. 65

ขั้นตอนการตั้งค่าระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์ เพื่อเป็นมาตรฐานในการตั้งค่าระบบเทคโนโลยีสารสนเทศภายในบริษัท และสามารถใช้งานได้อย่างมีประสิทธิภาพ

วิธีติดตั้งระบบเครือข่าย (Network)

1. Network Diagram



2. รายการอุปกรณ์ประกอบไปด้วยตามตารางข้างล่าง

Item	Model	Part Number	Serial No.	Hostname	IP Address
1	Hillstone SG-6000-E2800P Firewall		2508314195027350	BAI-Firewall	192.168.99.254
2	CBS250-24P-4G		FOC2631YA4K	BAI-SW01	192.168.99.101
3	CBS220-24FP-4G		DNI260900BF	BAI-SW02	192.168.99.102
4	CBS220-24FP-4G		DNI260900JX	BAI-SW03	192.168.99.103
5	Instant on AP11	R6K61A	CNJGK9T5FL	BAI-AP01	192.168.99.21
6	Instant on AP11	R6K61A	CNJGK9T5J3	BAI-AP02	192.168.99.22
7	Instant on AP11	R6K61A	CNJGK9T5LX	BAI-AP03	192.168.99.23
8	Instant on AP11	R6K61A	CNJGK9T4T3	BAI-AP04	192.168.99.24
9	Instant on AP11	R6K61A	CNJGK9T5JD	BAI-AP05	192.168.99.25
10	Instant on AP11	R6K61A	CNJGK9T5JZ	BAI-AP06	192.168.99.26
11	Instant on AP11	R6K61A	CNJGK9T5M6	BAI-AP07	192.168.99.27
12	Instant on AP11	R6K61A	CNNZK9TKB	BAI-AP08	192.168.99.28
13	Instant on AP11	R6K61A	CNNZK9TKCM	BAI-AP09	192.168.99.29
14	Instant on AP11	R6K61A	CNNZK9TK1Z	BAI-AP10	192.168.99.30

3. IP Address and VLan

VLAN	VLAN Name	IP address
200	VPN	192.168.200.0/24
10	Server	192.168.10.0/24
99	Network Management	192.168.99.0/24
101	Outlet ,Printer	192.168.101.0/24
102	Acc ,Fin	192.168.102.0/24
103	IT	192.168.103.0/24
104	DC,AGENT	192.168.104.0/24
105	COMSEC,BOD,HR	192.168.105.0/24
106	MK	192.168.106.0/24
107	LIST,SALE	192.168.107.0/24
108	REN,DESIGN,PUR	192.168.108.0/24
109	<Stand by>	192.168.109.0/24
110	<Stand by>	192.168.110.0/24
115	Guest-WiFi	192.168.115.0/24
116	CCTV	192.168.116.0/24

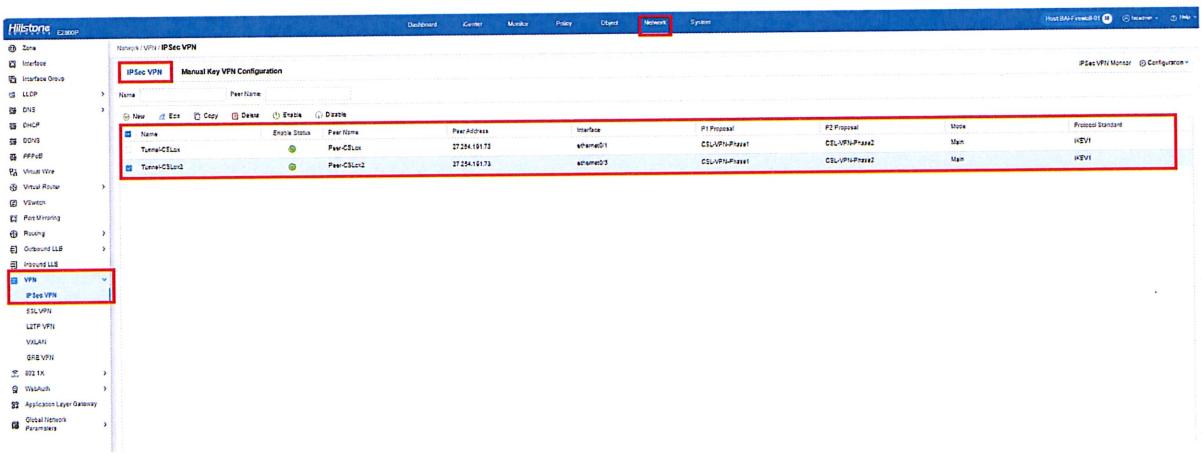
4. Wireless Network

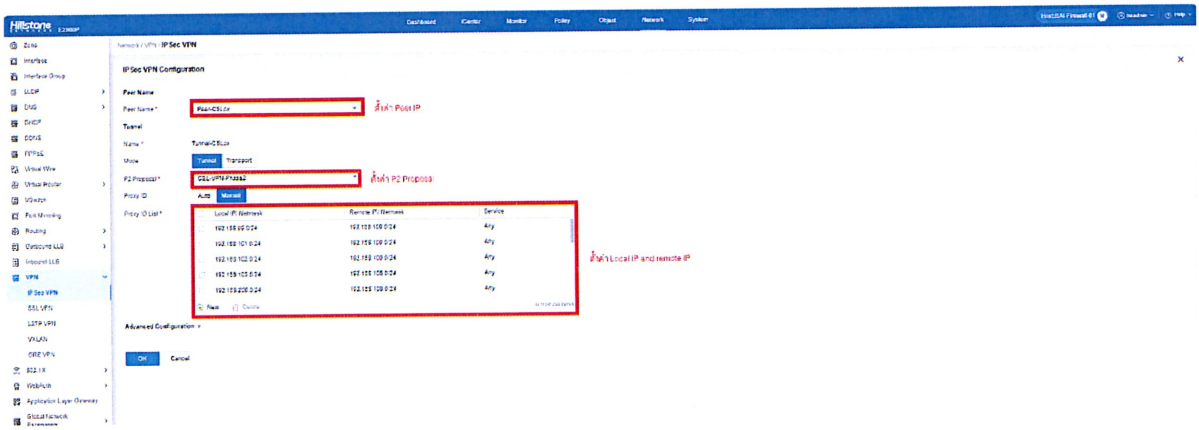
SSID	VLAN	Security Type
BAI-Internal	Dynamic VLAN	WPA2-Enterprise
BAI-Guest	115	Web Portal

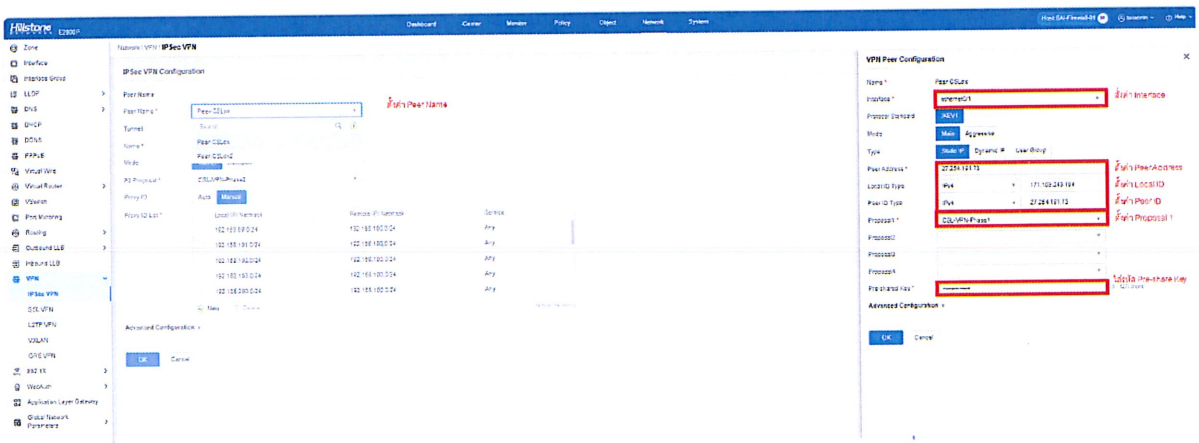
5. Configuration

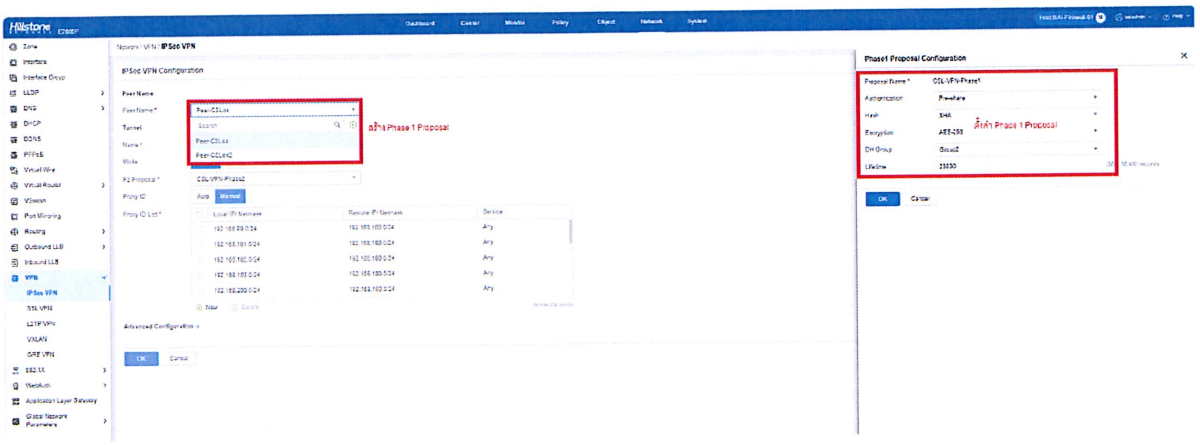
5.1. VPN (192.168.99.254)

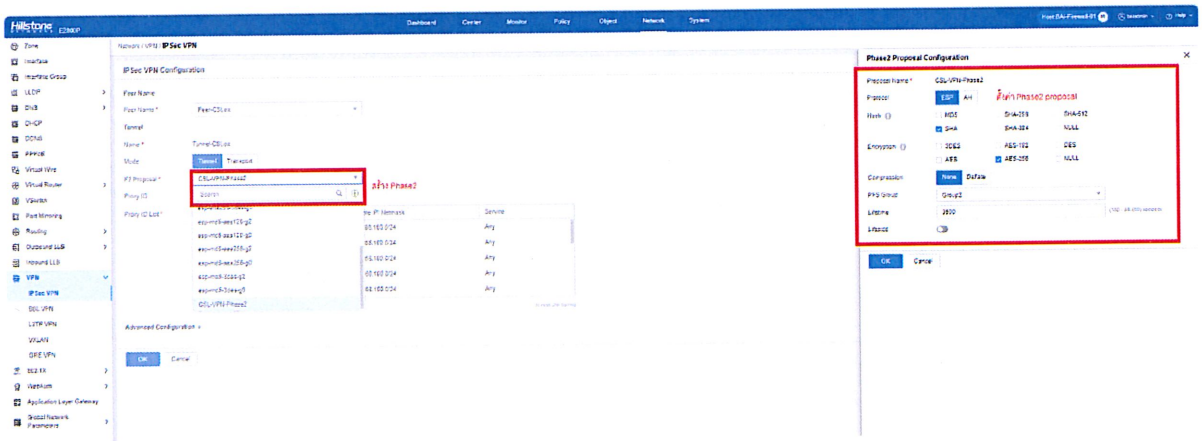
5.1.1. IPsec VPN



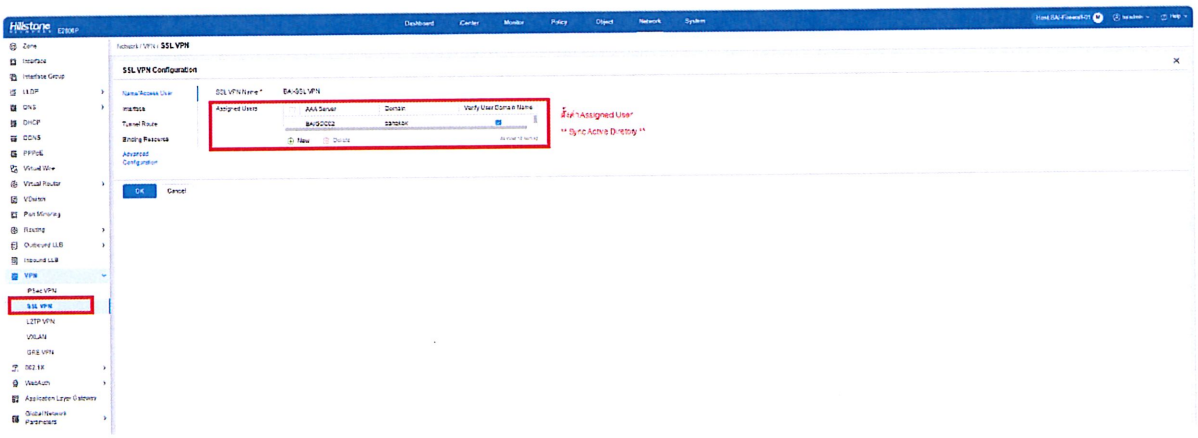




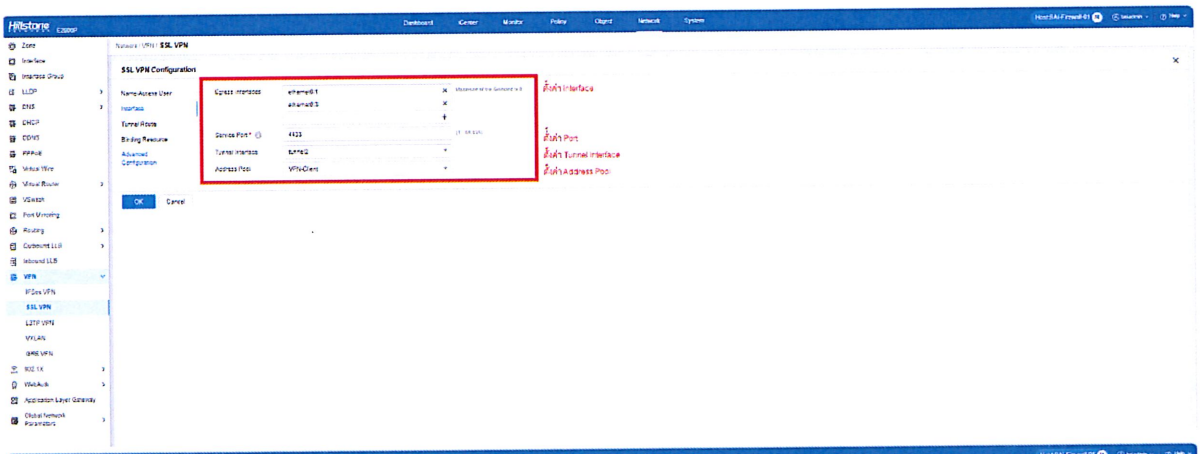

สร้าง Phase 1 Proposal
สร้าง Phase 1 Proposal


สร้าง Phase2
สร้าง Phase2 proposal

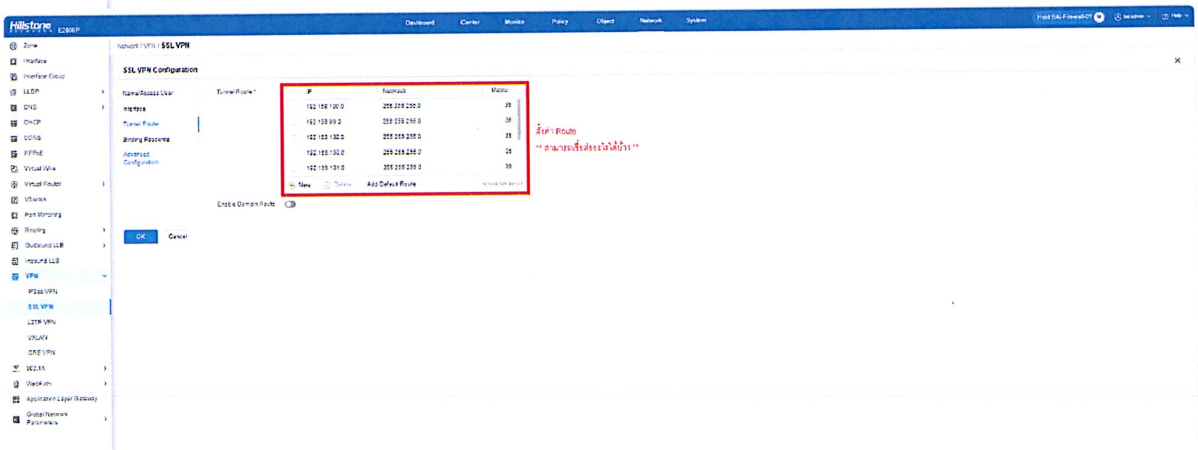
5.1.2. SSL VPN



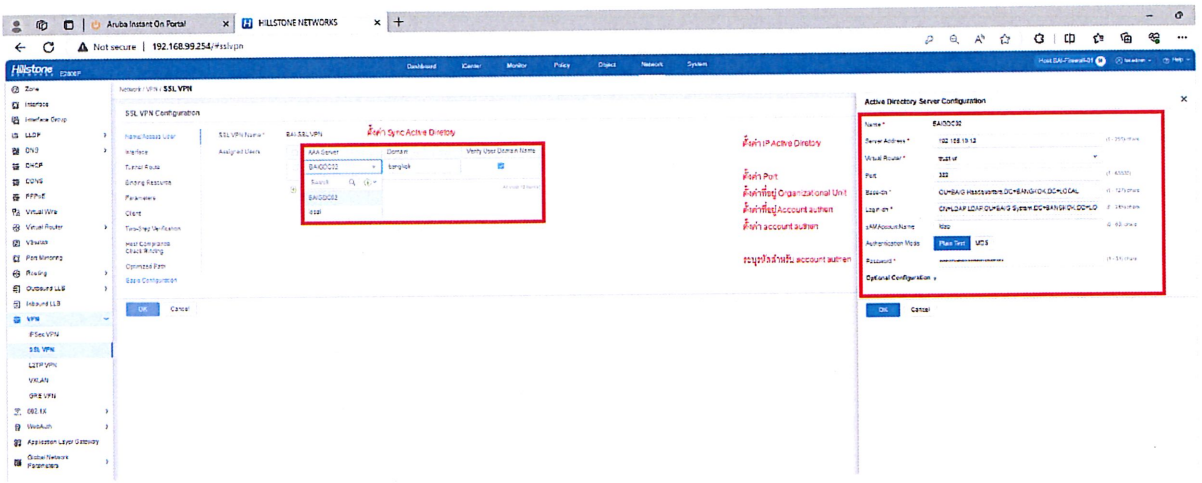
SSL VPN Configuration
ตั้งค่า Assigned User
** Sync Active Directory **

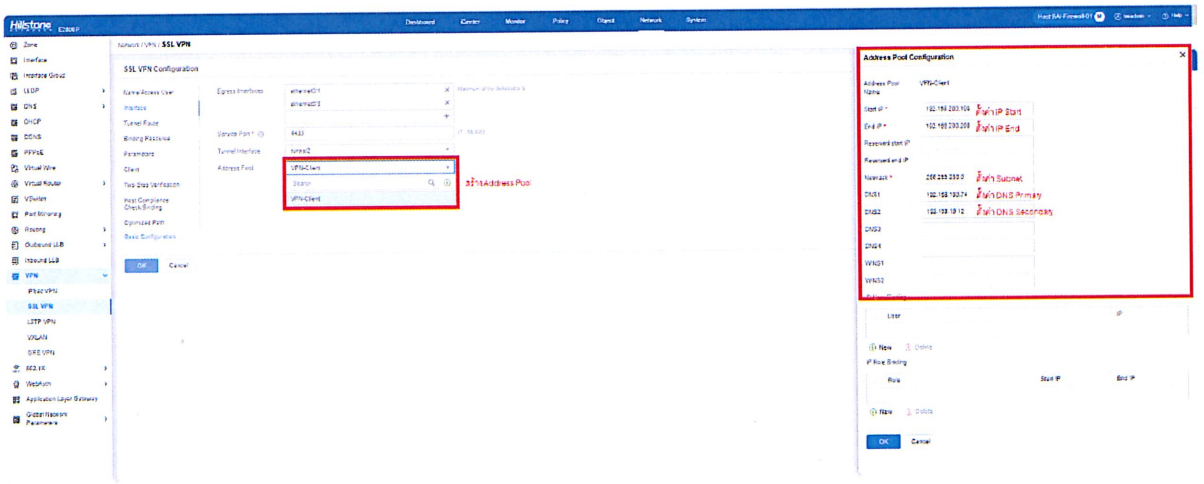


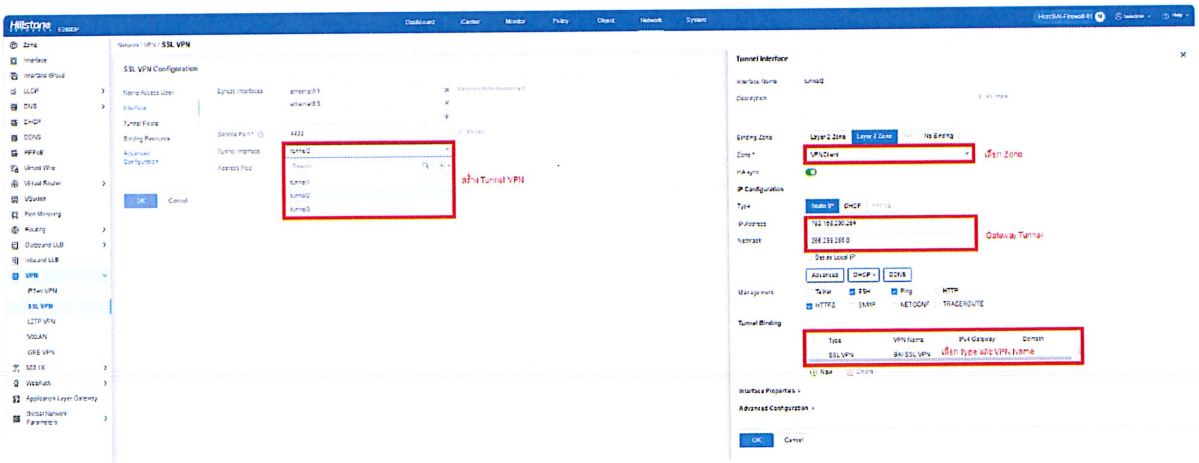
SSL VPN Configuration
ตั้งค่า Interface
ตั้งค่า Port
ตั้งค่า Tunnel Interface
ตั้งค่า Address Pool



SSL VPN Configuration
ตั้งค่า Route


ตั้งค่า Sync Active Directory
ตั้งค่า IP Active Directory
ตั้งค่า Port
ตั้งค่าที่อยู่ Organizational Unit
ตั้งค่าที่อยู่ Account authen
ตั้งค่า account authen
ระบุชื่อโดเมน account authen

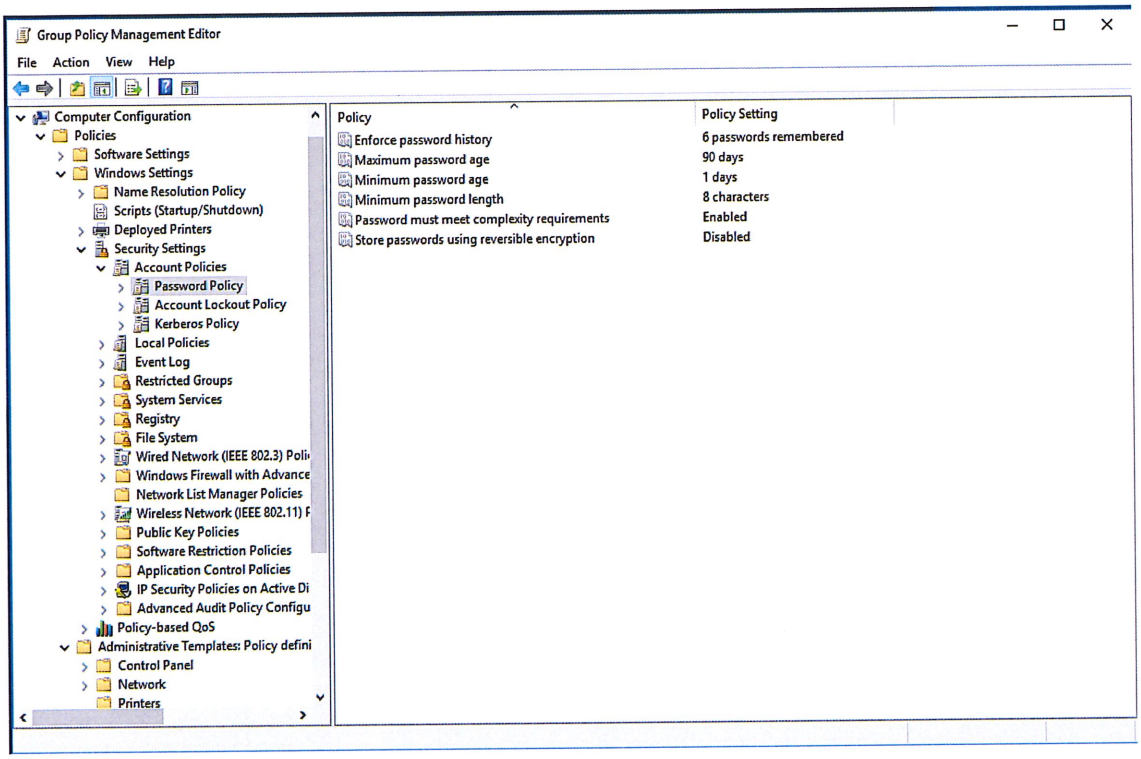

สร้าง Address Pool
ตั้งค่า IP Start
ตั้งค่า IP End
ตั้งค่า Subnet
ตั้งค่า DNS Primary
ตั้งค่า DNS Secondary


สร้าง Tunnel VPN
เลือก Zone
Gateway Tunnel
เลือก Type เป็น SSL VPN, Name

5.2. Active Directory (192.168.100.74)

5.2.1. Configuration Account Standard

5.2.1.1. Password Policy



5.2.1.1.1. Enforce password history ไม่สามารถใช้รหัสผ่านใหม่ซ้ำกับรหัสผ่านเก่า โดยจะจำรหัสผ่านเก่าไว้ตามจำนวนที่ให้กำหนด **"กำหนดไว้ 6 ครั้ง"**

5.2.1.1.2. Maximum password age: อายุสูงสุดของรหัสผ่านก่อนจะหมดอายุและถูกบังคับให้เปลี่ยนรหัสผ่านใหม่ มีค่าระหว่าง 1 – 999 วัน หรือ 0 คือ ไม่มีวันหมดอายุ **"กำหนดไว้ 90 วัน"**

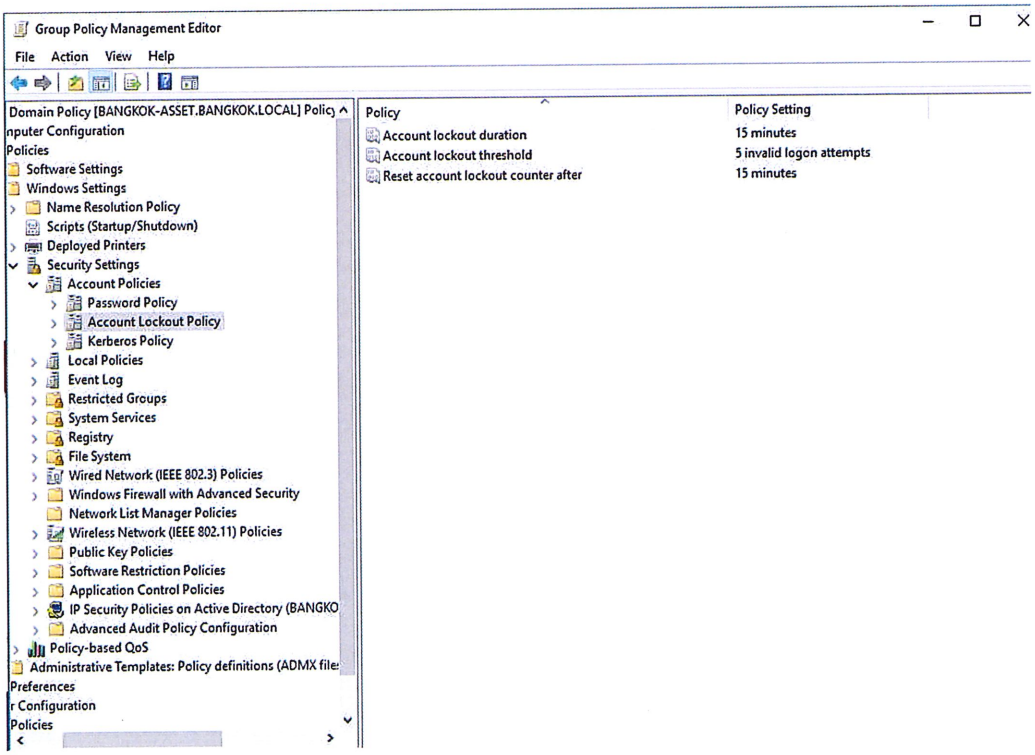
5.2.1.1.3. Minimum password age: อายุต่ำสุดของรหัสผ่านก่อนจะถูกบังคับให้เปลี่ยนรหัสผ่านใหม่ โดยต้องน้อยกว่าอายุสูงสุดของรหัสผ่าน ถ้าอายุสูงสุดเท่ากับ 0 ต้องตั้งค่าอายุต่ำสุดระหว่าง 0 – 998 วัน **"กำหนดไว้ 1 วัน"**

5.2.1.1.4. Minimum password length: ความยาวน้อยที่สุดของรหัสผ่าน มีค่าระหว่าง 1 – 14 ตัวอักษร หรือถ้าไม่ระบุจำนวนให้ใส่ค่า 0 **"กำหนดไว้ 8 ตัวอักษร"**

5.2.1.1.5. Password must meet complexity requirements: รหัสผ่านที่ต้องมีความซับซ้อน คือประกอบด้วยตัวเลข (0 – 9) ตัวอักษรพิมพ์ใหญ่ (A – Z) และพิมพ์เล็ก (a – z) รวมทั้งอักขระ(@#!) และไม่ให้เหมือนกับชื่อแอคเคานต์

5.2.1.1.6. Store password using reversible encryption: กำหนดให้ระบบปฏิบัติการเก็บรหัสผ่านโดยเข้ารหัสแบบย้อนกลับ (ค่าดีฟอลต์ คือ Disabled)

5.2.1.2. Account Lockout Policy



5.2.1.2.1. Account lockout duration: ระยะเวลาที่ยูสเซอร์แอคเคานต์ถูกล็อก มีค่าระหว่าง 1 – 99,999 นาที (ค่า 0 ต้องให้ผู้ดูแลระบบเท่านั้นจึงจะปลดล็อกได้) **“กำหนดไว้ 30 นาที”**

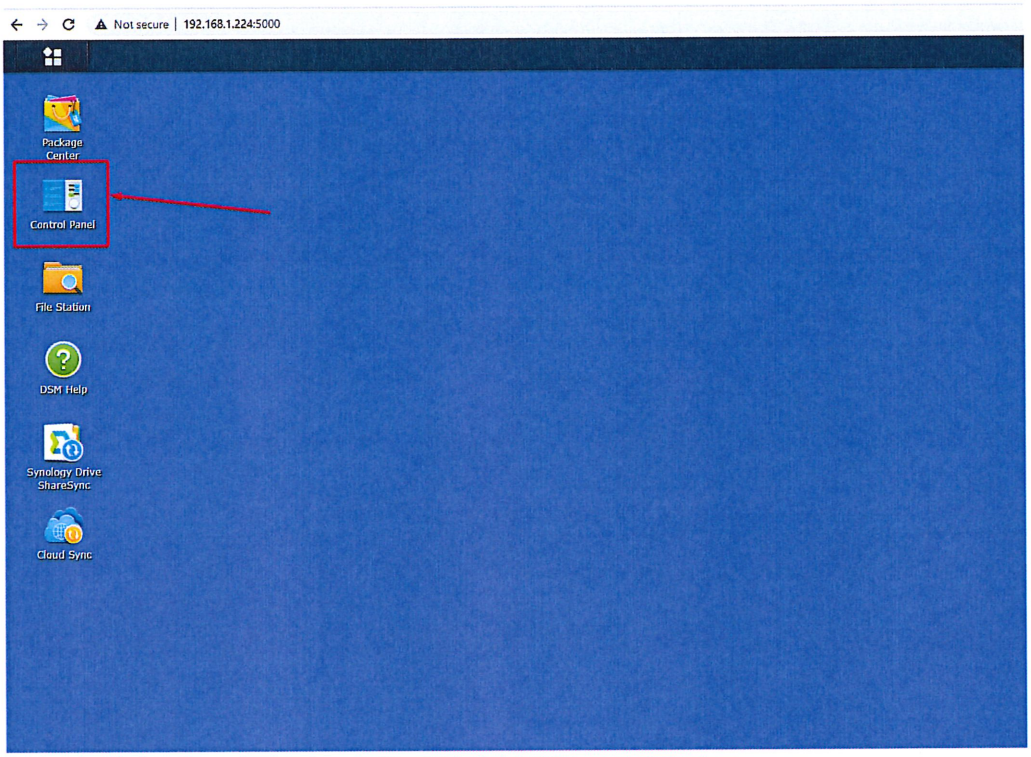
5.2.1.2.2. Account lockout threshold: จำนวนครั้งที่อนุญาตให้ยูสเซอร์สามารถพิมพ์รหัสผ่านผิดก่อนจะถูกเลือกยูสเซอร์แอคเคานต์ **“กำหนดไว้ 5 ครั้ง”**

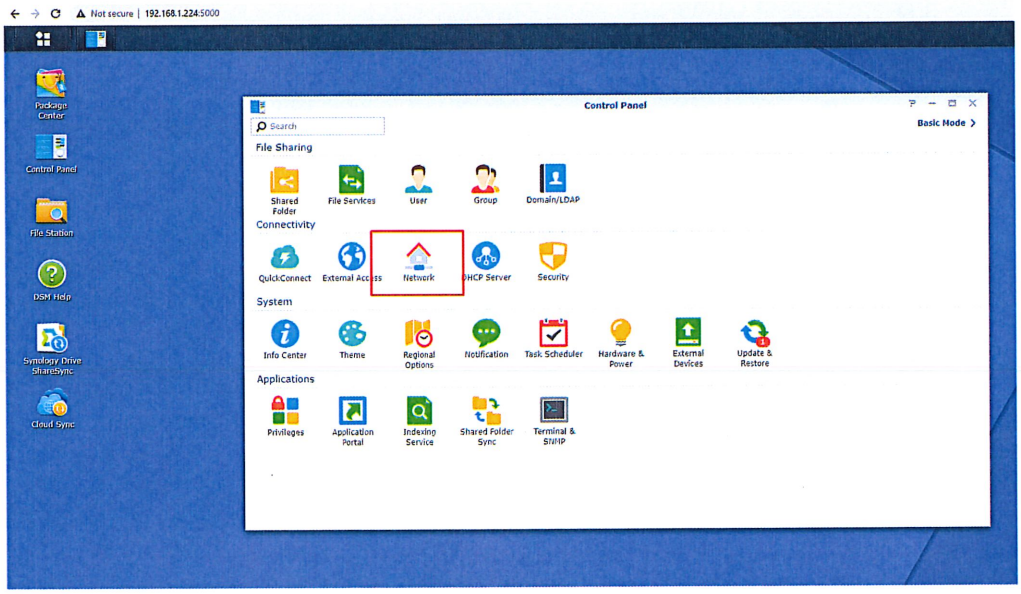
5.2.1.2.3. Reset account lockout counter after: ยกเลิกการล็อกแอคเคานต์หลังจากถูกล็อกผ่านไปตามจำนวนเวลาที่กำหนด **“กำหนดไว้ 15 นาที”**

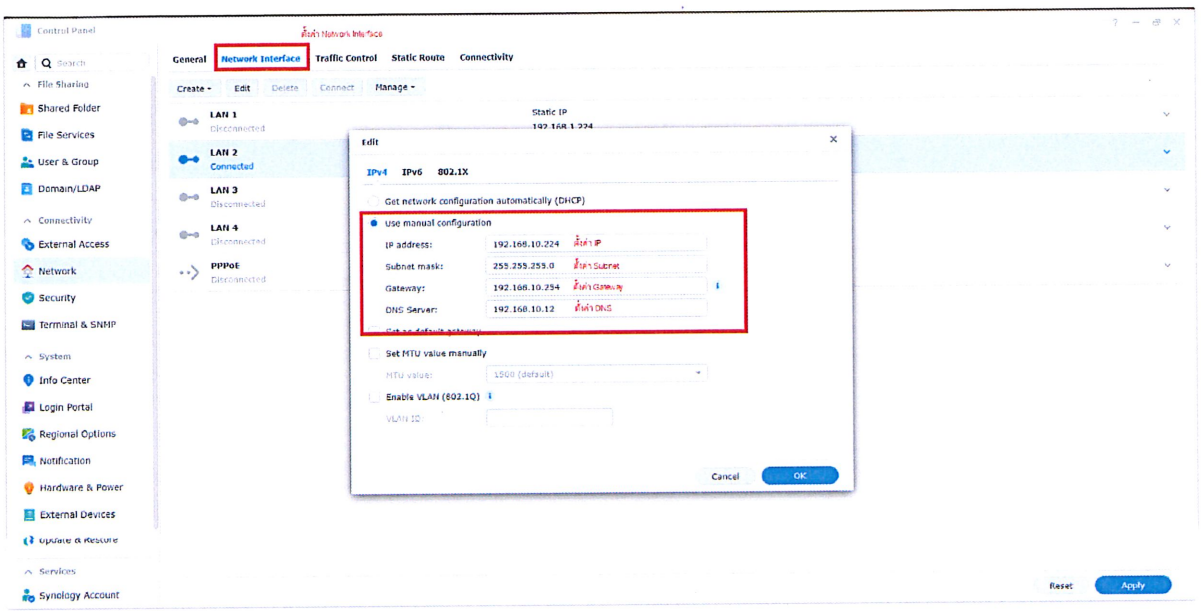
5.3. NAS Storage (192.168.10.224:5000)

5.3.1. วิธีการเข้าหน้าตั้งค่าเข้าผ่าน Browser และใส่ IP 192.168.10.224:5000

5.3.1.1. IP Configuration






Control Panel
ตั้งค่า Network Interface
General
Network Interface
Traffic Control
Static Route
Connectivity
Create
Edit
Delete
Connect
Manage
LAN 1
Disconnected
Static IP
LAN 2
Connected
LAN 3
Disconnected
LAN 4
Disconnected
PPPoE
Disconnected
File Sharing
Shared Folder
File Services
User & Group
Domain/LDAP
Connectivity
External Access
Network
Security
Terminal & SNMP
System
Info Center
Login Portal
Regional Options
Notification
Hardware & Power
External Devices
Update & Restore
Services
Synology Account
Edit
IPv4
IPv6
802.1X
Get network configuration automatically (DHCP)
Use manual configuration
IP address:
192.168.10.224
ตั้งค่า IP
Subnet mask:
255.255.255.0
ตั้งค่า Subnet
Gateway:
192.168.10.254
ตั้งค่า Gateway
DNS Server:
192.168.10.12
ตั้งค่า DNS
Set MTU value manually
MTU value:
1500 (default)
Enable VLAN (802.1Q)
VLAN ID:
Cancel
OK
Reset
Apply

ประวัติการการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	30 มีนาคม 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา
2	1.1	ปรับปรุงหลังจากติดตั้ง Firewall	1 สิงหาคม 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา
3	2.0	ปรับปรุงโครงสร้างระบบหลังย้ายสำนักงาน	20 มกราคม 2567	ชาญยุทธ วัฒนาศักดิกุล

ลงชื่อ_____

(ชาญยุทธ วัฒนาศักดิกุล)

ผู้รับผิดชอบ

วันที่ 20/1/67

ผู้อนุมัติ

ลงชื่อ_____

(ธนิศร ธนวงศ์เทพ)

ประธานเจ้าหน้าที่เทคโนโลยีสารสนเทศ

วันที่ 20/01/67

คู่มือสำหรับการใช้งานของ Admin Kintone

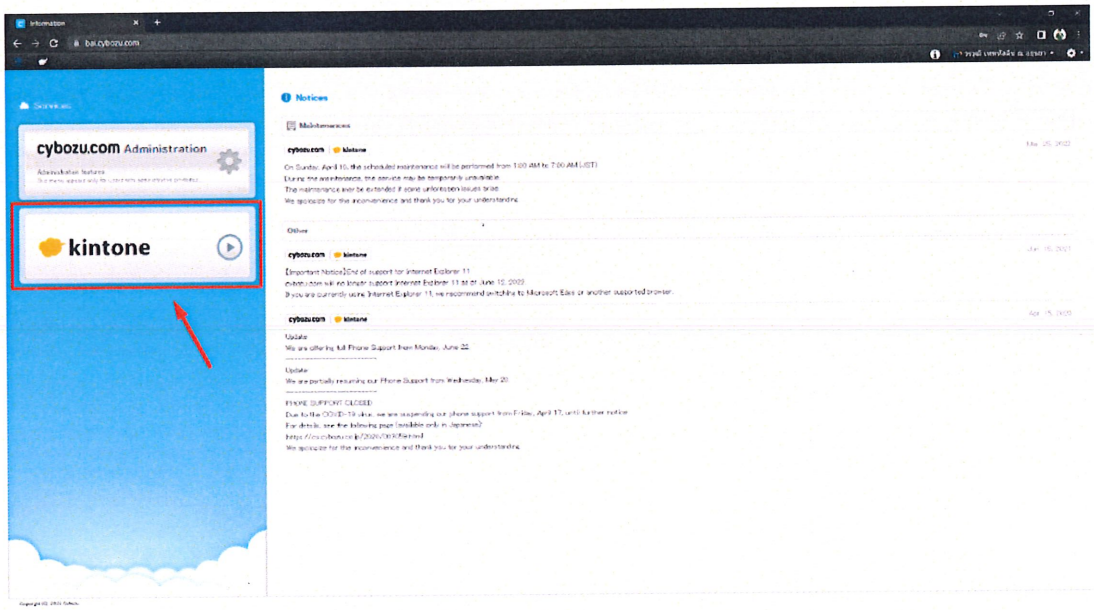
วัตถุประสงค์ เพื่อเป็นมาตรฐานในการใช้งาน User Administrator ภายในบริษัทให้ได้มีประสิทธิภาพ

ขั้นตอนการใช้งาน

1. Link สำหรับเข้า Kintone: bai.cybozu.com



1.1. ในหน้าแรกเป็นหน้า login ให้ใส่ username ในช่องหมายเลข 1 และใส่ password ในช่องหมายเลข 2 จากนั้นกดปุ่ม login ในกรอบหมายเลข 3

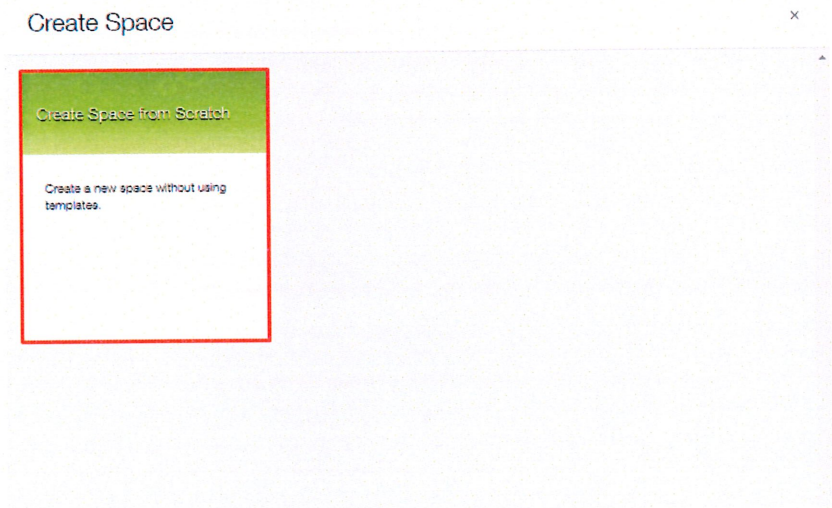


1.2. เมื่อทำการ login เข้ามาแล้ว ให้เรากดที่ปุ่มคำว่า kintone

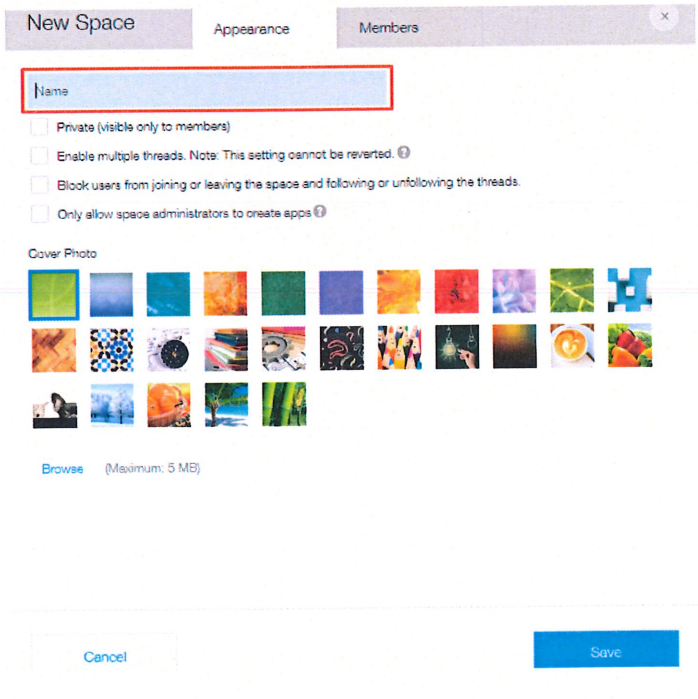
2. การสร้าง Spaces



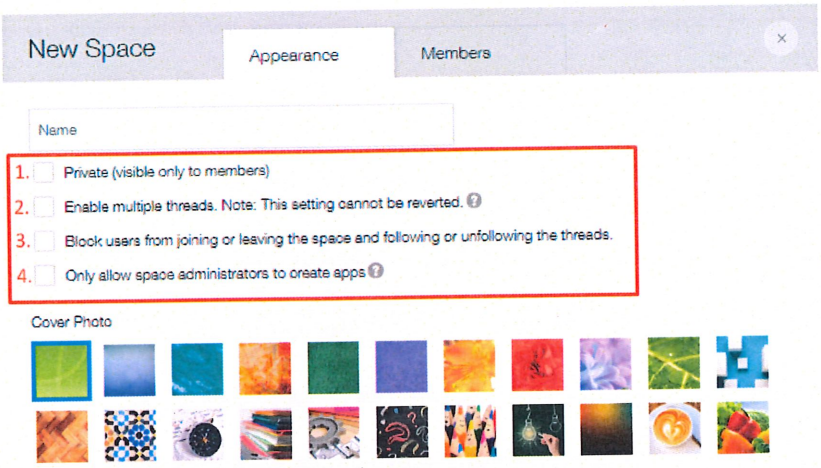
2.1. คลิกที่ปุ่ม + จากนั้นเลือก New Space



2.2. เลือก Create Space from Scratch



3. ตั้งชื่อ Space

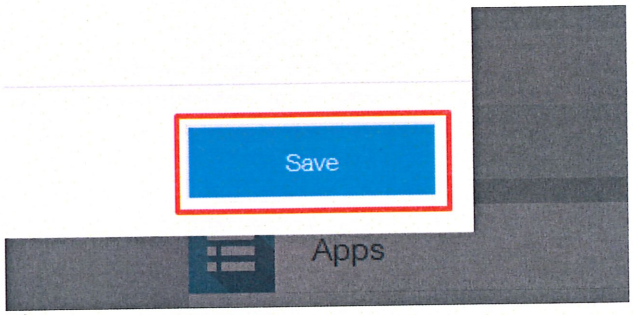


3.1. ส่วนตัว (มองเห็นได้เฉพาะสมาชิกเท่านั้น)

3.2. เปิดใช้งานหลายเธรด การทำเครื่องหมายที่ช่องนี้จะช่วยให้คุณสร้างชุดข้อความใหม่ใน Space ได้ ซึ่งมีประโยชน์สำหรับทีมของคุณในการสนทนาหัวข้อต่างๆ ในที่ต่างๆ ตัวเลือกนี้ยังเปิดใช้งาน Space portal ซึ่ง Space Administrator สามารถโพสต์ประกาศหรือแนบกราฟ Kintone เพื่อแบ่งปันกับทีม

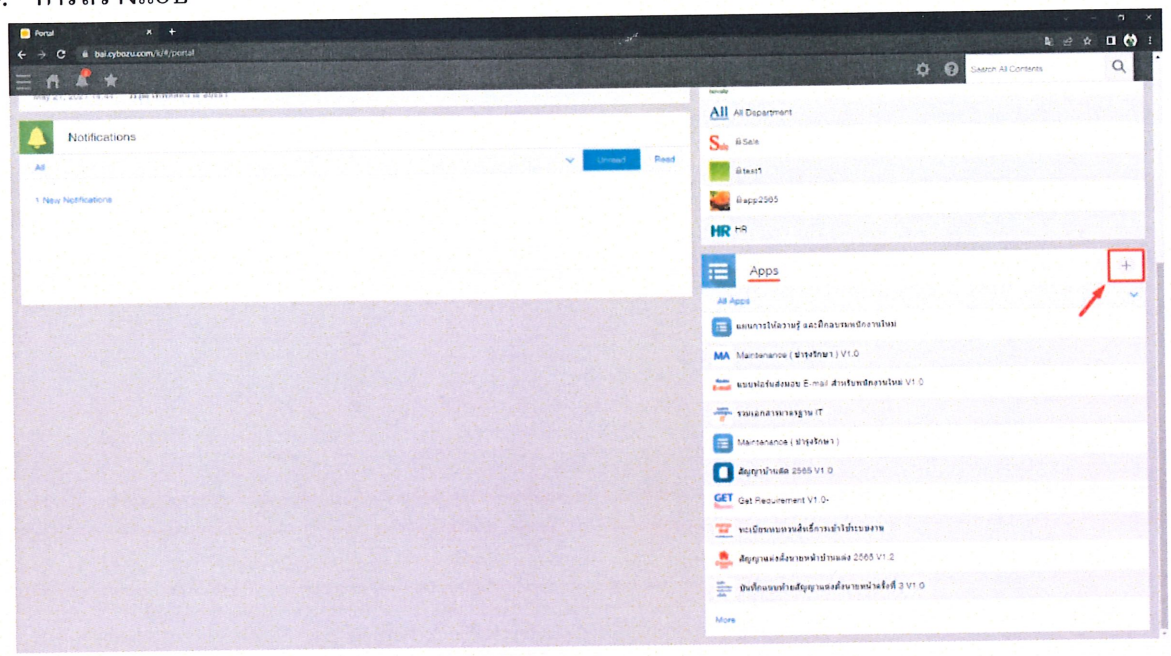
3.3. บล็อกผู้ใช้จาก space นี้

3.4. อนุญาตให้ผู้ดูแลระบบพื้นที่สร้างแอปเท่านั้น เลือกว่าจะอนุญาตเฉพาะผู้ดูแลระบบ Space หรือผู้ใช้ที่มีสิทธิ์สร้างแอปเพื่อสร้างแอปในพื้นที่นี้ คุณสามารถระบุผู้ดูแลระบบพื้นที่บนแท็บสมาชิก

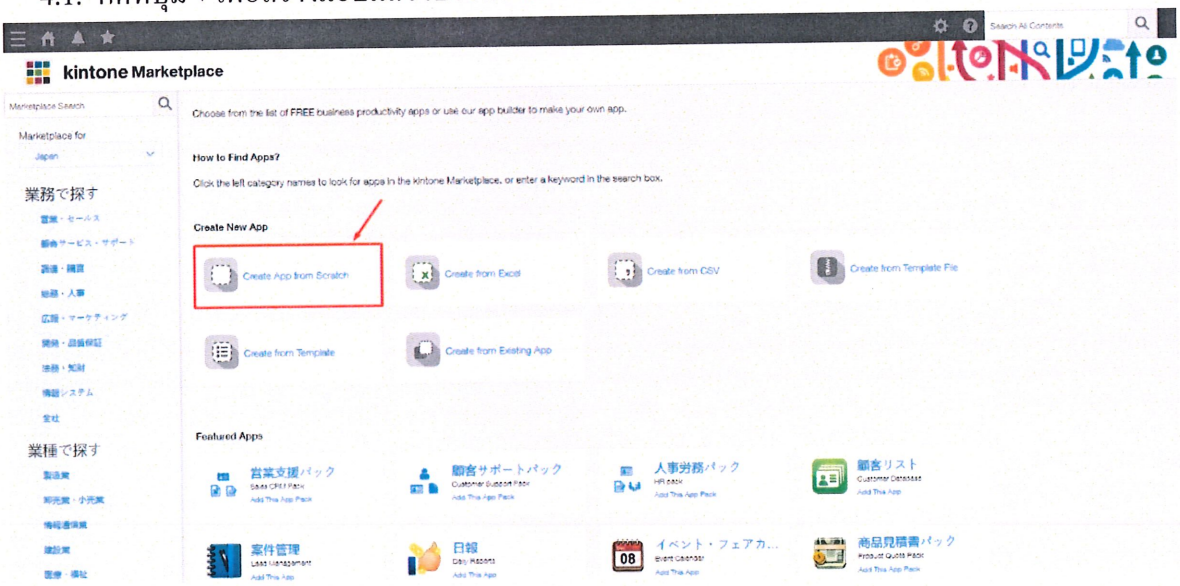


3.5. เสร็จแล้วให้คลิกที่ปุ่ม Save

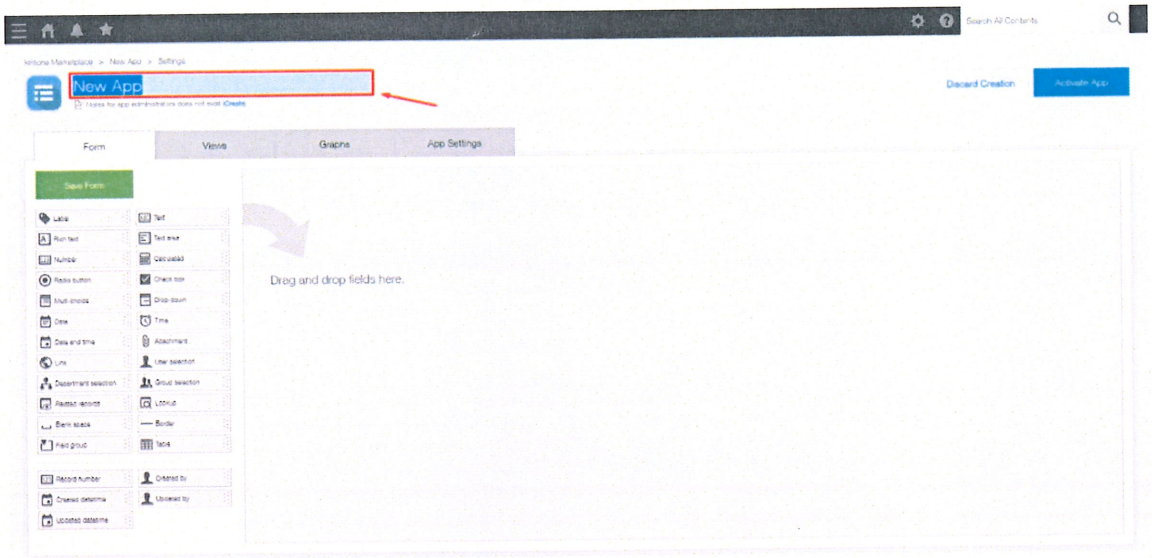
4. การสร้างแอป



4.1. กดที่ปุ่ม + เพื่อสร้างแอปแล้วไปยังหน้าการสร้างแอป

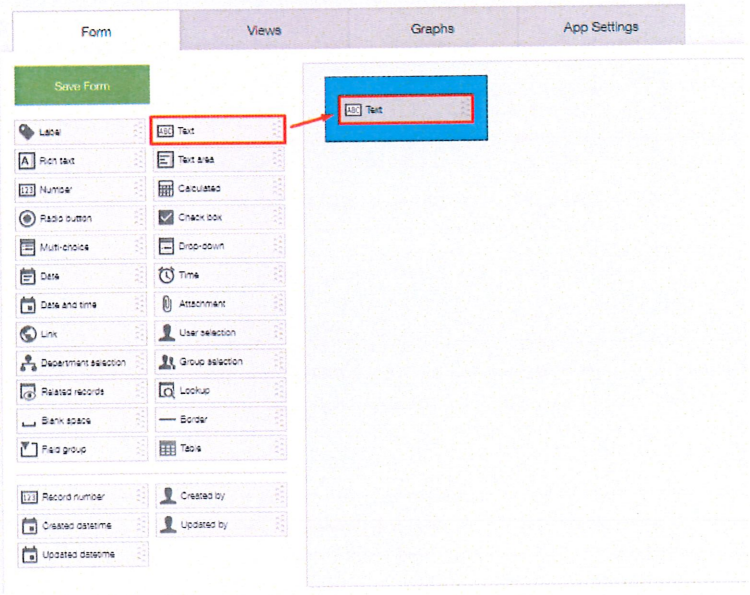


5. วิธีการสร้างแอป คลิกตัวเลือกแรก “Create App from Scratch” เพื่อสร้างหน้าเปล่า

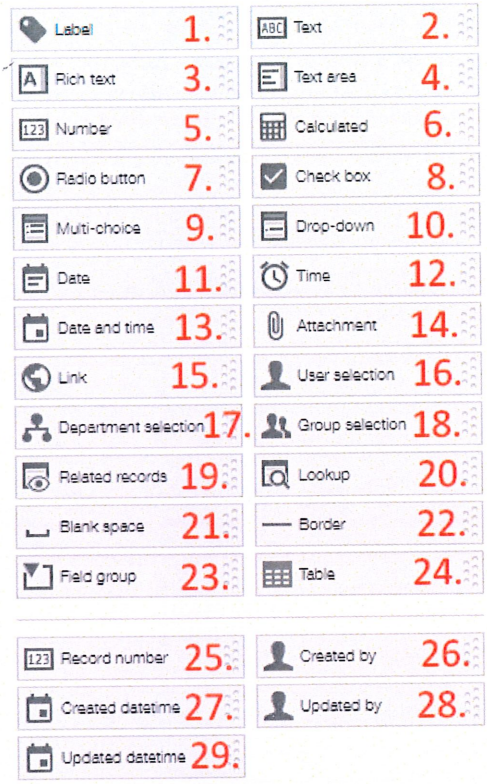


5.1. ขั้นตอนต่อไป ให้เราตั้งชื่อแอป

6. การตั้งค่าแบบฟอร์ม



6.1. ในหน้านี้เราสามารถจัดเรียงฟิลด์และจัดตำแหน่งได้อย่างอิสระโดยการลากไอคอนจากทางด้านซ้ายมาวางในส่วนต่างๆ



โดยไอคอนต่างๆทางด้านซ้ายมีหน้าที่การทำงานดังนี้

6.1.1. Label – เป็นเหมือนการติดฉลากข้อความ

6.1.2. Text – เป็นช่องให้พิมพ์ข้อความทั่วๆไป

6.1.3. Rich text – เป็นการพิมพ์ข้อความแบบมีเครื่องมือให้จัดเรียงให้สวยงาม

6.1.4. Text area – เป็นฟิลด์ที่สามารถพิมพ์ข้อความได้หลายบรรทัด

6.1.5. Number – เป็นการพิมพ์ตัวเลขทั่วไป

6.1.6. Calculated – สามารถใส่สูตรแล้วแสดงค่าที่คำนวนได้

6.1.7. Radio button – เป็นการสร้างปุ่มกดเพื่อเลือก

6.1.8. Check box – สร้างกล่องให้ทำเครื่องหมายได้หลายตัวเลือก

6.1.9. Multi-choice – เป็นการสร้างช่องที่มีหลายตัวเลือก

6.1.10. Drop-down – ฟิลด์ที่สามารถกดแล้วมีตัวเลือกแสดงลงมาให้เลือกหลายตัวเลือก

6.1.11. Date – เป็นช่องให้ใส่วันที่

6.1.12. Time – เป็นช่องแสดงเวลา ณ ตอนนั้น

6.1.13. Date and time – เป็นช่องให้ใส่วันที่และเวลา

6.1.14. Attachment – เป็นช่องสำหรับแนบไฟล์ต่างๆ

6.1.15. Link – เป็นช่องว่างให้ใส่ลิงค์

6.1.16. User selection – เป็นฟิลด์สำหรับเลือกผู้ใช้

6.1.17. Department selection – เป็นการเลือกค้นหาแผนกที่เราได้สร้างไว้

6.1.18. Group selection – เป็นฟิลด์สำหรับเลือกกลุ่ม

6.1.19. Related record – เป็นการแสดง record ที่ตรงกับเงื่อนไขที่ระบุโดยใช้ฟิลด์ record ที่เกี่ยวข้อง

6.1.20. Lookup – เป็นการดึงข้อมูลบางอย่างจากแอปอื่นเพื่อมาแสดง

6.1.21. Blank space – เป็นการใส่ช่องว่างเปล่าๆเพื่อเว้นระยะ

6.1.22. Border – เป็นฟิลด์เส้นขอบมีไว้เพื่อกำหนดขอบเบตระหว่างฟิลด์เพื่อจัดระเบียบของแบบฟอร์ม

6.1.23. Field group – เป็นการจัดกลุ่มของฟิลด์

6.1.24. Table – เป็นการสร้างตารางโดยสามารถลากฟิลด์ที่เหมือนกันลงมาใส่ตารางได้

6.1.25. Record number – ทุกครั้งที่มีการเพิ่ม record หมายเลขจะถูกกำหนดให้ฟิลด์โดยอัตโนมัติ

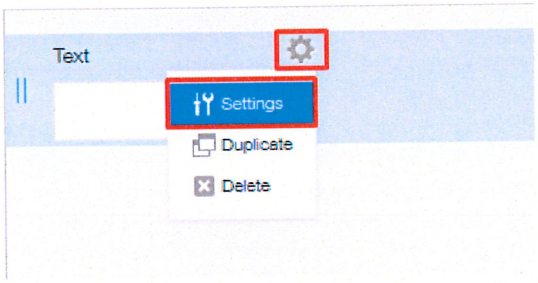
6.1.26. Created by – เป็นการดึงค่าผู้ทำมาแสดงโดยอัตโนมัติ

6.1.27. Created datetime – ใส่วันที่และเวลาโดยอัตโนมัติเมื่อมีการบันทึก record

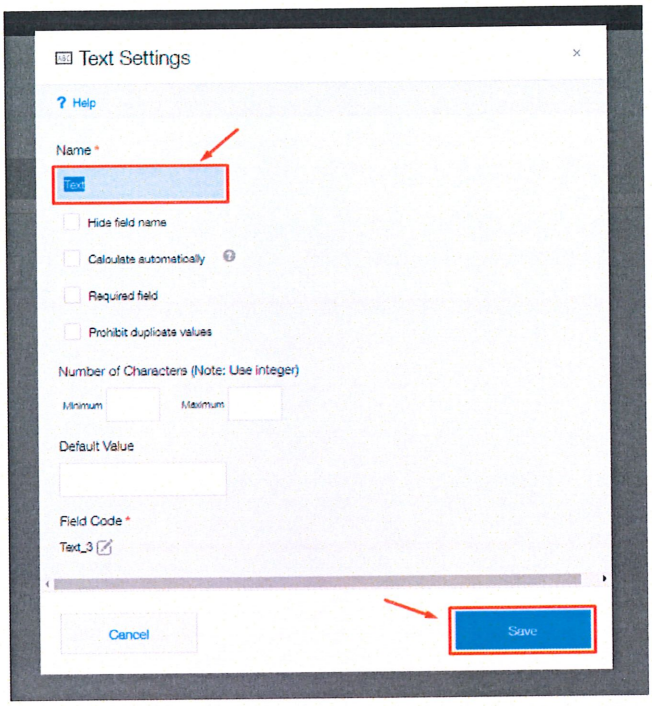
6.1.28. Updated by – เป็นการดึงค่าผู้แก้ไขมาแสดงโดยอัตโนมัติ

6.1.29. Updated datetime – วันที่และเวลาที่บันทึกจะถูกเปลี่ยนและบันทึกโดยอัตโนมัติ

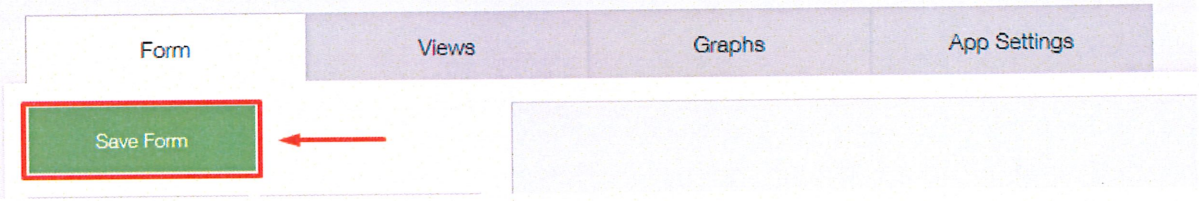
7. วิธีการเปลี่ยนชื่อของฟิลด์



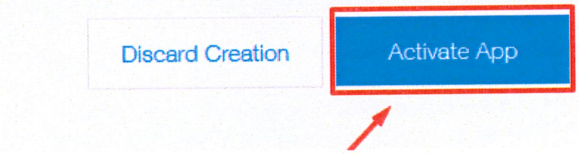
7.1. วางเมาส์เหนือไอคอนฟันเฟือง คลิกที่คำว่า Settings



7.2. ใส่ชื่อที่เราต้องการตั้งในฟิลด์ แล้วคลิกปุ่ม Save



7.3. เมื่อเสร็จสิ้นการตั้งค่ารายการ หากไม่มีปัญหาใดๆ ให้คลิก Save Form



7.4. คลิก Activate App เพื่อเริ่มใช้งานแอป

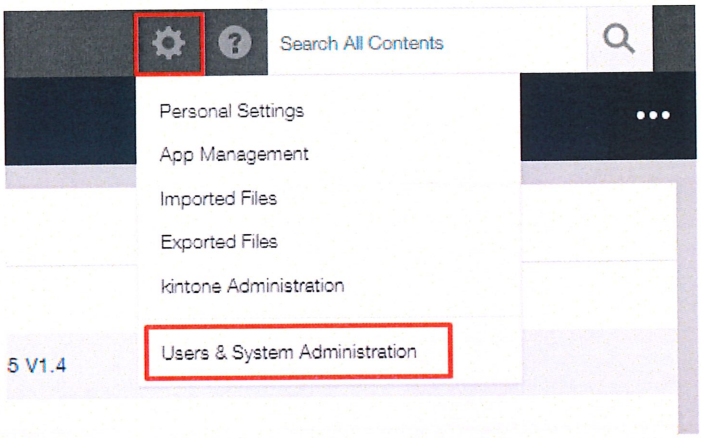
8. การสร้างแอปเสร็จสมบูรณ์ ตอนนี้คุณมีกล่องสำหรับจัดการงานของทีมแล้ว ลงทะเบียนงาน กำหนดบุคคล และแชร์งานกับทีมโดยใช้แอปเพื่อแสดงงานของทีม



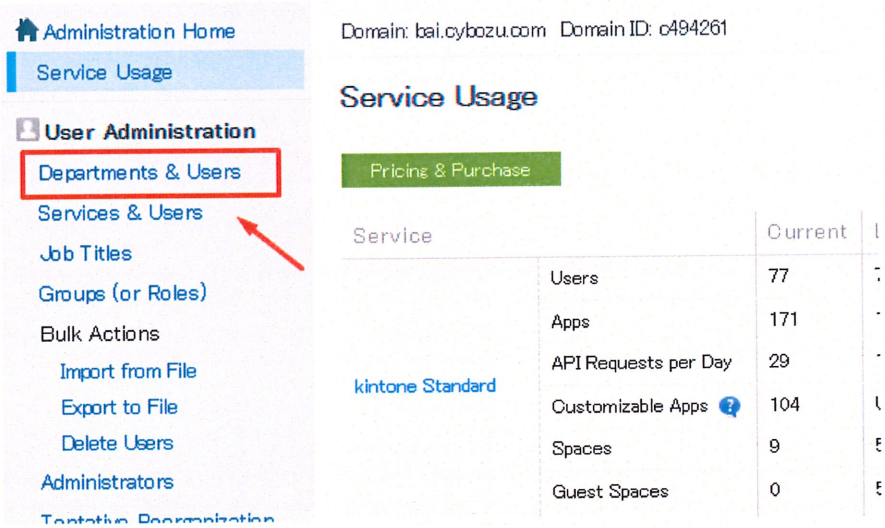
Tips: เพิ่มแอปที่ใช้บ่อยใน "รายการโปรด" คลิกไอคอนหมุดที่ด้านขวาเพื่อบันทึกลงในรายการโปรด ทำให้สามารถกรองและค้นหาแอปที่บันทึกไว้ในรายการโปรดได้ในหน้าบนสุด

9. ลงทะเบียนผู้ใช้ kintone

9.1. เมื่อสร้างแอปเสร็จสมบูรณ์ ในขั้นตอนถัดไป เราจะลงทะเบียนผู้ใช้แอป



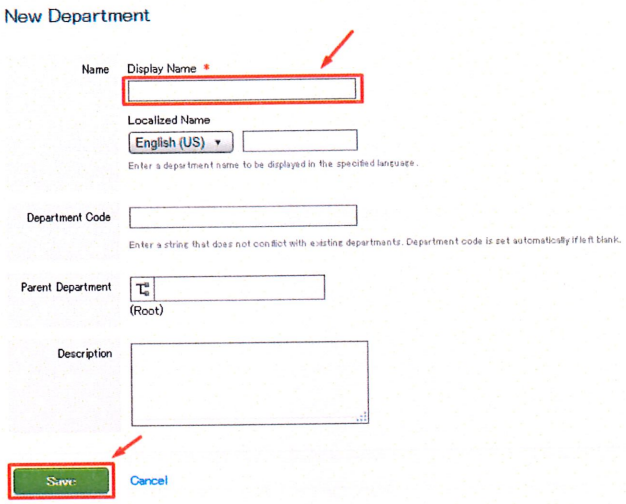
9.2. ไปที่มุมบนขวา คลิกที่รูปฟันเฟือง แล้วไปที่ Users & System Administration



9.3. คลิกที่ Departments & Users

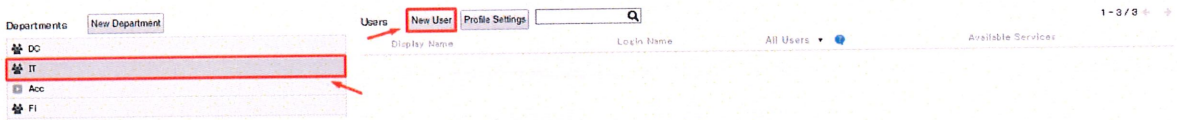


9.4. คลิกที่ปุ่ม New Department

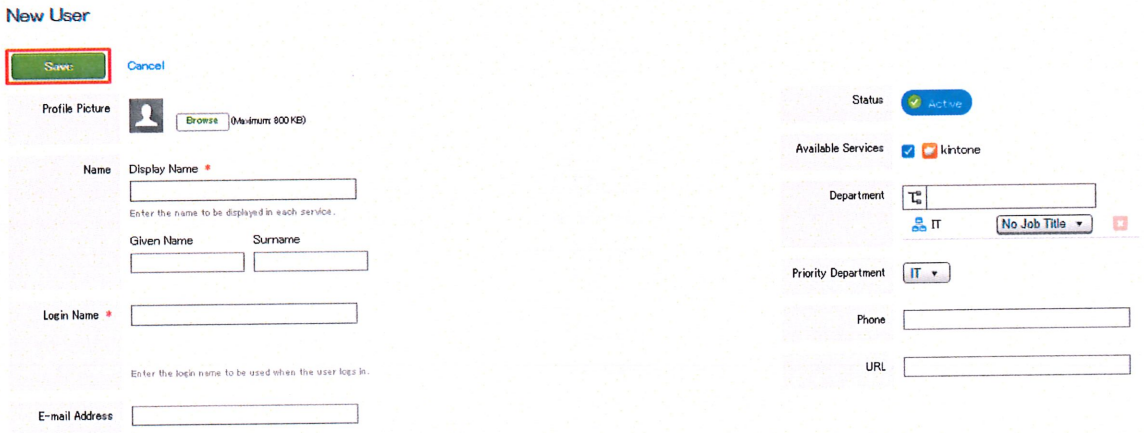


9.5. ป้อนชื่อในกล่อง Display Name เสร็จแล้วคลิกที่ปุ่ม Save

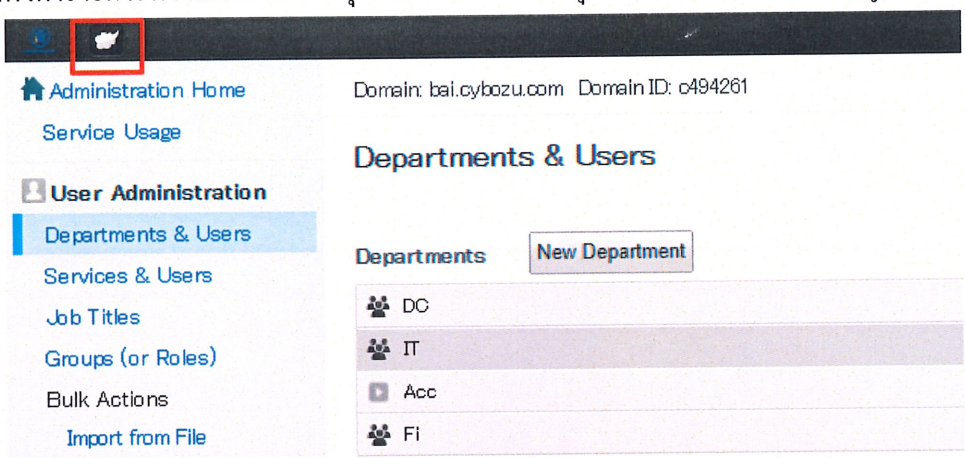
10. วิธีเพิ่มผู้ใช้ในกลุ่ม



10.1.คลิกที่ชื่อกลุ่ม แล้วคลิกปุ่ม New User เพื่อไปยังหน้าการลงทะเบียนผู้ใช้

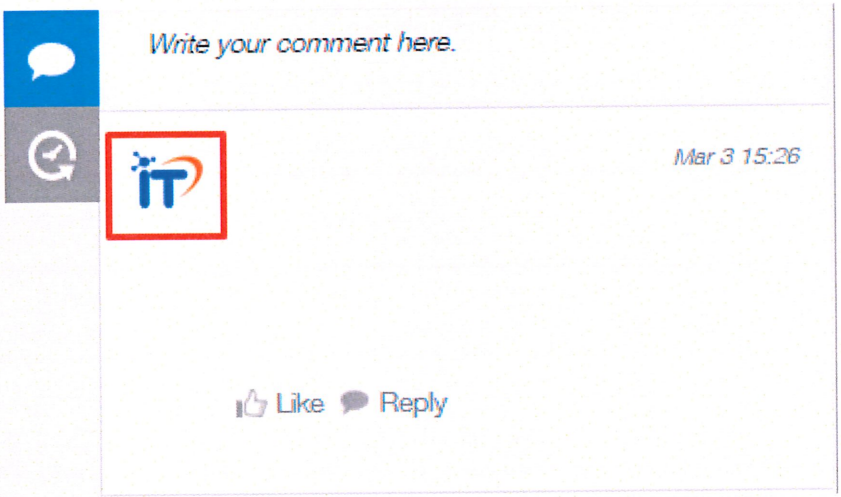


10.2.ตั้งค่ารายการที่จำเป็นแล้วคลิกปุ่ม Save เป็นการสิ้นสุดขั้นตอนการลงทะเบียนผู้ใช้



10.3.คลิกไอคอนรูปก้อนเมฆที่ด้านบนซ้ายเพื่อกลับไปยังหน้าหลัก

10.4.ผู้ใช้สามารถแก้ไขภาพและข้อมูลของผู้ใช้ เช่น ข้อมูลติดต่อ ได้ในภายหลัง



10.5.ผู้ใช้สามารถเปลี่ยนภาพไอคอนที่แสดงข้างชื่อของตนได้ตลอดจนแก้ไขข้อมูล เช่น ข้อมูลติดต่อ และวันเกิด ในขั้นตอนการลงทะเบียนผู้ใช้เริ่มต้น การตั้งค่าฟิลด์ที่จำเป็น เช่น ชื่อที่แสดง ชื่อล็อกอิน และรหัสผ่าน

11. วิธีการใช้งานแอปที่เราสร้าง



11.1.ดูที่รายชื่อแอปทางด้านขวามือ เลือกกดเข้าแอปที่เราต้องการ จากนั้นกดปุ่ม + ด้านบนขวา



11.2.ทำการกรอกข้อมูลต่างๆให้ครบถ้วน จากนั้นกดปุ่ม Save ด้านบนซ้าย

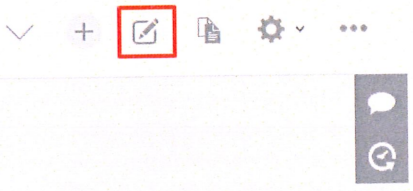


11.3.เราจะทำการลงทะเบียนงานของสมาชิกอื่นๆด้วย

12. วิธีแก้ไขและเปลี่ยนแปลงเนื้อหาที่ลงทะเบียน



12.1.หากมีการเปลี่ยนแปลงในเนื้อหาที่ลงทะเบียน คุณจะต้องแก้ไขบันทึก

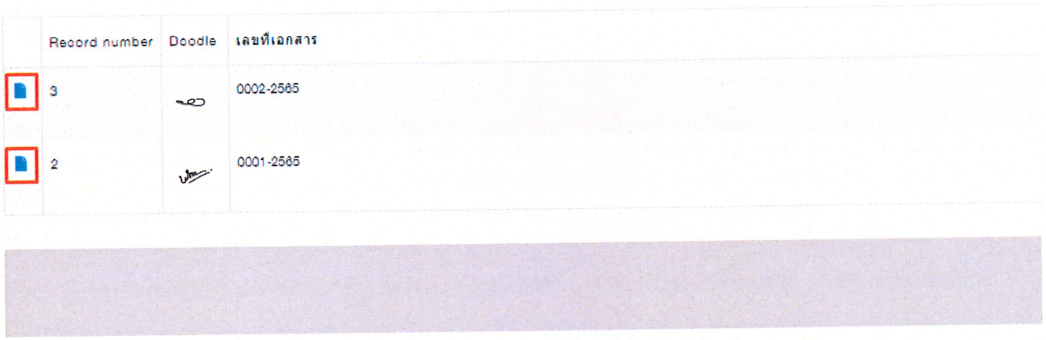


12.2.กดที่ไอคอนตามภาพอยู่ที่มุมบนด้านขวา คุณสามารถแก้ไขเนื้อหาต่างๆได้

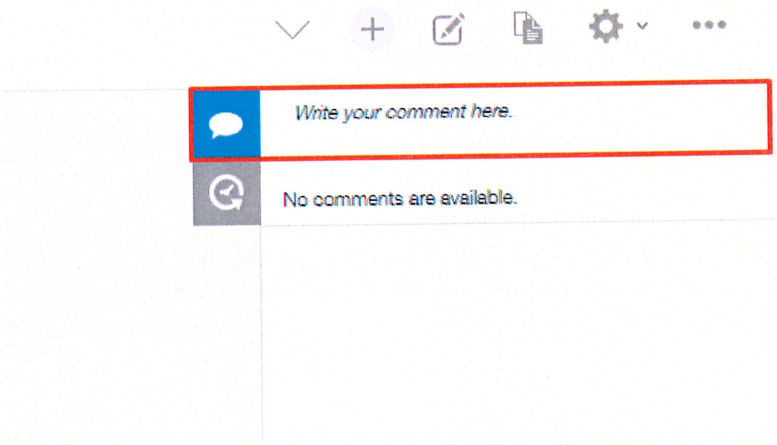


12.3.เมื่อแก้ไขเสร็จแล้ว ให้กดปุ่ม Save ด้านบนซ้าย

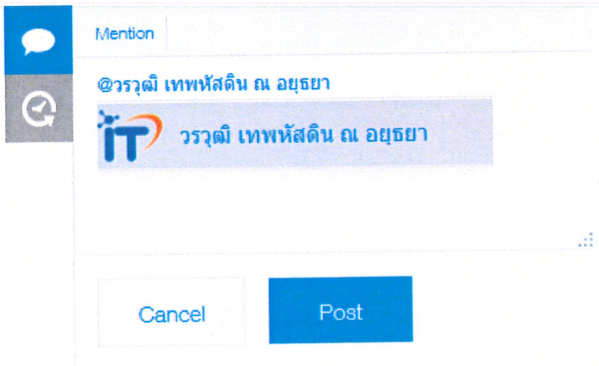
13. Comment functions



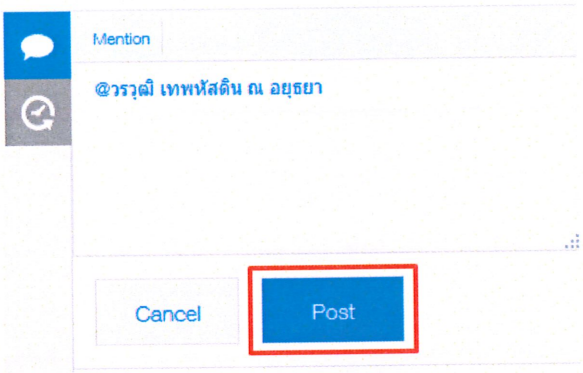
13.1.เปิดรายการบันทึกแล้วคลิกไอคอนสีน้ำเงินทางด้านซ้ายเพื่อเปิดหน้าจอรายละเอียด



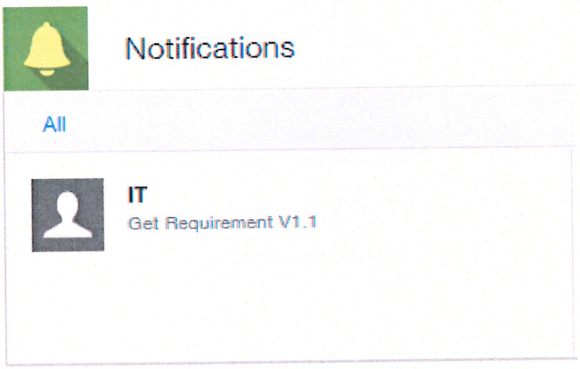
13.2.จากนั้นคลิก "แสดงความคิดเห็น" ที่ด้านขวาของหน้าจอรายละเอียด



13.3.พิมพ์เครื่องหมาย @ ป้อนชื่อของบุคคลที่คุณต้องการแสดงความคิดเห็น เมื่อคุณพิมพ์ชื่อของบุคคลนั้นจนถึงจุดใดจุดหนึ่ง รายชื่อผู้ใช้ที่เกี่ยวข้องจะปรากฏขึ้น คลิกที่ชื่อที่คุณต้องการแสดงความคิดเห็น



13.4.ป้อนความคิดเห็นของคุณแล้วคลิก "โพสต์"

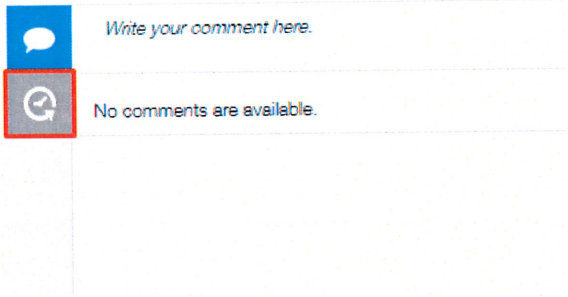


13.5.คุณจะได้รับแจ้งความคิดเห็นที่ส่งถึงคุณในพอร์ทัล kintone

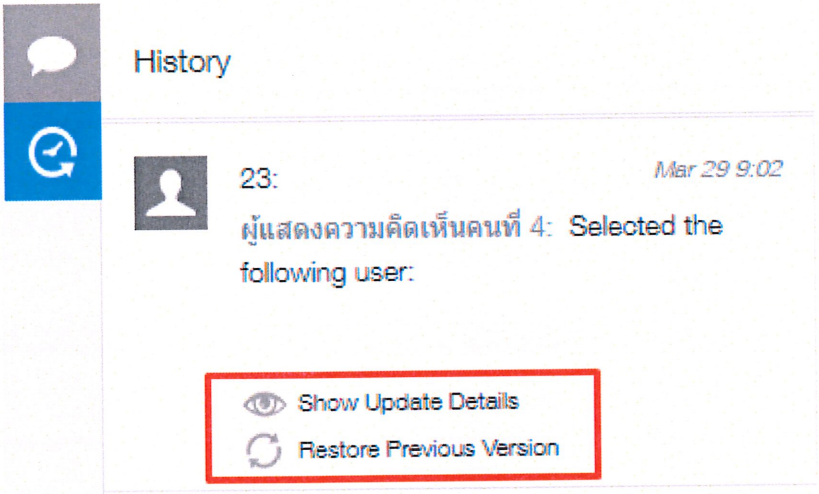
หมายเหตุ แอป Kintone มีฟังก์ชัน "ประวัติการแก้ไข" ซึ่งจะบันทึกโดยอัตโนมัติว่าใครเป็นผู้เปลี่ยนแปลงรายการใด เมื่อแชร์ข้อมูลบนซอฟต์แวร์ เช่น Excel จะเป็นเรื่องง่ายที่จะลืมว่าไฟล์ใดเป็นไฟล์ล่าสุด หรือมีการเปลี่ยนแปลงใดบ้างฟังก์ชันประวัติการแก้ไขไม่เพียงแต่ป้องกันสถานการณ์ดังกล่าว แต่ยังช่วยให้ผู้ใช้สามารถเปลี่ยนกลับเป็นข้อมูลเก่าได้ ในกรณีที่มีคนเขียนทับไฟล์โดยไม่ได้ตั้งใจ ช่วยป้องกันปัญหาที่มักเกิดขึ้นเมื่อแชร์ข้อมูล



13.6.เปิดหน้าจอรายการบันทึกและคลิกไอคอนสีน้ำเงินทางด้านซ้ายเพื่อเปิดหน้าจอรายละเอียด

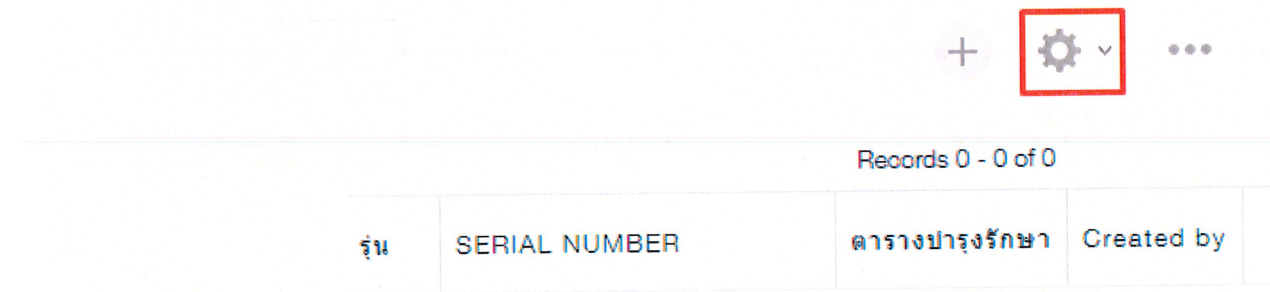


13.7.คลิกไอคอนที่ด้านขวาของหน้าจอรายละเอียด

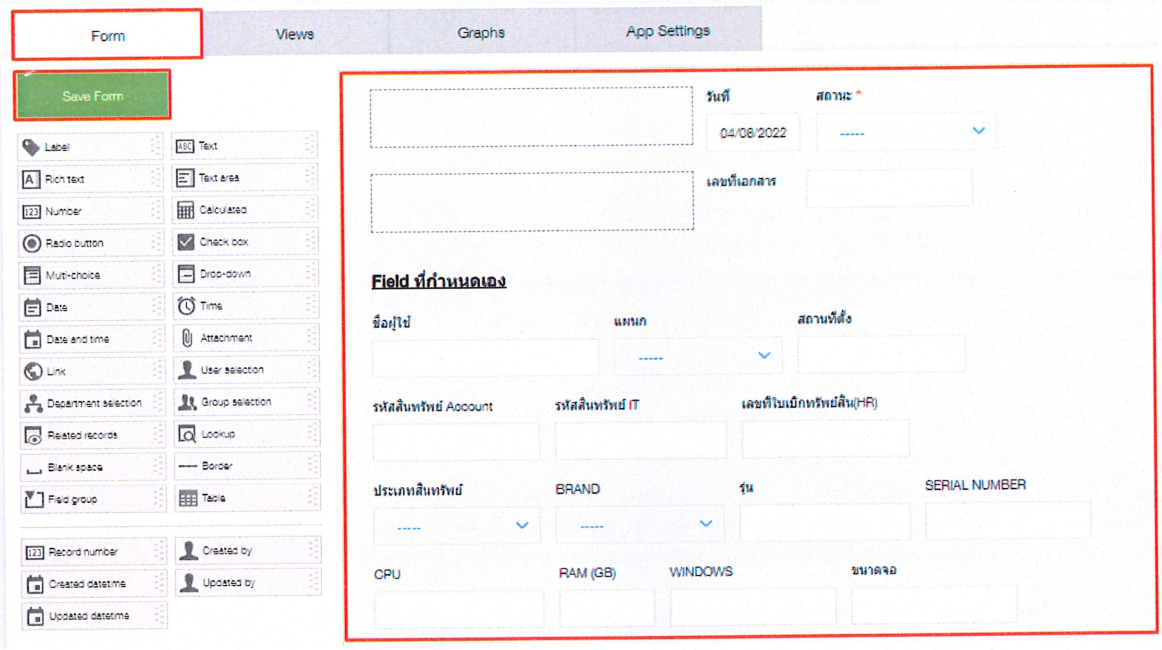


13.8.ตรวจสอบประวัติการแก้ไข และเปลี่ยนกลับเป็นเวอร์ชันเก่าหากจำเป็นโดยคลิกที่ "Show Update Details" ส่วนที่เปลี่ยนแปลงจะถูกเน้น หากต้องการเลิกทำการเปลี่ยนแปลงนี้ ให้คลิกปุ่ม "Restore Previous Version" ด้านล่าง

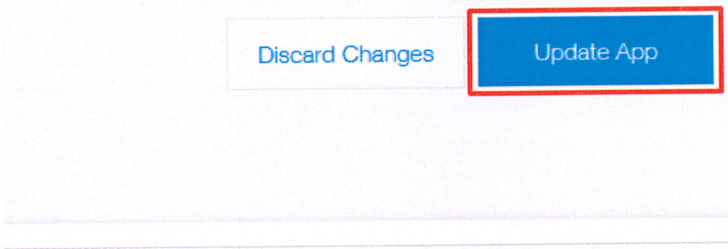
14. การแก้ไขแบบฟอร์ม



14.1.ไปที่หน้าแอป จากนั้นกดที่รูปฟันเฟืองด้านบนขวา

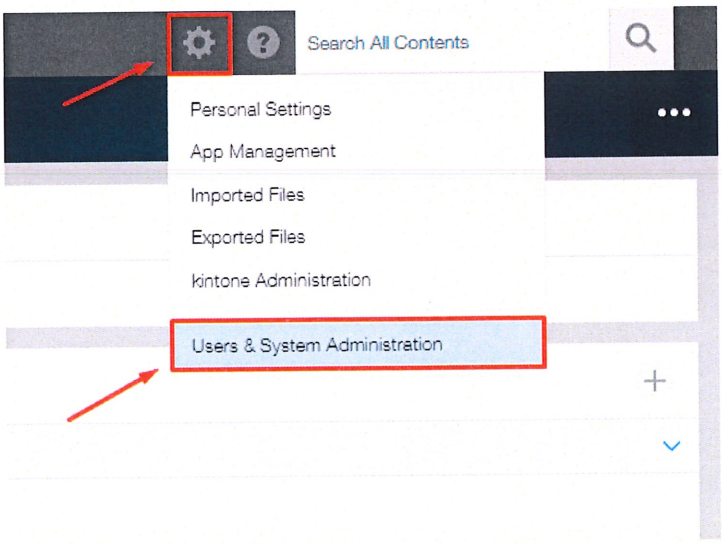


14.2. ในหน้า Form นี้ ฟิลด์ทางด้านขวามือเราสามารถแก้ไขได้เลย เมื่อแก้ไขเสร็จแล้วให้กดปุ่ม Save ด้านบนซ้าย

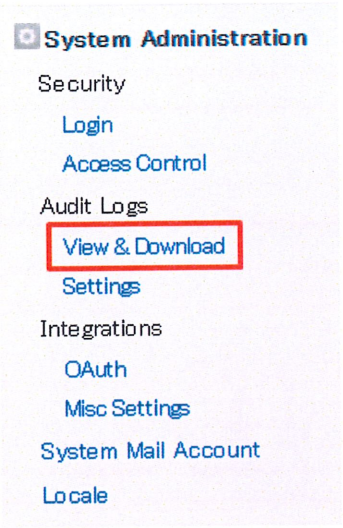


14.3. เสร็จแล้วให้กดที่ปุ่ม Update App ทางด้านบนขวา

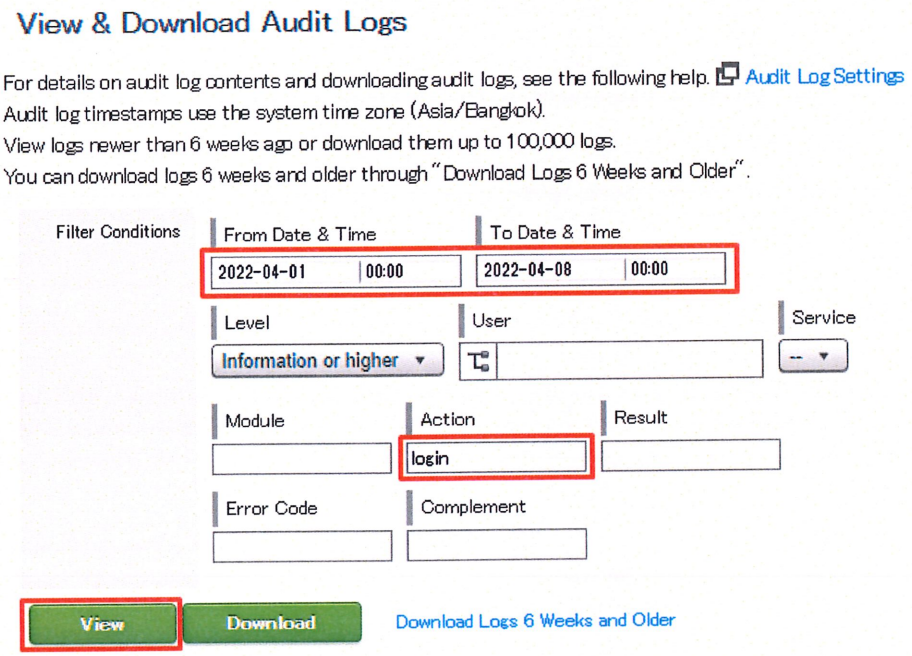
15. วิธีการ Save Log



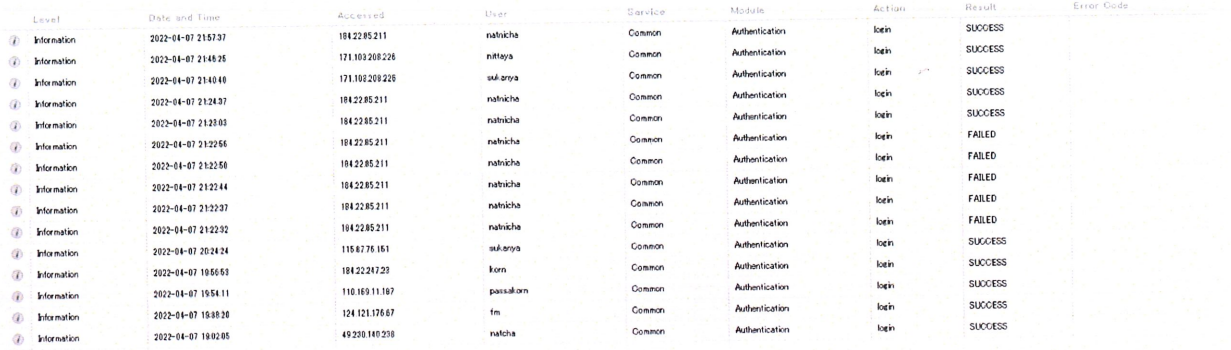
15.1.กดที่รูปฟันเฟืองด้านบนขวา แล้วคลิกที่ Users & System Administration



15.2.คลิกที่ View & Download

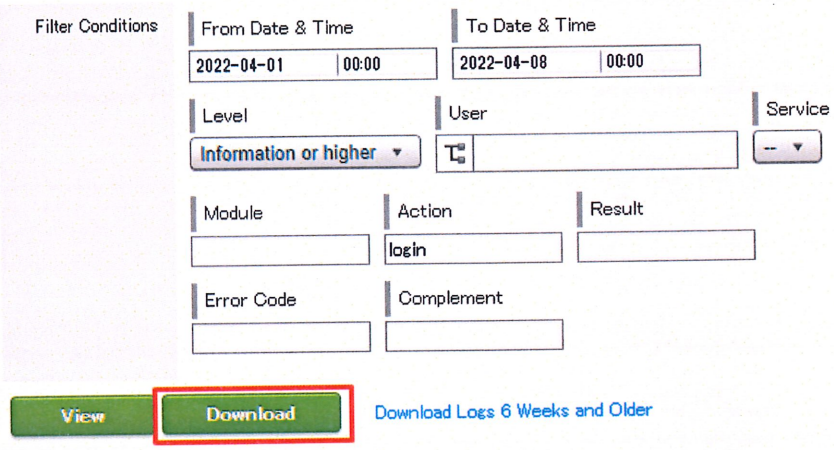


15.3.เลือกวันที่เริ่มต้นและสิ้นสุดที่ต้องการ จากนั้นเลือกดูคำว่า Login แล้วคลิกที่ปุ่ม View เพื่อตรวจสอบข้อมูล

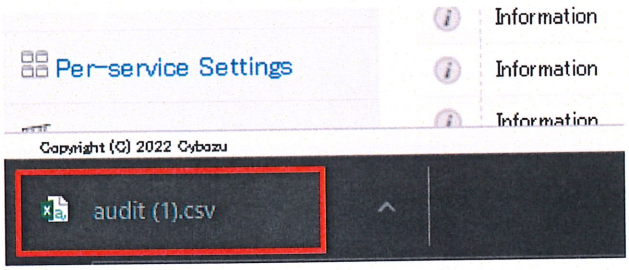


Level	Date and Time	Accessed	User	Service	Module	Action	Result	Error Code
Information	2022-04-07 21:57:37	184.22.85.211	natnicha	Common	Authentication	login	SUCCESS	
Information	2022-04-07 21:46:25	171.100.208.226	nittaya	Common	Authentication	login	SUCCESS	
Information	2022-04-07 21:40:40	171.100.209.226	sukanya	Common	Authentication	login	SUCCESS	
Information	2022-04-07 21:24:07	184.22.85.211	natnicha	Common	Authentication	login	SUCCESS	
Information	2022-04-07 21:23:03	184.22.85.211	natnicha	Common	Authentication	login	SUCCESS	
Information	2022-04-07 21:22:56	184.22.85.211	natnicha	Common	Authentication	login	FAILED	
Information	2022-04-07 21:22:50	184.22.85.211	natnicha	Common	Authentication	login	FAILED	
Information	2022-04-07 21:22:44	184.22.85.211	natnicha	Common	Authentication	login	FAILED	
Information	2022-04-07 21:22:37	184.22.85.211	natnicha	Common	Authentication	login	FAILED	
Information	2022-04-07 21:22:32	184.22.85.211	natnicha	Common	Authentication	login	FAILED	
Information	2022-04-07 20:24:24	115.67.76.161	sukanya	Common	Authentication	login	SUCCESS	
Information	2022-04-07 19:56:53	184.22.247.23	korn	Common	Authentication	login	SUCCESS	
Information	2022-04-07 19:54:11	110.169.11.187	passakorn	Common	Authentication	login	SUCCESS	
Information	2022-04-07 19:38:20	124.121.176.67	fm	Common	Authentication	login	SUCCESS	
Information	2022-04-07 19:02:05	49.230.140.238	natcha	Common	Authentication	login	SUCCESS	

15.4.ตัวอย่างข้อมูลที่เราเลือกกรองตามวันที่ และ Action คือ Login

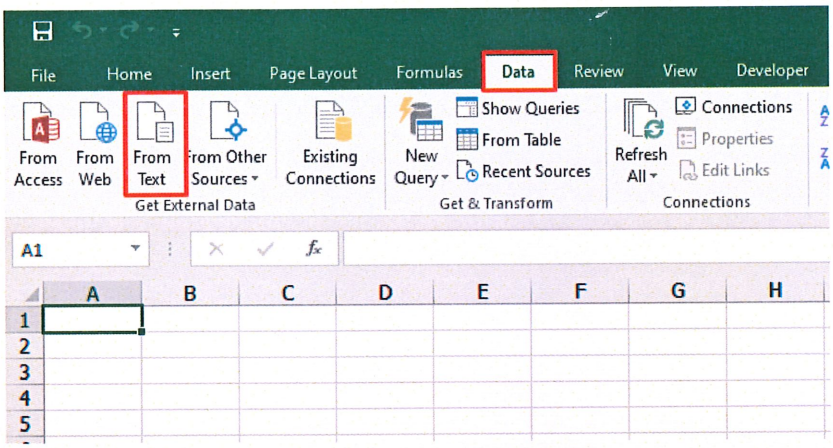


15.5.เมื่อตรวจสอบข้อมูลแล้ว หากต้องการดาวน์โหลด ให้คลิกที่ปุ่ม Download

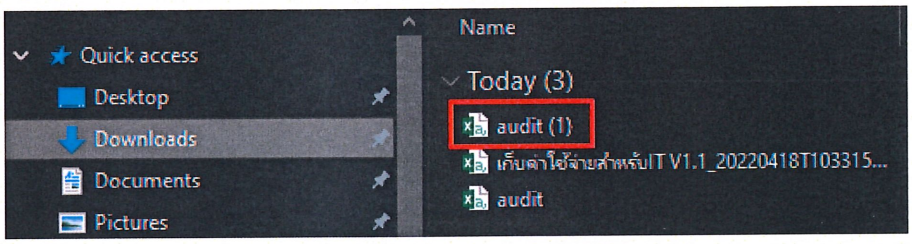


15.6.ทำการดาวน์โหลดไฟล์เรียบร้อย

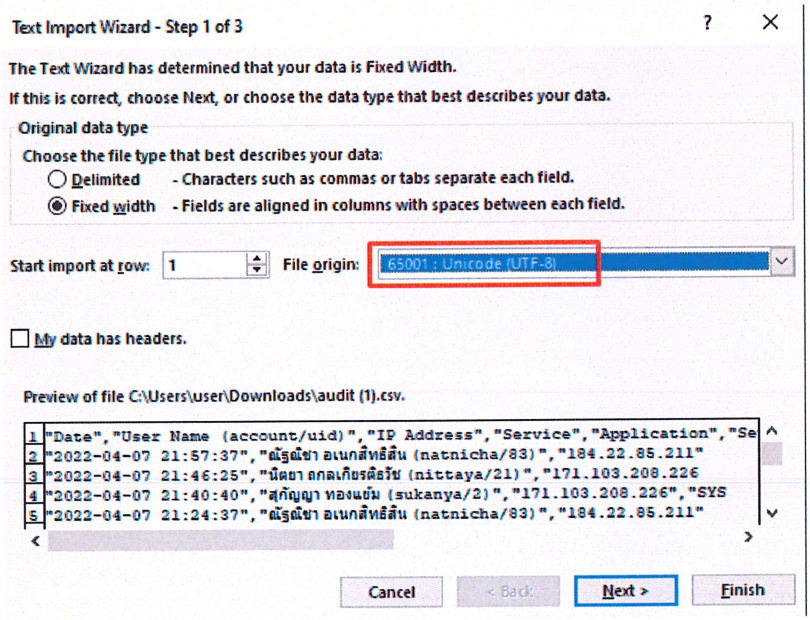
16. วิธีเปิดไฟล์ Logs



16.1.เปิด Excel จากนั้นไปที่ Data แล้วคลิกที่ From Text

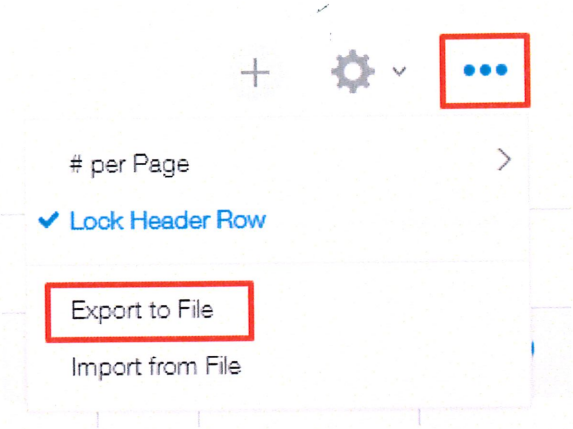


16.2.เลือกไฟล์ที่เราได้ทำการดาวน์โหลดไว้

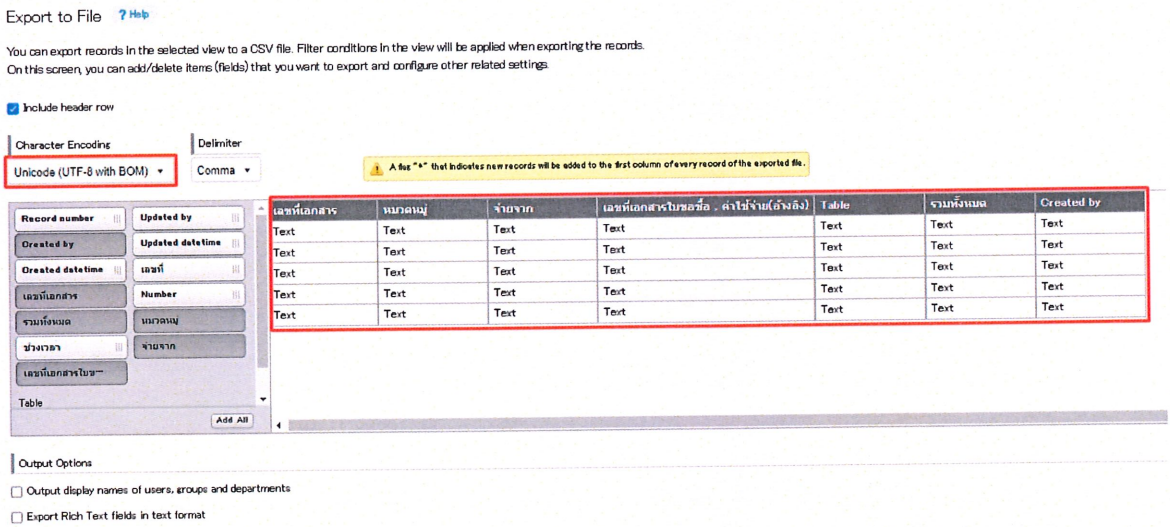


16.3.เลือก Unicode (UTF-8) จากนั้นกด Next -> Next -> Finish -> OK

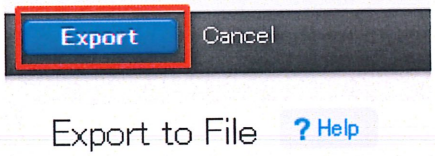
17. วิธีการ Export File



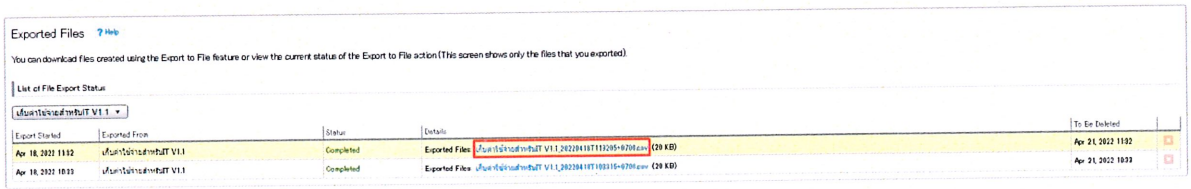
17.1.เข้า Apps ที่เราต้องการ คลิกที่ Options ด้านบนขวา แล้วไปที่ Export to File



17.2.เลือกตัวอักษรเป็น Unicode (UTF-8 with BOM) จากนั้นเลือกคอลัมน์ที่เราต้องการแสดง



17.3.เสร็จแล้วคลิกที่ปุ่ม Export ด้านบนขวา



17.4.จากนั้นจะมีรายการให้เลือกดาวน์โหลด คลิกที่ชื่อไฟล์เพื่อดาวน์โหลด

ลงชื่อ วรวุฒิ เทพทัสดิน

(วรวุฒิ เทพทัสดิน ณ อยุธยา)

ผู้รับผิดชอบ

วันที่ 25 มี.ค 65

ผู้อนุมัติ

ลงชื่อ ธนิพร ธนวงศ์เกษม

(ธนิพร ธนวงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 25 มี.ค. 65

ขั้นตอนการสำรวจความพึงพอใจผู้ใช้งาน

วัตถุประสงค์

1. เพื่อเป็นการสำรวจความพึงพอใจของผู้ใช้คอมพิวเตอร์ในบริษัท อยู่ในระดับใด
2. เพื่อนำมาปรับปรุง และพัฒนาเพื่อให้ตอบสนองต่อความต้องการของผู้ใช้

ขั้นตอนการสำรวจ

1. ตั้งคำถามที่จะถามกันในแผนก IT
2. เมื่อได้คำถามที่จะถามแล้ว นำมาทำแบบสอบถามผ่าน Google form
3. ส่งไปยังกลุ่มเป้าหมาย หรือผู้ใช้งานที่ต้องการ
4. โดยกำหนดการส่งแบบสอบถามในเดือนตุลาคมของทุกปี
5. โดยความคาดหวังที่จะได้ผลการตอบแบบสอบถามคืนภายในวันที่ 31 ตุลาคม
6. ทำการรวบรวม และสรุปผลที่ได้จากการสำรวจ ในเดือนพฤศจิกายน
7. ข้อมูลที่ได้แบ่งเป็น 2 ส่วน
   7.1. ความพึงพอใจ ผลที่ได้จะนำไปแก้ไข และปรับปรุงในส่วนที่ผู้ใช้งานไม่พึงใจสูงสุดใน 3 อันดับแรก แล้วพิจารณาอันดับถัดไป
   7.2. ความต้องการเพิ่มเติมของผู้ใช้งาน จะนำรวบรวมเป็นโครงการสำหรับปีถัดไป
8. นำผลสรุปเสนอต่อประธานกรรมการบริหาร
   8.1. ความพึงพอใจ เป็น KPI ในการวัดความพึงพอใจของแผนกในระดับใด
   8.2. เสนอ พร้อมขออนุมัติงบประมาณในการลงทุนต่อไป

ผู้อนุมัติ

ลงชื่อ กร อิร

(น.รกร ธรรมมาพาณิชย์)

ผู้รับผิดชอบ

วันที่ 25 มี.ค 65

ลงชื่อ ธนิศร ธนวงศ์เกษม

(ธนิศร ธนวงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 25 มี.ค. 65

ขั้นตอนการตรวจสอบความเรียบร้อยห้อง Server

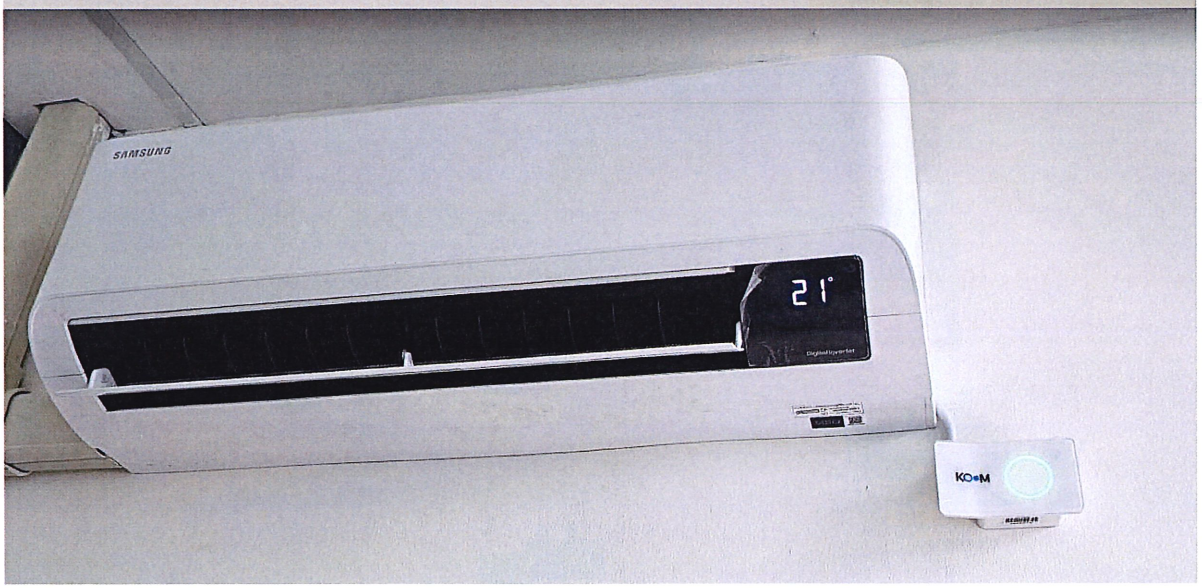
วัตถุประสงค์

1. เพื่อเป็นการรักษาความปลอดภัย และป้องกันเหตุที่ไม่คาดคิดภายในห้อง Server
2. เพื่อให้ Server และอุปกรณ์ต่างๆ ในห้อง Server ทำงานได้อย่างปกติ

ขั้นตอนการตรวจสอบอุปกรณ์ภายในห้อง Server

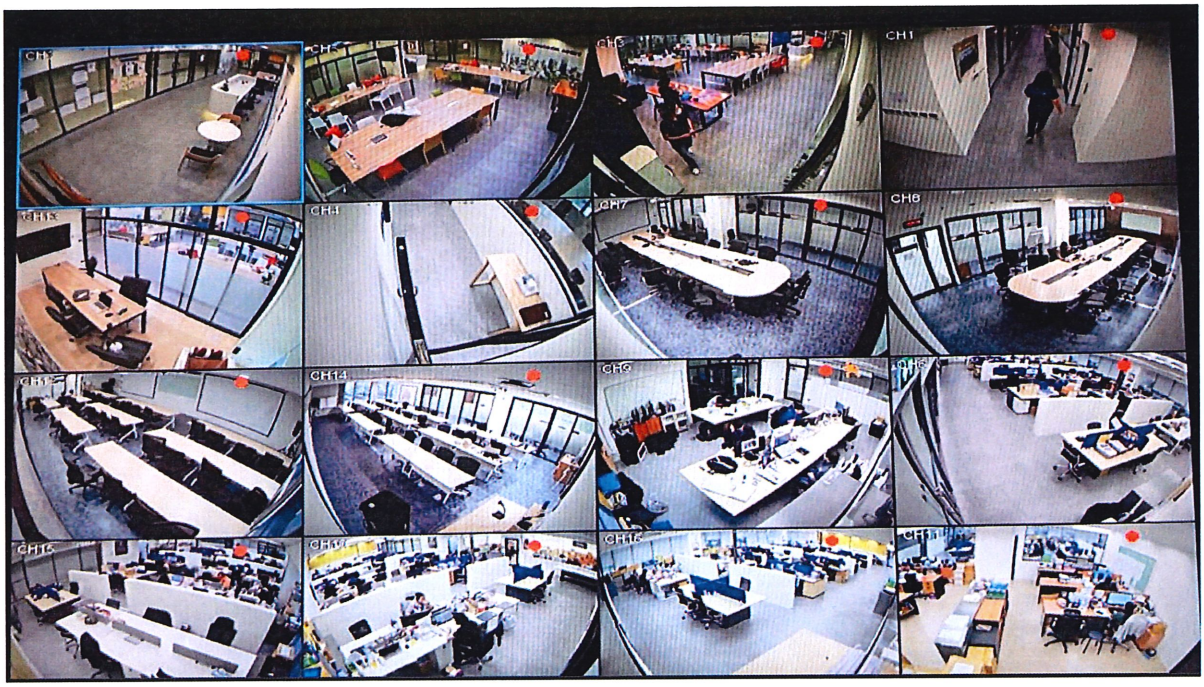
1. ตรวจสอบอุณหภูมิ และเครื่องปรับอากาศ
   1.1. อุณหภูมิภายในห้อง Server จะต้องมีอุณหภูมิอยู่ประมาณ 19-21 องศาเซลเซียส
   1.2. เครื่องปรับอากาศ 2 เครื่องทำงานปกติ และสลับการทำงานหรือไม่



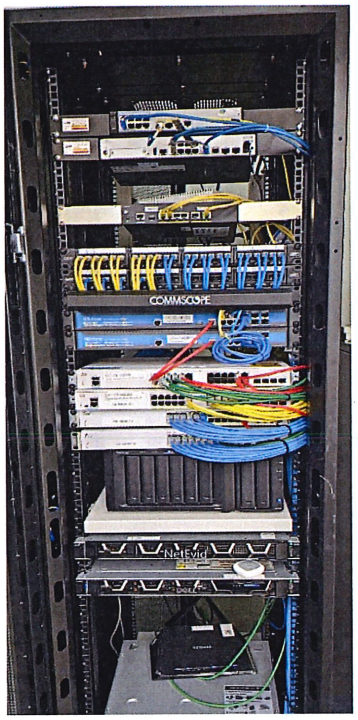


2. ตรวจสอบทำงานของกล้องวงจรปิด

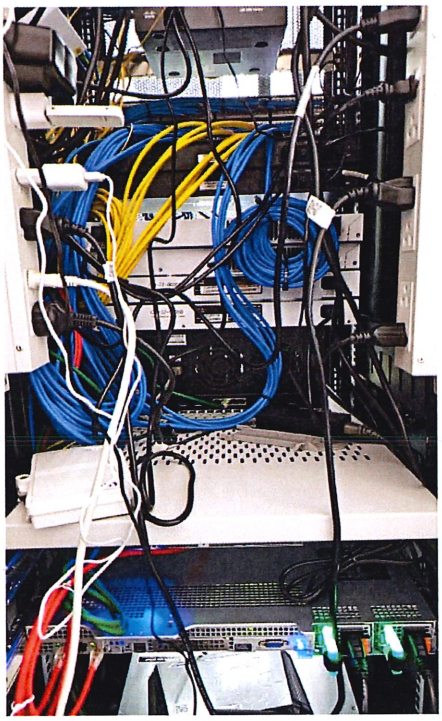
2.1. ตรวจสอบว่ากล้องวงจรปิดทั้ง 8 ตัวว่าสามารถใช้งานได้หรือไม่



3. ตรวจสอบสถานะไฟและสายไฟของอุปกรณ์ต่อพ่วงทั้งหมดในตู้ Rack (ทั้งด้านหน้าและด้านหลัง)



ตู้ด้านหน้า



ด้านหลัง

3.1. ตรวจสอบสถานะทุกระบบปกติหรือไม่

UP = ปกติ

Warning = แจ้งเตือนสิ่งผิดปกติแต่สามารถใช้งานได้

Down = ไม่สามารถใช้งานได้



3.1.1. ตรวจสอบน้ำหนักของถังดับเพลิง

3.1.1.1. โดยวิธีชั่งน้ำหนักของถังปกติ 13 กิโลกรัม ห้ามลดลงเกิน 1 กิโลกรัม



4. บันทึกผลการตรวจสอบพร้อมลงนามในเอกสารการตรวจห้อง Server หากมีเหตุการณ์ผิดปกติ ให้ลงบันทึกพร้อมทั้งรายงานไปยังผู้บริหาร IT แล้วดำเนินแก้ไขทันที
5. ส่งรายงานทั้งหมดให้ผู้บริหาร IT ตรวจสอบพร้อมลงนามทุกสิ้นเดือน

ประวัติการการปรับปรุงเอกสาร				
ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	19 เมษายน 256	วรวุฒิ เทพหัสดิน ณ อยุธยา
2	2.0	ปรับปรุงหลังย้ายสำนักงาน	15 มกราคม 2567	ชาญยุทธ วัฒนาศักดิกุล

ผู้อนุมัติ

ลงชื่อ_____

(นาย ชาญยุทธ วัฒนาศักดิกุล)

ผู้รับผิดชอบ

วันที่ 15/01/67

ลงชื่อ_____

(นางสาว ธนิศร ธนวงศ์เกษม)

ประธานเจ้าหน้าที่เทคโนโลยีสารสนเทศ

วันที่ 15/01/67.

ขั้นตอนการพัฒนาและฝึกอบรมพนักงาน

วัตถุประสงค์

1. เพื่อพัฒนาบุคลากรทั้ง IT และ พนักงานบริษัทให้มีความรู้สามารถทันยุคทันสมัยในเรื่องเทคโนโลยีสารสนเทศ
2. เพื่อให้บุคลากรมีการเรียนรู้ ตระหนักถึง และเพิ่มประสิทธิภาพการทำงานในเรื่องเทคโนโลยีสารสนเทศและนำมาใช้ให้เกิดประโยชน์ต่อองค์กร

ขั้นตอนการพัฒนาและฝึกอบรมพนักงานแบ่งเป็น 2 ส่วน

1. การฝึกอบรมให้กับพนักงาน IT จะต้องมีการฝึกอบรมที่เป็น IT ทั้งที่เป็น Online/e-Learning หรือ On site ให้ได้ปีละอย่างน้อย 40 ชั่วโมง
   1.1. การขออนุมัติเรียนหรือฝึกอบรมที่มีค่าใช้จ่ายให้เป็นไปตามระเบียบข้อบังคับของบริษัท
   1.2. การฝึกอบรมที่ไม่มีค่าใช้จ่าย สามารถขออนุมัติจากผู้บริหารฝ่าย IT ขึ้นไป
   1.3. เมื่อผ่านการฝึกอบรมเรียบร้อยแล้ว ให้กรอกรายละเอียดการฝึกอบรม จำนวนชั่วโมงที่ฝึกอบรม พร้อมหลักฐานที่ได้ฝึกอบรมอย่างใดอย่างหนึ่งไม่ว่าจะเป็น Certification หรือ รูปถ่าย หรือ ลายมือในการฝึกอบรมในตารางการฝึกอบรม
   1.4. ส่งตารางการฝึกอบรมที่กรอกเรียบร้อย ส่งให้ผู้บริหารฝ่าย IT ในวันสุดท้ายการทำงานของปีนั้นๆ
   1.5. ผลการฝึกอบรมถ้าต่ำกว่า 40ชั่วโมง ผู้บริหารฝ่าย IT สามารถนำมาใช้ในการพิจารณาการประเมินประสิทธิภาพการทำงานของเจ้าหน้าที่ได้ โดยเฉพาะในกรณีที่ไม่ถึงจำนวนที่กำหนด 2 ปีติดต่อกัน
   1.6. ข้อมูลที่ใช้กรอกในฟอร์มตารางบันทึกการฝึกอบรมประจำปี 40 ชั่วโมงตามตารางข้างล่าง

ตารางบันทึกการฝึกอบรมประจำปี 40 ชั่วโมง

ฝ่ายเทคโนโลยีสารสนเทศ

ประจำปี _____

ชื่อ _____ **นามสกุล** _____

ตำแหน่ง _____

วันที่	เรื่อง	จำนวนชั่วโมง	หมายเหตุ/หลักฐาน

ลงชื่อ _____ **ลงชื่อ** _____

( ) ( )

วันที่ _____ **วันที่** _____

ผู้ฝึกอบรม **ผู้จัดการ/ผู้อำนวยการฝ่าย**

2. การฝึกอบรมให้กับพนักงานหรือผู้ใช้งานคอมพิวเตอร์ จะมีการฝึกอบรม หรือให้ความรู้ดังต่อไปนี้
   2.1. พนักงานของทางบริษัท จะต้องได้รับการฝึกอบรม เรื่องการใช้ Application พื้นฐานของทางบริษัท ตั้งแต่วันแรกของการทำงาน
   2.2. พนักงานของทางบริษัท จะต้องได้รับการฝึกอบรมนโยบายเทคโนโลยีสารสนเทศ ปีละ 1 ครั้ง เพื่อเป็นการย้ำเตือน
   2.3. พนักงานของทางบริษัทฯ จะได้รับการฝึกอบรมเรื่องการใช้งาน plug in ใหม่ๆของระบบพื้นฐานที่ทางบริษัทใช้งาน
   2.4. ทุกครั้งที่มีการฝึกอบรมเรียบร้อยแล้ว จะให้พนักงานที่ได้รับการฝึกอบรมลงนามรับทราบการฝึกอบรมเป็นลายลักษณ์อักษร

2.4.1. สำหรับกรณีที่ฝึกอบรมทาง Online ผู้จัดฝึกอบรม จะเป็นผู้ Capture หน้าต่างการฝึกอบรม ที่มีการแสดงหน้าของผู้เข้ารับการฝึกอบรม เพื่อเป็นการยืนยันว่าได้รับการฝึกอบรมเรียบร้อยแล้ว

2.5. ตัวอย่างแผนการฝึกอบรมทั้งปีที่ได้วางแผนไว้ในแต่ล่ะปี

บริษัท บางกอก แอสเซท อินเตอร์ กรุ๊ป จำกัด

แผนการฝึกอบรมพนักงานของ BAIG

ลำดับ	หัวข้อ	วัตถุประสงค์	ระยะเวลาดำเนินงาน											
			ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.
1	การใช้งานApplicationพื้นฐานของBAIG	เพื่อให้พนักงานใหม่สามารถใช้งานApp	1 , 15	1 , 15	1 , 15	1 , 15	1 , 15	1 , 15	1 , 15	1 , 15	1 , 15	1 , 15	1 , 15	1 , 15
		พื้นฐานของทางBAIG ได้												
2	ความปลอดภัยสารสนเทศ							1						

ผู้อนุมัติ

ลงชื่อ กร อิร

(น.ส.กร ธรรมมาพาณิชย์)

ผู้รับผิดชอบ

วันที่ 10 เม.ย 65

ลงชื่อ ธนภร ธนวงศ์เกษม

(ธนิศร ธนวงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 10 เม.ย 65

BANGKOK ASSET INTERGROUP	คู่มือกระบวนการปฏิบัติงาน (Procedure Manual)	IT-Procedure-024	
	การบริหารจัดการ Log	ฉบับที่ : 1.0	แผ่นที่ : 1/1
	Log Management Procedure	เริ่มใช้ : 19 เม.ย 65	

1. วัตถุประสงค์

   1.1. เพื่อความมั่นคงปลอดภัยในทุกระบบที่มีความสำคัญต่อบริษัท

   1.2. เพื่อเป็นการป้องกันการโจมตี หรือ โจรกรรมข้อมูลจากผู้ไม่หวังดีต่อบริษัท

   1.3. เพื่อเป็นไปตามกฎหมาย และปฏิบัติตามพรบ.คอมพิวเตอร์ในการเก็บ Log

2. ขั้นตอนการบริหาร Log

   2.1. ผู้ดูแลทั้ง IT infrastructure/IT Development จะนำ Log ที่ได้ทำการเก็บไว้มาพิจารณาความผิดปกติหรือไม่ โดยที่ทาง IT Infrastructure จะตรวจสอบทุกวันทำการ ส่วนทางด้าน IT Development จะตรวจสอบทุก 15 วัน

   2.1.1. หากพบว่ามีความผิดปกติของข้อมูล

   2.1.1.1. ให้รายการผู้บริหารฝ่าย IT ทันที

   2.1.1.2. เรียกประชุมทีม IT อย่างเร่งด่วน เพื่อกำหนดแนวทางการแก้ไขและป้องกัน

   2.1.1.3. รายงานการแก้ไขและป้องกันให้กับผู้บริหารฝ่ายคอมพิวเตอร์เป็นระยะ ก่อนสรุปเป็นผลการแก้ไขและป้องกัน

   2.1.2. หากพบว่ามีความผิดปกติของข้อมูล แล้วยังไม่สามารถแก้ไขภายใน 24ชั่วโมง ให้รายงานประธานกรรมการบริหารเพื่อแก้ไขทันที

   2.1.3. หากพบว่าข้อมูลปกติ ก็ให้ลงนามปกติ

   2.2. นำเสนอต่อผู้บริหารฝ่ายคอมพิวเตอร์ ลงนามรับทราบทุกสิ้นเดือน

ผู้อนุมัติ

ลงชื่อ วรวุฒิ เทพทัสดิน

(วรวุฒิ เทพทัสดิน ณ อยุธยา)

ผู้รับผิดชอบ

วันที่ 10 เม.ย 65

ลงชื่อ ธนภร ธนวงศ์เกษม

(ธนภร ธนวงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 10 เม.ย 65

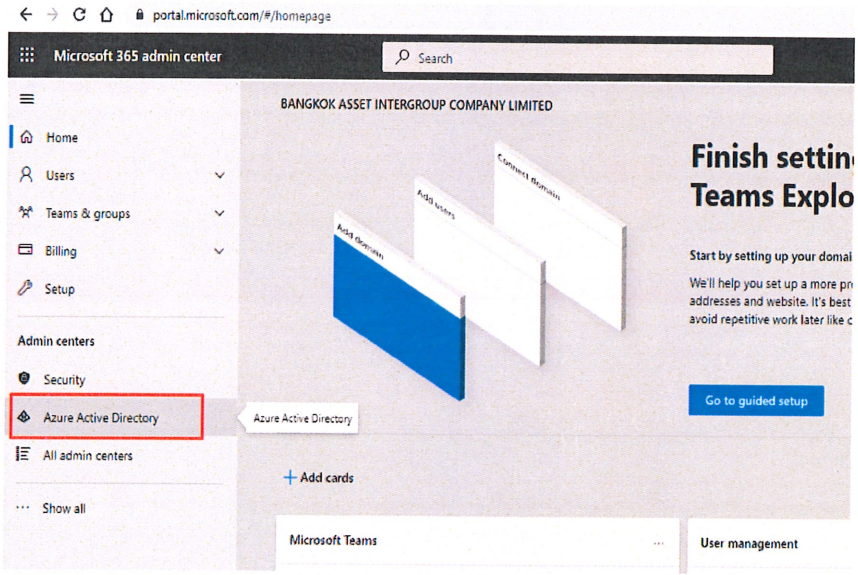
1. วัตถุประสงค์ เพื่อเป็นไปตามกฎหมาย และปฏิบัติตามพรบ.คอมพิวเตอร์ในการเก็บ Log
2. ขั้นตอนการเก็บ Log

2.1. คลิกที่ url : https://portal.microsoft.com/

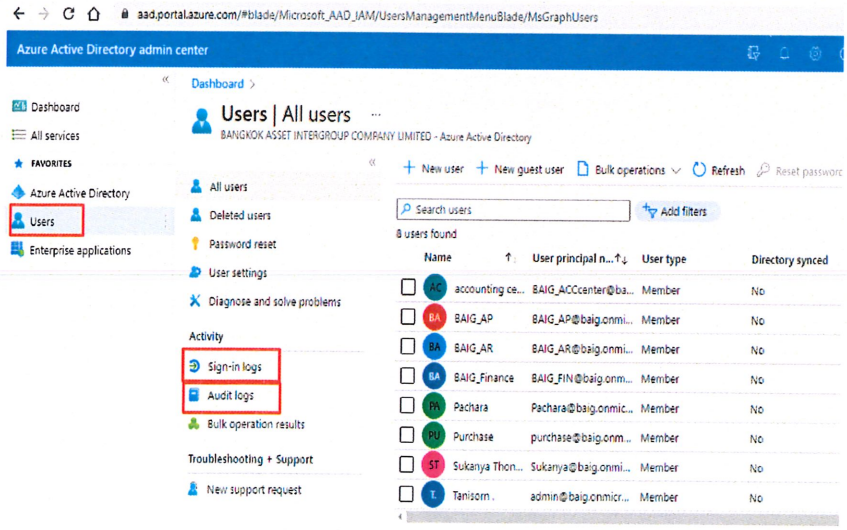
2.2. ใช้ user ของ admin

2.2.1. user : admin@baig.onmicrosoft.com

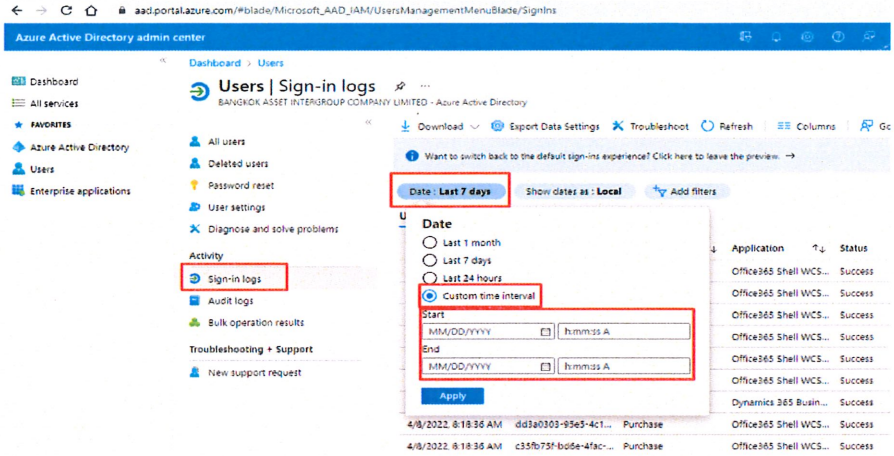
2.2.2. password: (อยู่ที่ admin)



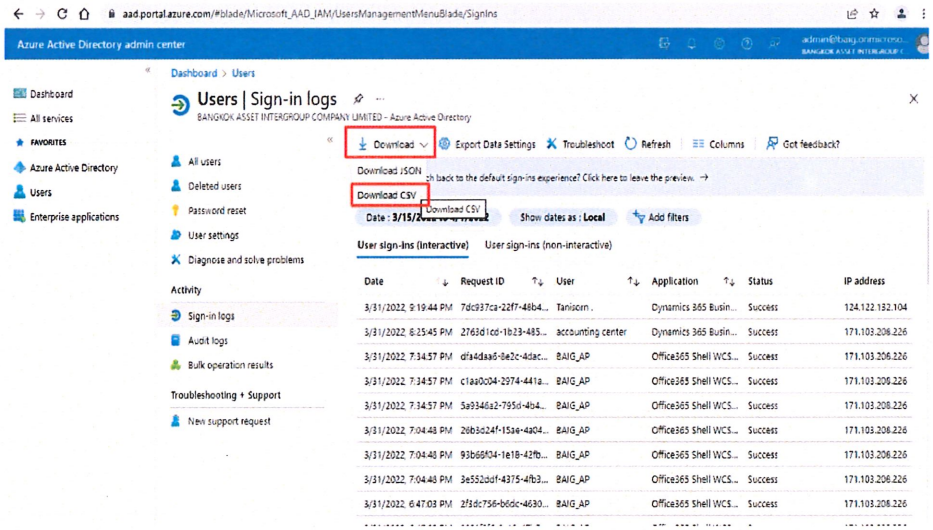
2.2.3. เก็บ log ของ Sign-in logs และ Audit logs



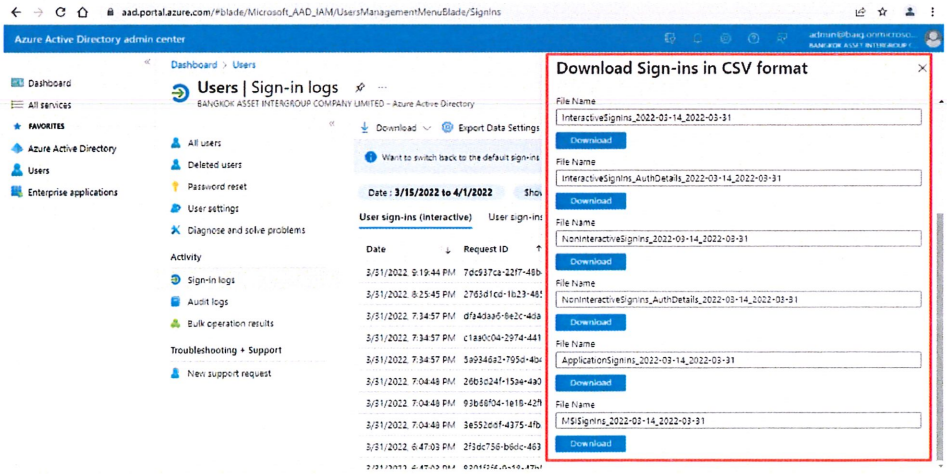
2.2.3.1. Sign-in logs เลือกช่วงวันที่ โดยสามารถทำได้ ทุกวันที่ 1 และ 16 หรือ เดือนล่ะ 2 ครั้ง



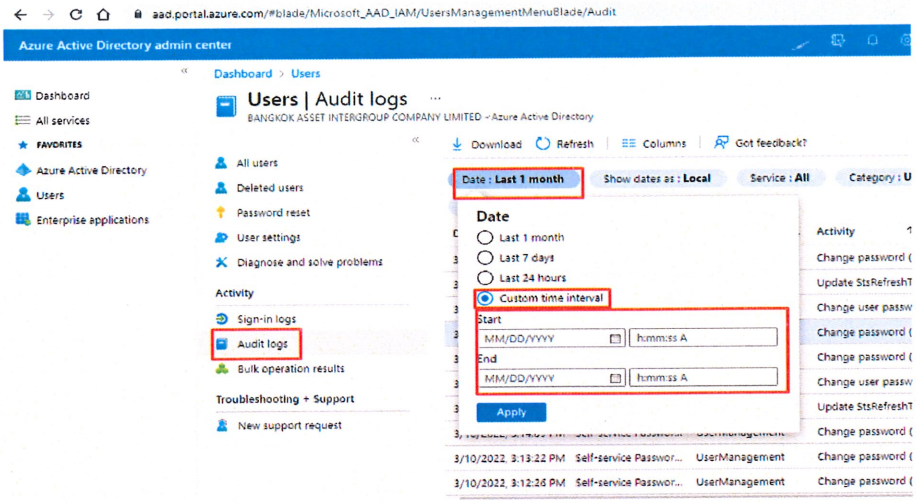
2.2.3.2. กด download เป็น CSV



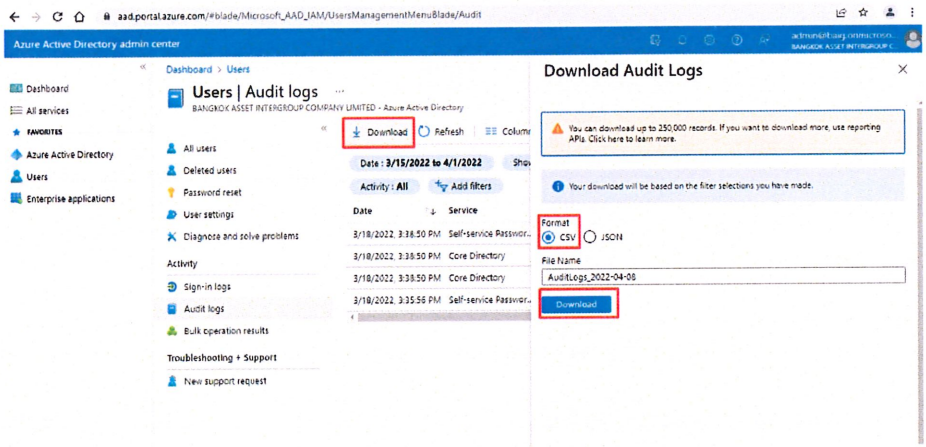
2.2.3.3.กด download ทั้ง 6 ไฟล์



2.2.3.4. Audit logs เลือกช่วงวันที่ โดยสามารถทำได้ ทุกวันที่ 1 และ 16 หรือ เดือนล่ะ 2 ครั้ง



2.2.3.5. กด download เลือก formatเป็น CSV จากนั้นกด download



ผู้อนุมัติ

ลงชื่อ ณัฐธิดา สิงห์ดง

(น.ส. ณัฐธิดา สิงห์ดง)

ผู้รับผิดชอบ

วันที่ 10 เม.ย 65

ลงชื่อ ธนพร ธนวงศ์เกษม

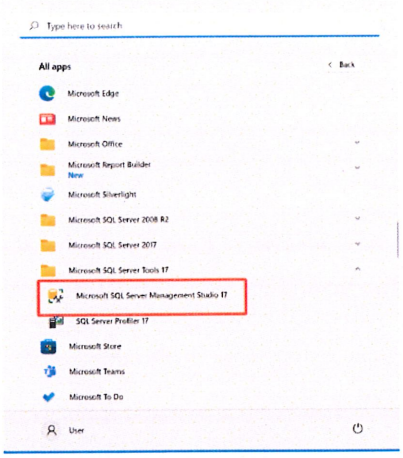
(ธนพร ธนวงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 10 เม.ย 65

1. วัตถุประสงค์ เพื่อเป็นไปตามกฎหมาย และปฏิบัติตามพรบ.คอมพิวเตอร์ในการเก็บ Log
2. ขั้นตอนการเก็บ Log

2.1. เปิดโปรแกรม SQL management

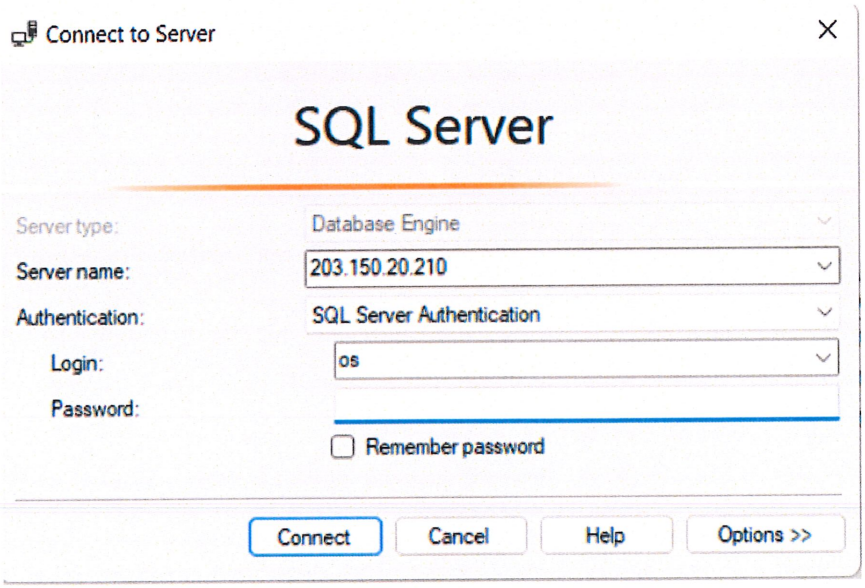


2.2. Connect Database OS

2.2.1.Server Name: 203.150.20.210

2.2.2.Login: OS

2.2.3.Password (อยู่ที่ Admin)



2.3. เมื่อ Connect Database แล้ว ให้โหลดข้อมูลตาม Query ต่อไปนี้

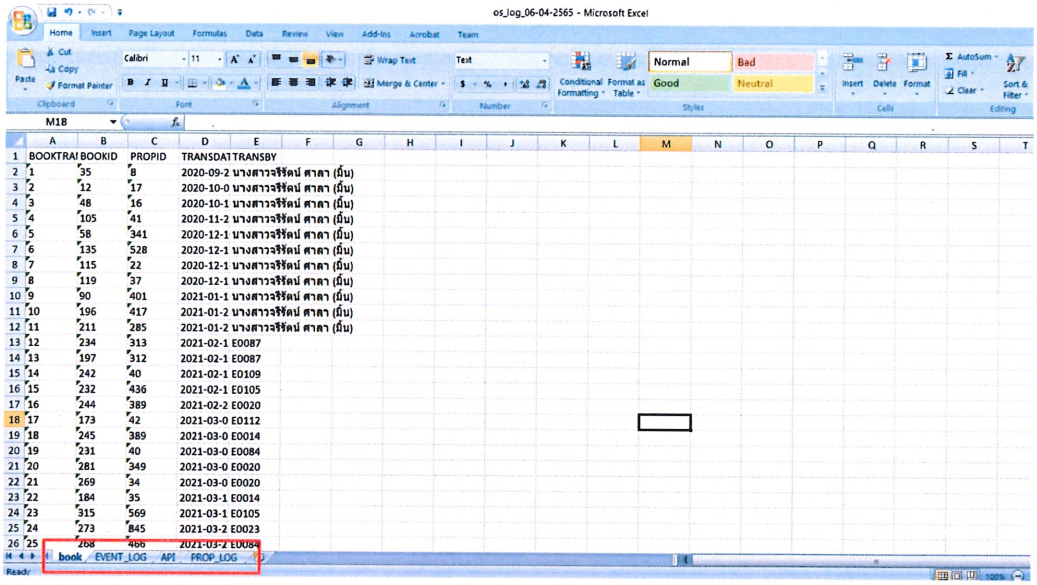
2.3.1.SELECT * FROM EVENT_LOG

2.3.2.SELECT * FROM BOOKTRANSLOG

2.3.3.SELECT * FROM PROP_LOG

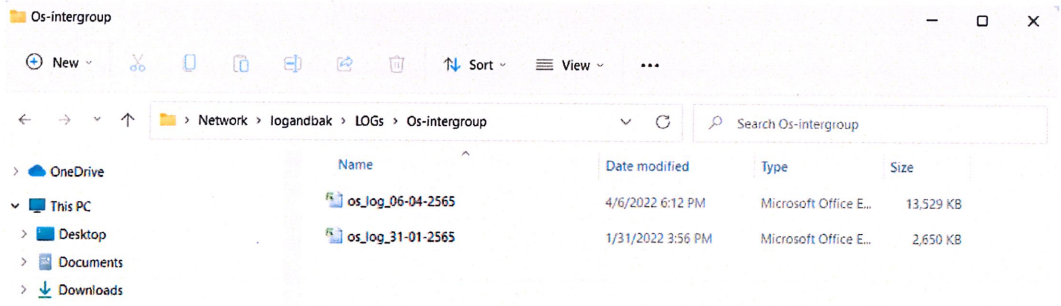
2.3.4.SELECT * FROM APITransectionData

2.4. ทำการ copy ข้อมูลใส่ใน excel แยก sheet



	BOOKTRAI	BOOKID	PROPID	TRANSDAT	TRANSBY
2	1	35	8	2020-09-2	นางสาวรัชดาพร ศาลา (มืน)
3	2	12	17	2020-10-0	นางสาวรัชดาพร ศาลา (มืน)
4	3	48	16	2020-10-1	นางสาวรัชดาพร ศาลา (มืน)
5	4	105	41	2020-11-2	นางสาวรัชดาพร ศาลา (มืน)
6	5	58	341	2020-12-1	นางสาวรัชดาพร ศาลา (มืน)
7	6	135	528	2020-12-1	นางสาวรัชดาพร ศาลา (มืน)
8	7	115	22	2020-12-1	นางสาวรัชดาพร ศาลา (มืน)
9	8	119	37	2020-12-1	นางสาวรัชดาพร ศาลา (มืน)
10	9	90	401	2021-01-1	นางสาวรัชดาพร ศาลา (มืน)
11	10	196	417	2021-01-2	นางสาวรัชดาพร ศาลา (มืน)
12	11	211	285	2021-01-2	นางสาวรัชดาพร ศาลา (มืน)
13	12	234	313	2021-02-1	E0087
14	13	197	312	2021-02-1	E0087
15	14	242	40	2021-02-1	E0109
16	15	232	436	2021-02-1	E0105
17	16	244	389	2021-02-2	E0020
18	17	173	42	2021-03-0	E0112
19	18	245	389	2021-03-0	E0014
20	19	231	40	2021-03-0	E0084
21	20	281	349	2021-03-0	E0020
22	21	269	34	2021-03-0	E0020
23	22	184	35	2021-03-1	E0014
24	23	315	569	2021-03-1	E0105
25	24	273	845	2021-03-2	E0023
26	25	268	466	2021-03-2	E0084

2.5. ทำการ copy ไฟล์ที่ได้ไปใส่ไว้ในเครื่อง LOGANDBAK



ลงชื่อ ณัฐธิดา สิงห์ดา

(น.ส. ณัฐธิดา สิงห์ดง)

ผู้รับผิดชอบ

วันที่ 10 เม.ย 65

ผู้อนุมัติ

ลงชื่อ ชนิสร ถนอมศักดิ์เกษม

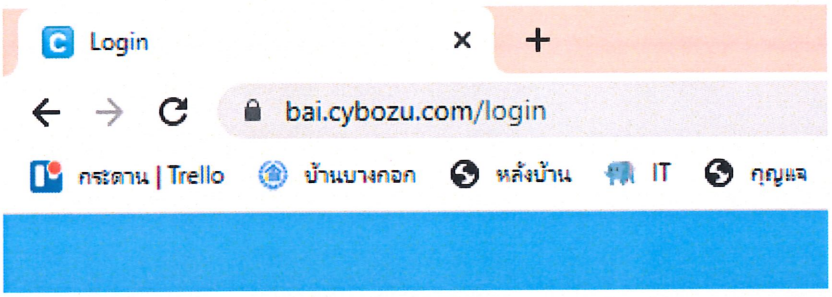
(ชนิสร ถนอมศักดิ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

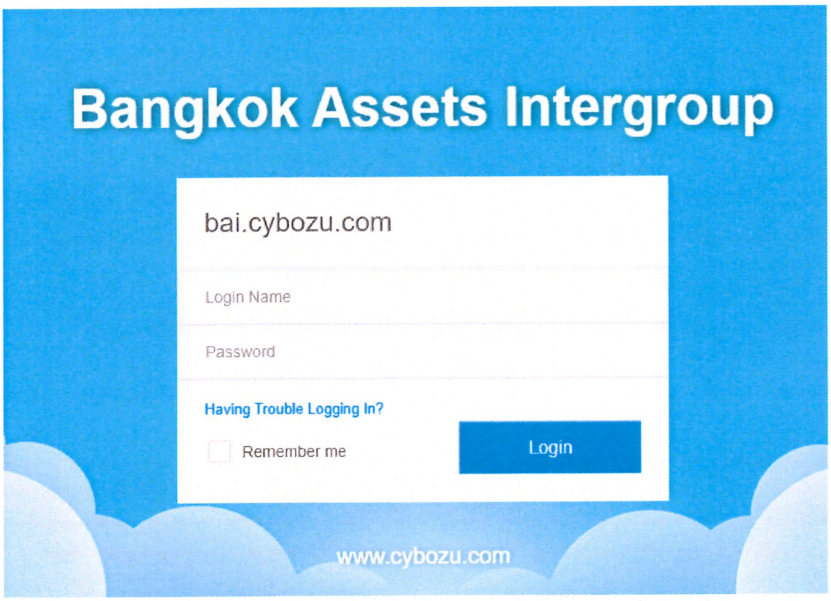
วันที่ 10 เม.ย 65

1. วัตถุประสงค์ เพื่อเป็นไปตามกฎหมาย และปฏิบัติตามพรบ.คอมพิวเตอร์ในการเก็บ Log
2. ขั้นตอนการเก็บ Log

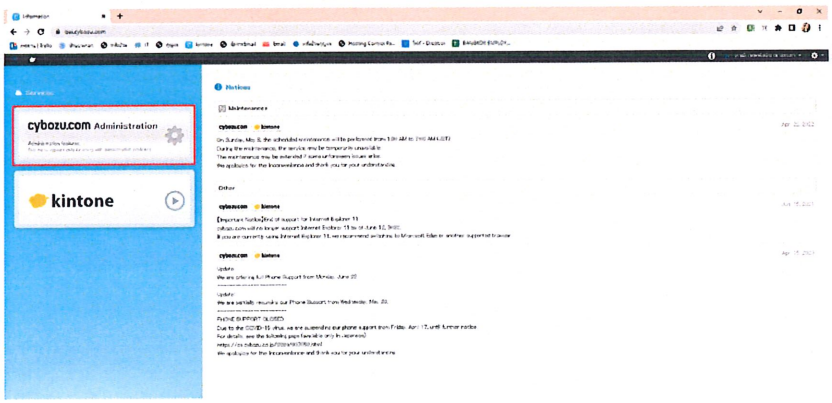
2.1. เข้าไปที่ https://bai.cybozu.com/



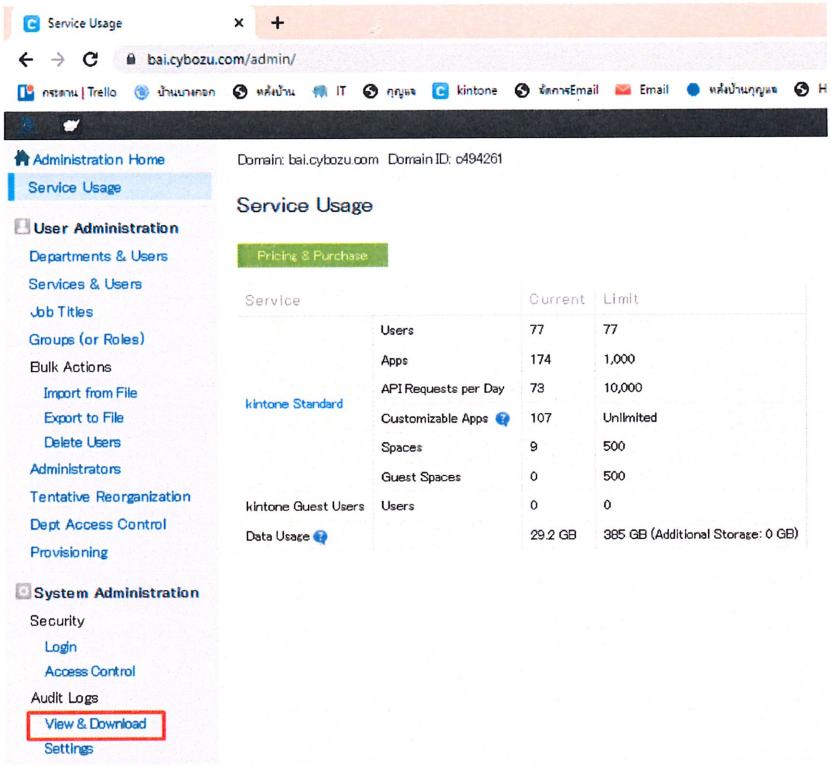
2.2. Login ด้วย USERNAME และ PASSWORD ของ Admin



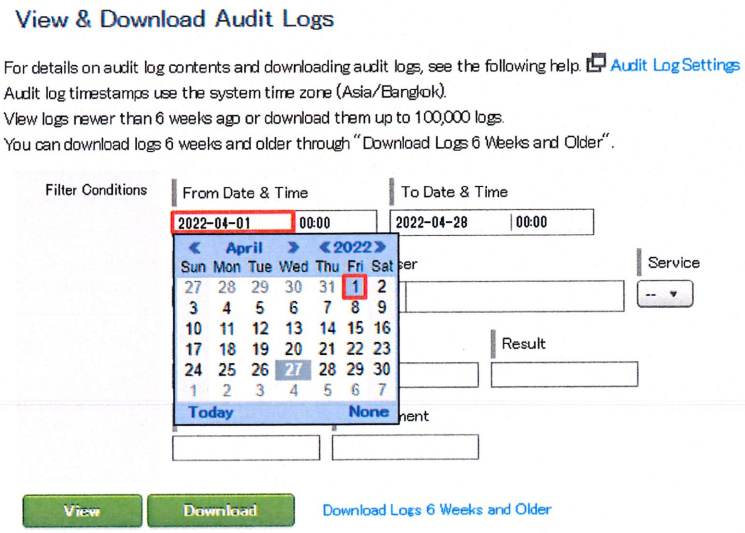
2.3. ไปที่เมนู cybozu.com Administration



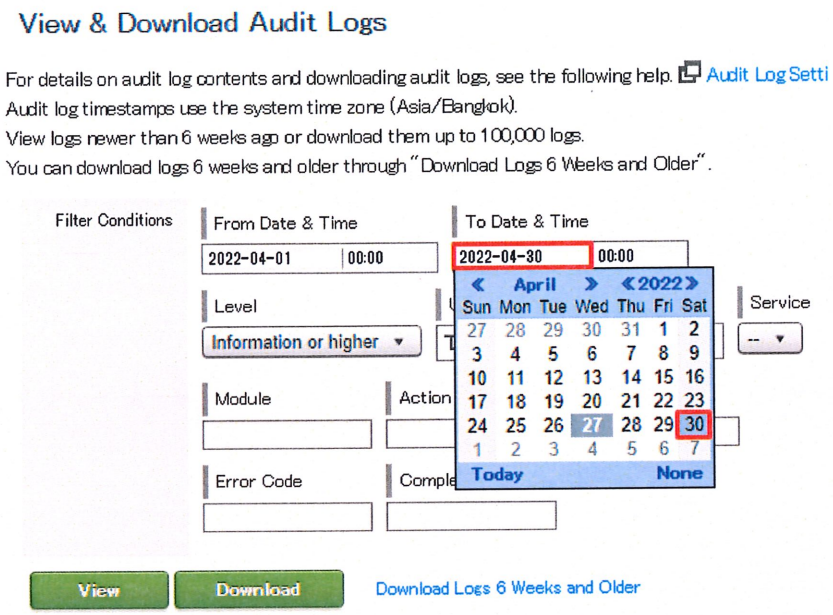
2.4. ไปที่เมนู View & Download



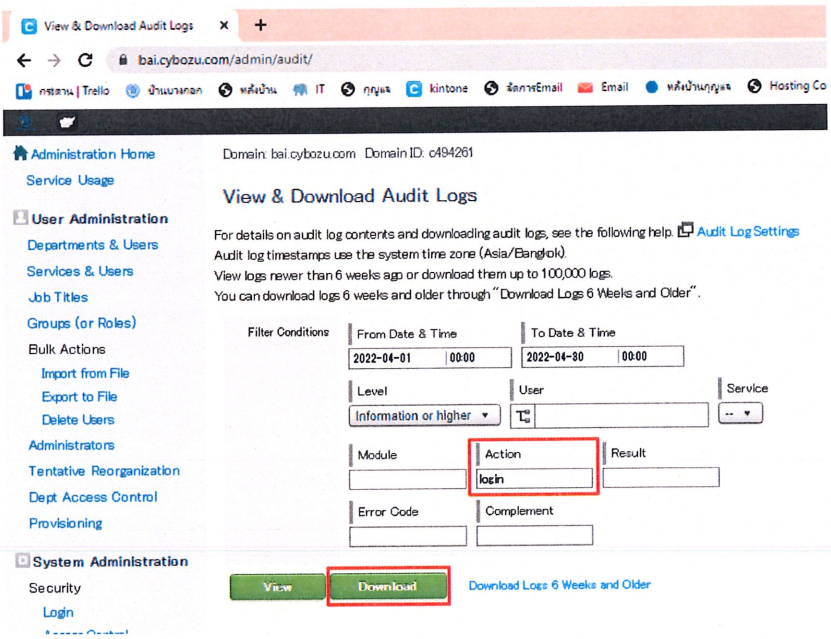
2.5. เลือกไปที่ From Date & Time กดปุ่มปฏิทิน เพื่อเลือกวัน เดือน ปี เริ่มต้น



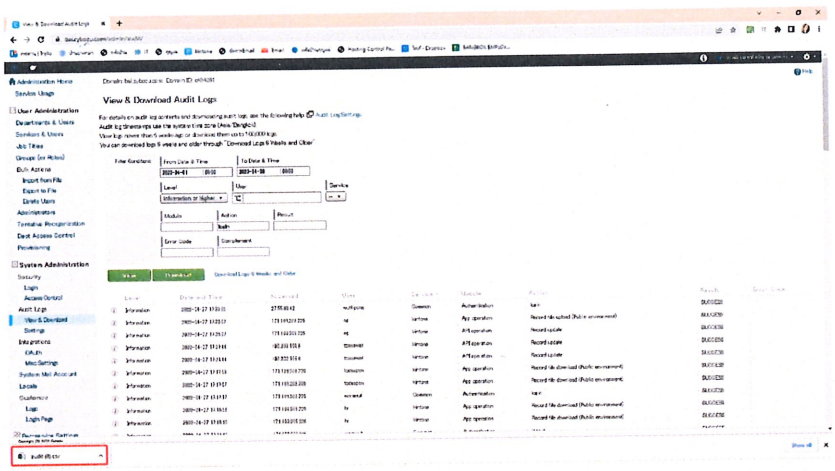
2.6. ไปที่ To Date & Time กดปุ่มปฏิทิน เพื่อเลือกวัน เดือน ปี สิ้นสุด



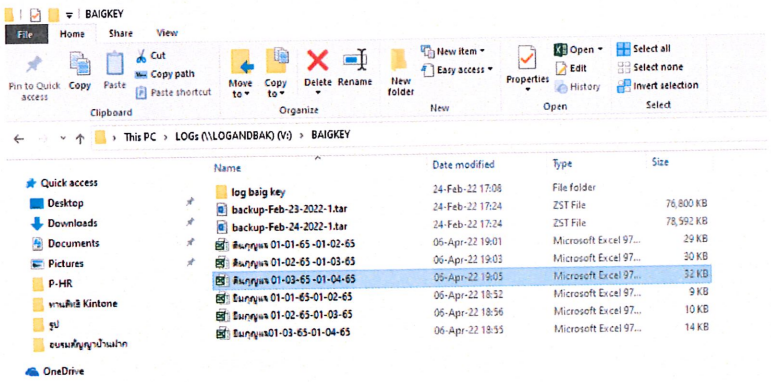
2.7. เลือกไปที่ Action พิมพ์คำว่า login จากนั้นกด Download



2.8. จะปรากฏไฟล์ที่ download อยู่ใน folder download



2.9. เมื่อระบบดาวน์โหลดไฟล์ EXCEL เสร็จเรียบร้อยแล้ว ให้ทำการ copy ไปไว้ที่เครื่อง LOGANDBAK



ลงชื่อ วรวุฒิ เทพทัลลิน)

(วรวุฒิ เทพทัลลิน)

ผู้รับผิดชอบ

วันที่ 10 เม.ย 65

ผู้อนุมัติ

ลงชื่อ ธนิศร ธนวงศ์เกษม

(ธนิศร ธนวงศ์เกษม)

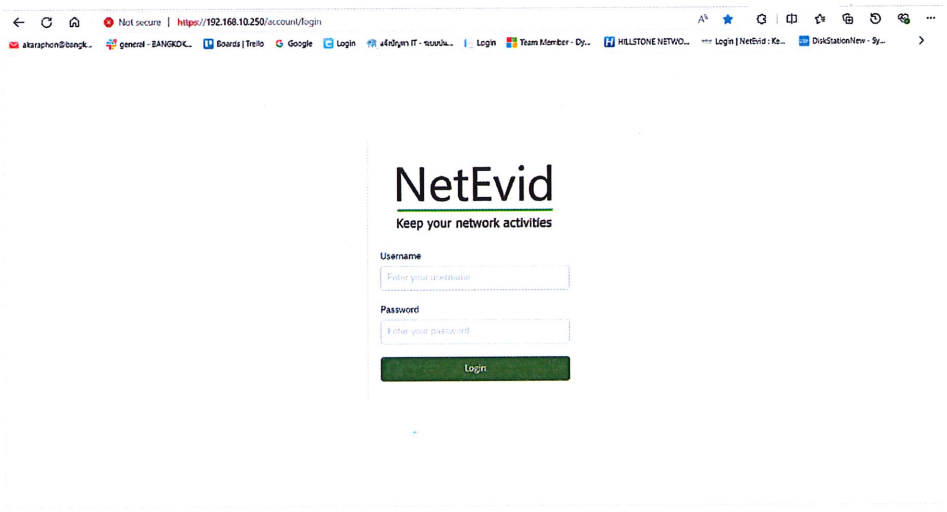
ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 10 เม.ย 65

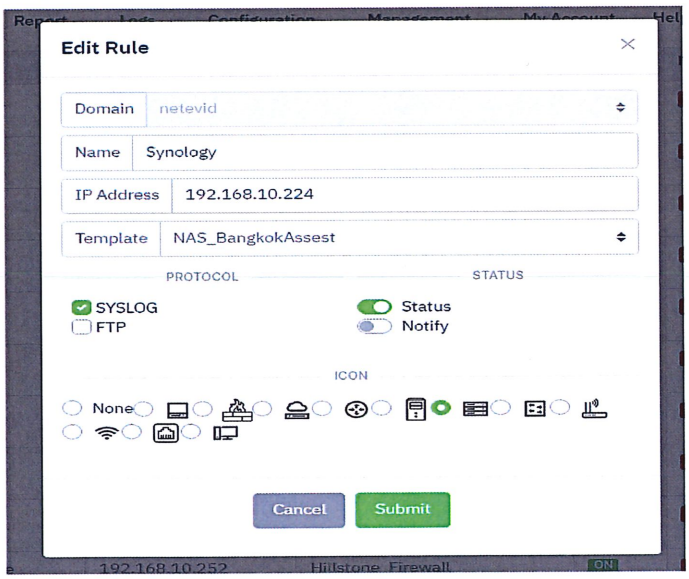
วัตถุประสงค์ เพื่อไปตามกฎหมาย และปฏิบัติตามพรบ. คอมพิวเตอร์ในการเก็บ Log

ขั้นตอนการเก็บ Log

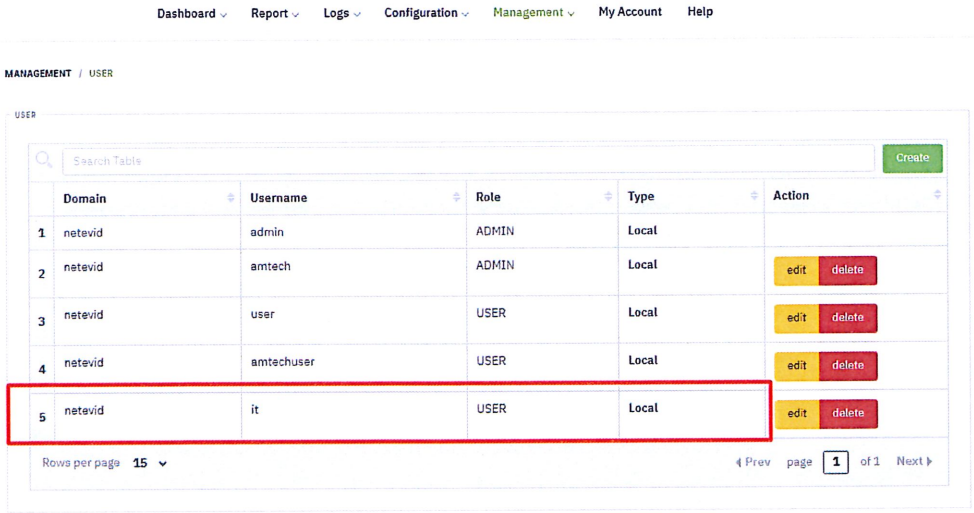
1. เข้าไปที่ Logs Server (192.168.10.250)



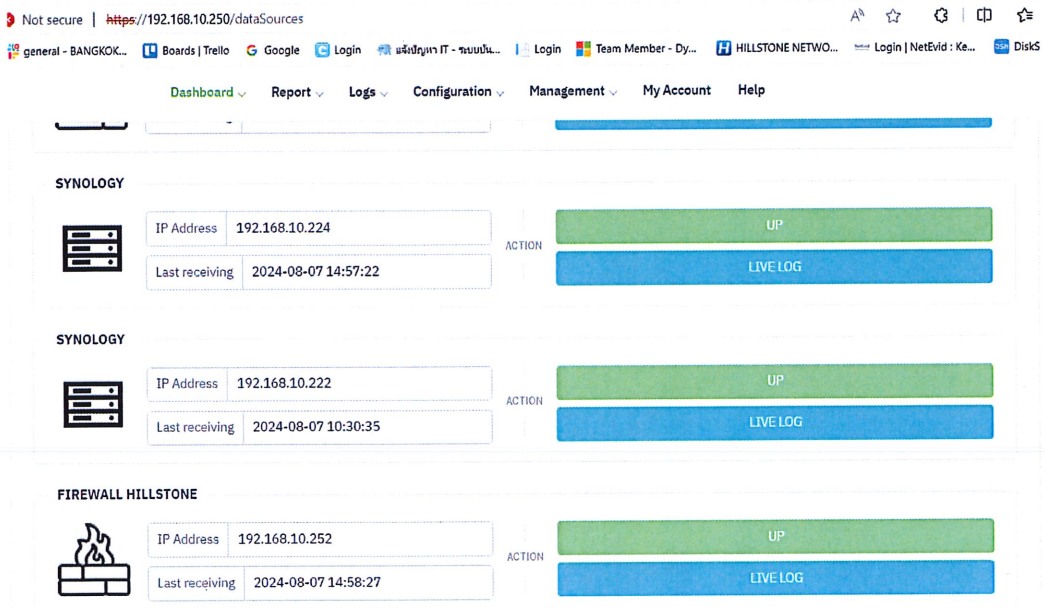
2. Login ด้วย User Administrator (จัดเก็บโดย IT Infrastructure)
3. ดูที่ Menu Logs (เลือก Logs Rules และตั้งค่า IP)



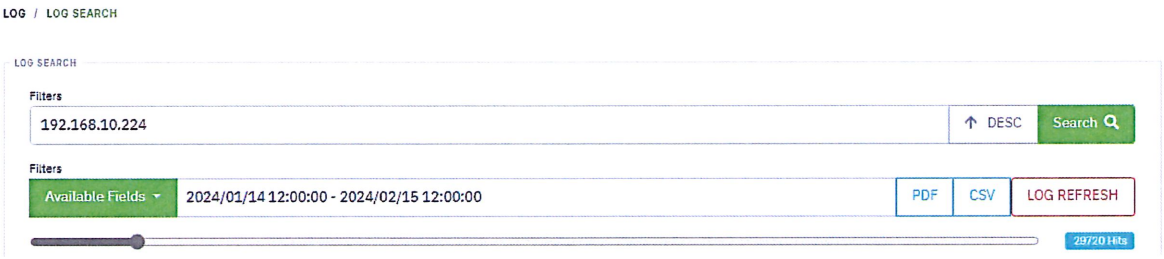
4. Login ด้วย User ที่เป็นสิทธิ์ User ทั่วไป (เนื่องจาก User Admin จะมีไว้ตั้งค่าเพียงอย่างเดียวไม่สามารถดูหรือเรียก Log Report ได้)



5. ไปที่ Menu Dashboard เลือก Data Sources Status และเลือก Synology และเข้าไปที่ LIVE



6. ไปที่ Menu Report และเลือก Search เราจะทำการ Filter โดยพิม 192.168.10.224 และ เลือกช่องเวลา (สามารถเก็บ Logs ไว้ได้ 180 วัน) จะเห็นว่าสามารถ Export ได้ 2 แบบคือ PDF และ CSV



ประวัติการปรับปรุงเอกสาร				
ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	19 เมษายน 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา
2	2.0	ปรับปรุงระบบการจัดเก็บ Log และให้เก็บได้ 180 วัน	1 กันยายน 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา
3	2.1	แก้ไขIP	15 กุมภาพันธ์ 2567	ชาญยุทธ วัฒนาศักดิกุล

ลงชื่อ_____

(นาย ชาญยุทธ วัฒนาศักดิกุล)

ผู้รับผิดชอบ

วันที่ 15/02/67

ผู้อนุมัติ

ลงชื่อ_____

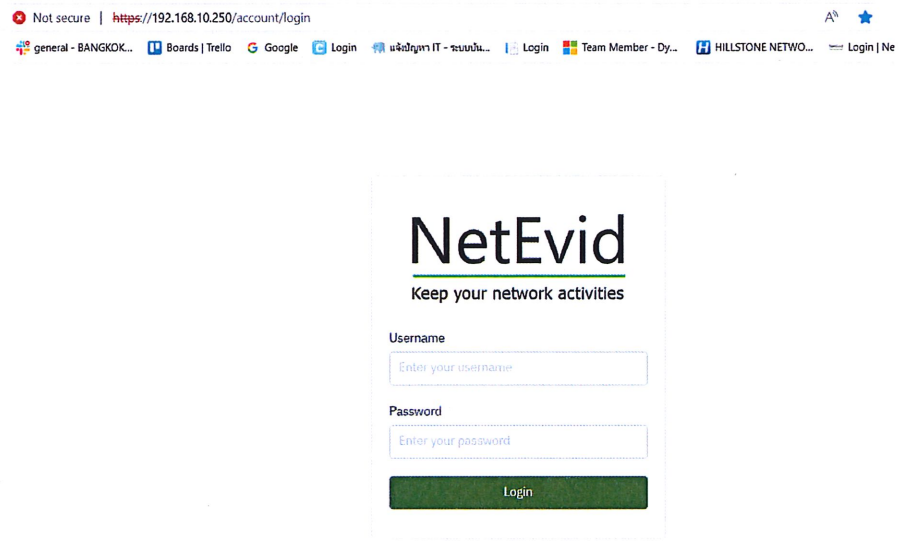
(นางสาว ธนิศร ธนวงศ์เกษม)

ประธานเจ้าหน้าที่เทคโนโลยีสารสนเทศ

วันที่ 15/02/67

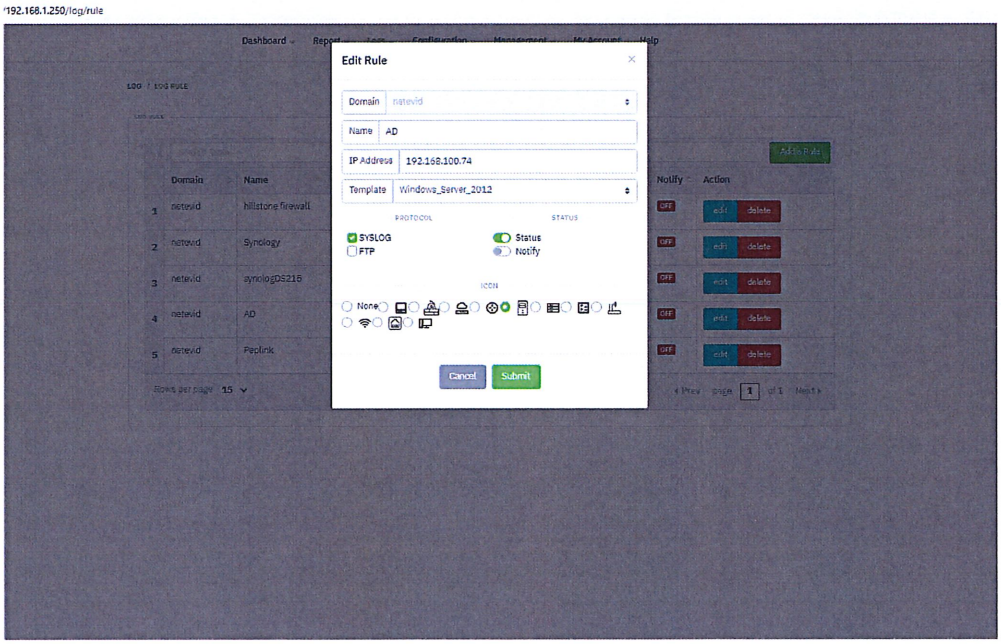
1. **วัตถุประสงค์** เพื่อเป็นไปตามกฎหมาย และปฏิบัติตามพรบ.คอมพิวเตอร์ในการเก็บ Log
2. **ขั้นตอนการเก็บ Log**

2.1. เข้าไปที่ Logs Server (192.168.10.250)

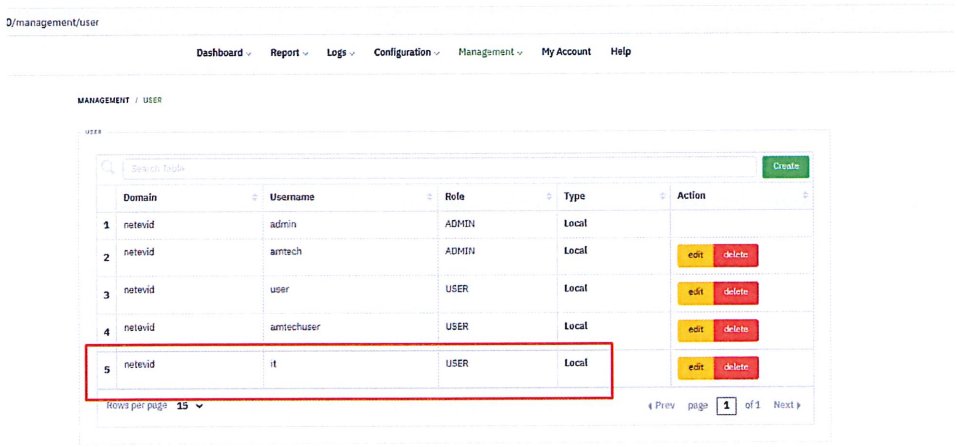


2.2. Login ด้วย User Administrator (จัดเก็บโดย IT Infrastructure)

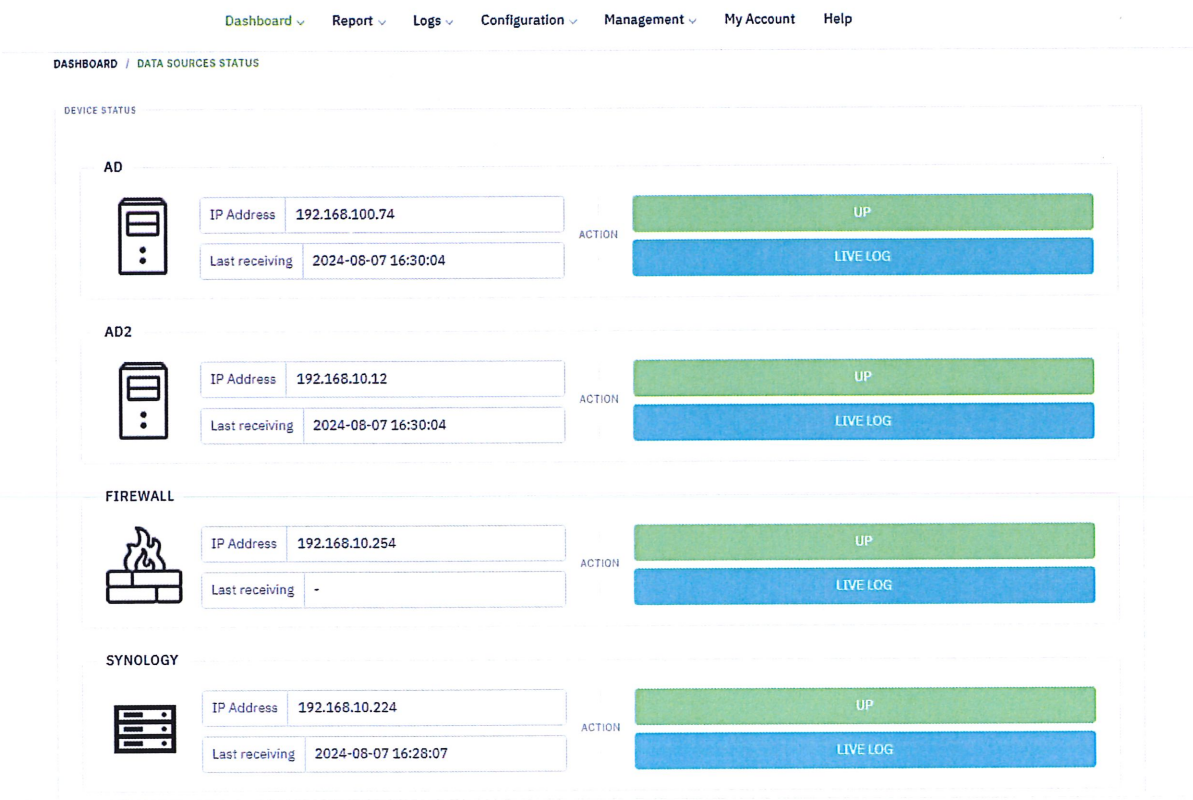
2.3. ดูที่ Menu Logs (เลือก Logs Rules และตั้งค่า IP)



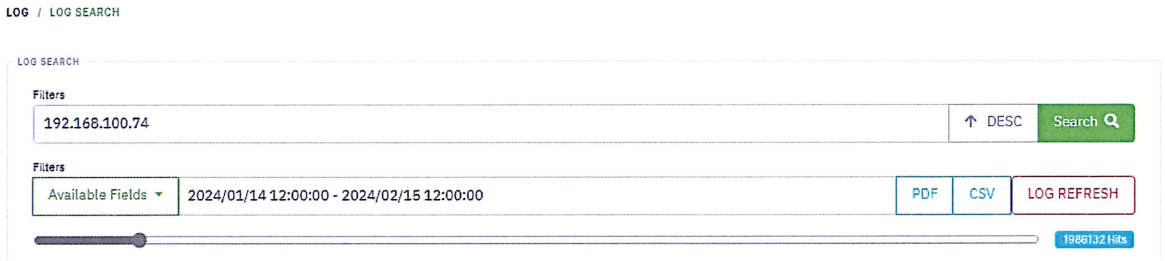
2.4. หลังจากนั้น Login ด้วย User ที่เป็นสิทธิ์ User ทั่วไป (เนื่องจาก User Admin จะมีไว้ตั้งค่าเพียงอย่างเดียวไม่สามารถดูหรือเรียก Logs Report ได้)



2.5. ไปที่ Menu Dashboard เลือก Data Sources Status และเลือก AD และเข้าไปที่ LIVE



2.6. ให้ไปที่ Menu Report และเลือก Search เราจะทำการ Filter โดยพิมพ์ 192.168.100.74 และเลือกช่วงเวลา (สามารถเก็บ Logs ไว้ได้ 180 วัน) จะเห็นว่าสามารถ Export ได้ 2 แบบคือ PDF และ CSV



ประวัติการการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	19 เมษายน 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา
2	2.0	ปรับปรุงระบบการจัดเก็บ Log และให้เก็บได้ 180วัน	1 กันยายน 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา
3	2.1	แก้ไขIP	15 กุมภาพันธ์ 2567	ชาญยุทธ วัฒนาศักดิกุล

ลงชื่อ_____

(นาย ชาญยุทธ วัฒนาศักดิกุล)

ผู้รับผิดชอบ

วันที่ 15/02/67

ผู้อนุมัติ

ลงชื่อ_____

(นางสาว ธนิศร ธนวงศ์เกษม)

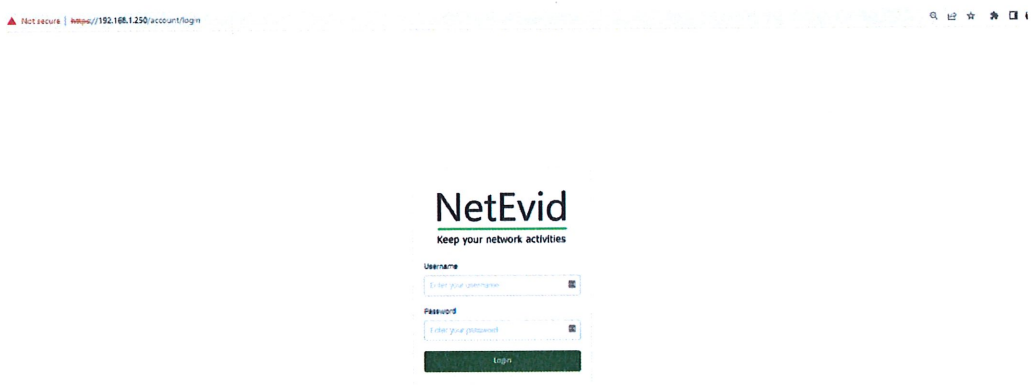
ประธานเจ้าหน้าที่เทคโนโลยีสารสนเทศ

วันที่ 15/02/67

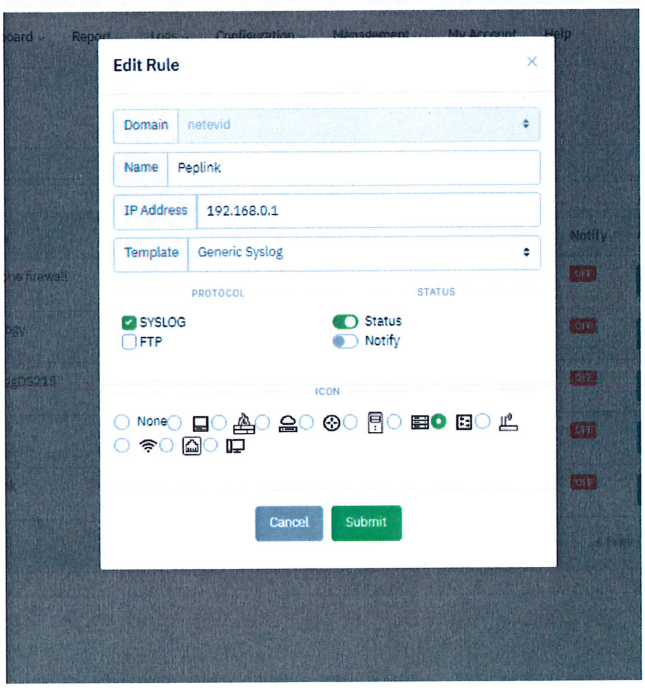
1. วัตถุประสงค์ เพื่อเป็นไปตามกฎหมาย และปฏิบัติตามพรบ.คอมพิวเตอร์ในการเก็บ Log
2. ขั้นตอนการเก็บ Log

   2.1. เข้าที่ Url: 192.168.1.250

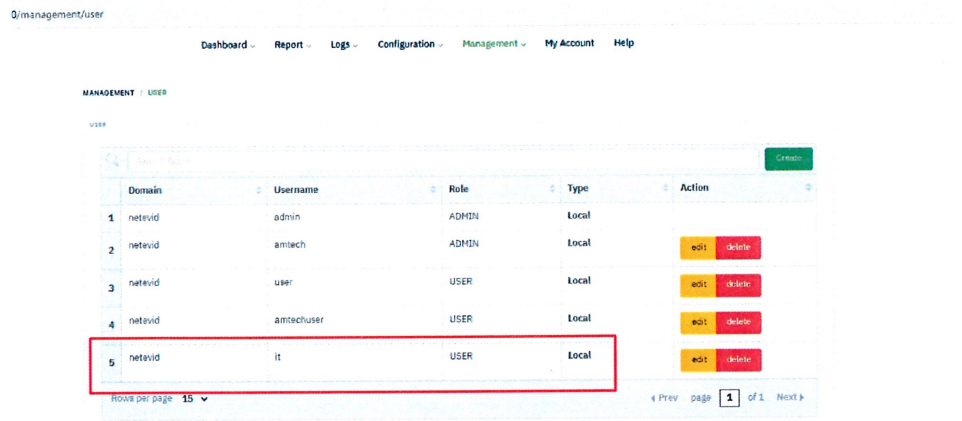
   2.2. Login ด้วย User Administrator (จัดเก็บโดย IT Infrastructure)



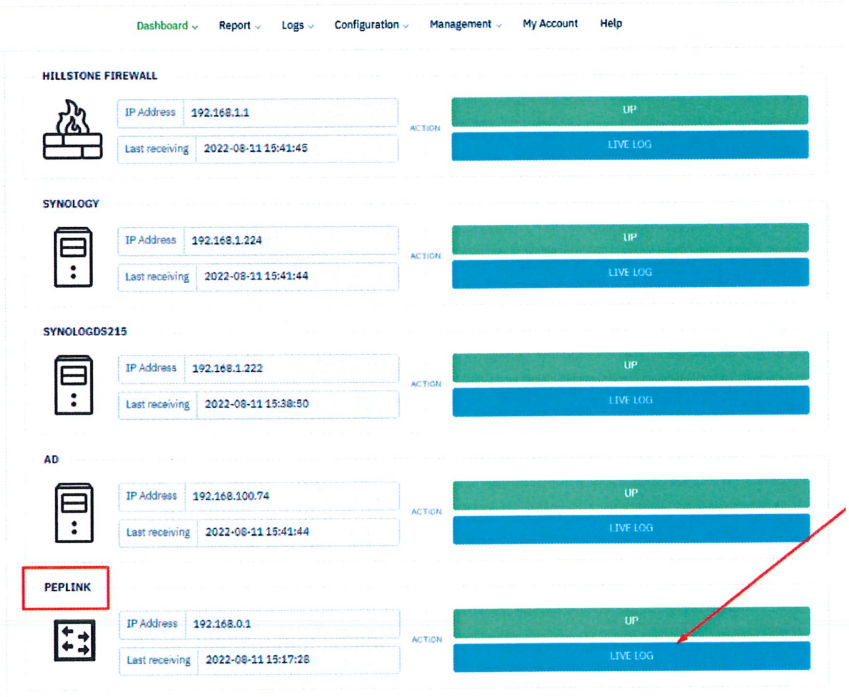
   2.3. ดูที่ Menu Logs (เลือก Logs Rules และตั้งค่า IP)



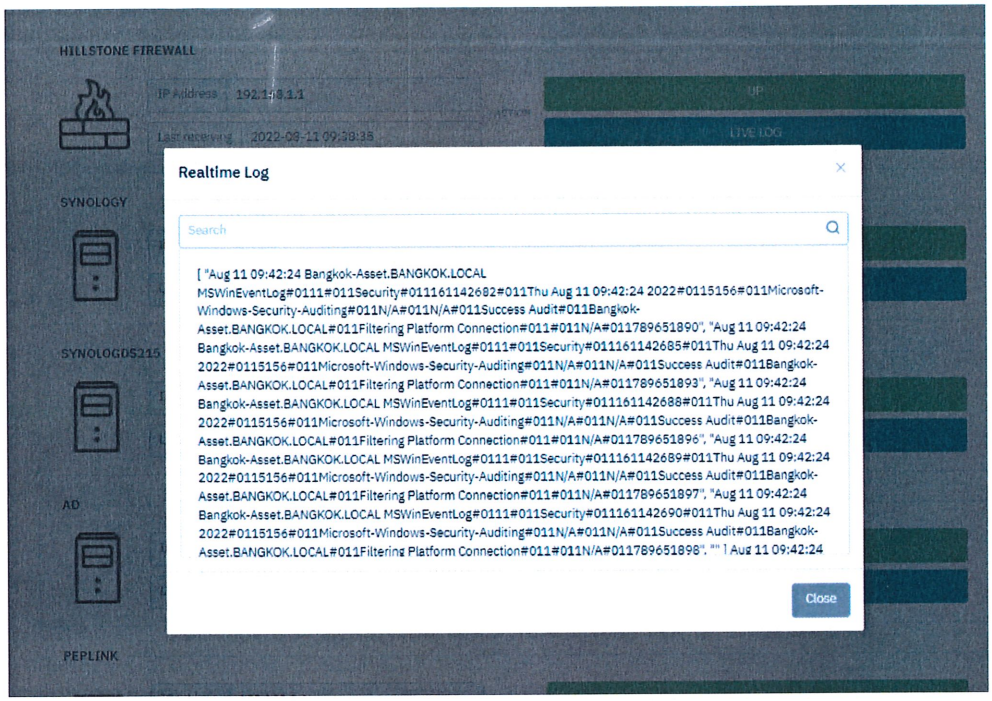
2.4. หลังจากนั้น Login ด้วย User ที่เป็นสิทธิ์ User ทั่วไป (เนื่องจาก User Admin จะมีไว้ตั้งค่าเพียงอย่างเดียวไม่สามารถดูหรือเรียก Logs Report ได้)



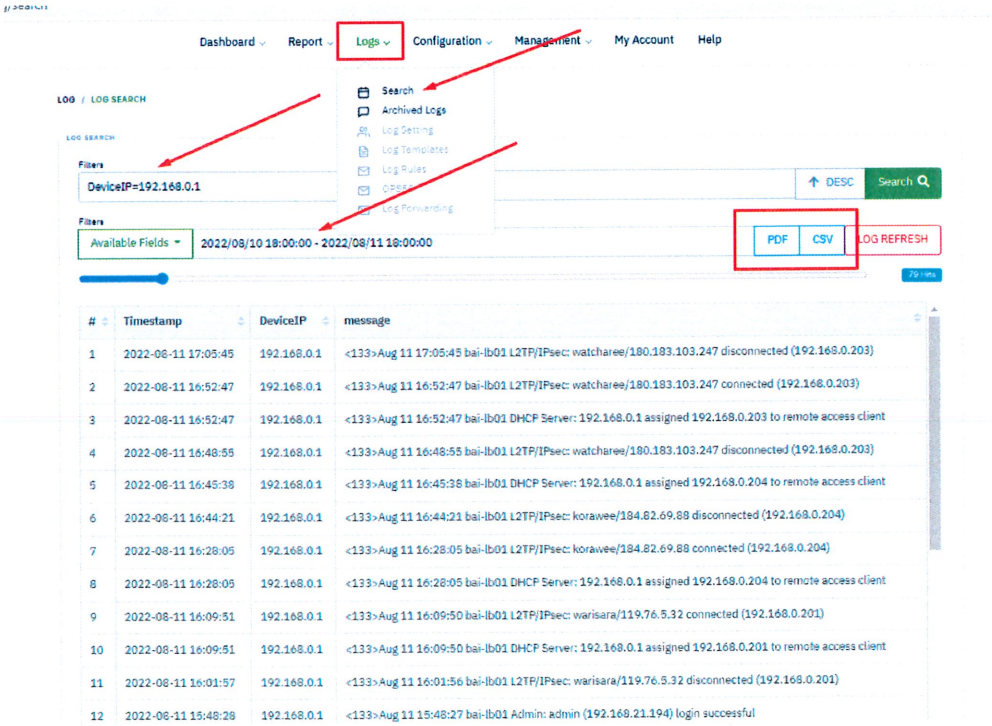
2.5. ไปที่ Menu Dashboard เลือก Data Sources Status และเลือก PEPLINK และเข้าไปที่ LIVE



2.6. จะเห็น Realtime Logs ที่เป็นแบบการเข้ารหัสไว้



2.7. ให้ไปที่ Menu Report และเลือก Search เราจะทำการ Filter โดยพิม DeviceIP=192.168.0.1 และเลือกช่วงเวลา (สามารถเก็บ Logs ไว้ได้ 180 วัน) จะเห็นว่าสามารถ Export ได้ 2 แบบคือ PDF และ CSV



2.7.1 จะได้รูปแบบการจัดเก็บ Logs ดังนี้

#	Timestamp	DeviceIP	message
1	2022-08-11 17:05:45	192.168.0.1	<133>Aug 11 17:05:45 bai-lb01 L2TP/IPsec: watcharee/180.183.103.247 disconnected (192.168.0.203)
2	2022-08-11 16:52:47	192.168.0.1	<133>Aug 11 16:52:47 bai-lb01 L2TP/IPsec: watcharee/180.183.103.247 connected (192.168.0.203)
3	2022-08-11 16:52:47	192.168.0.1	<133>Aug 11 16:52:47 bai-lb01 DHCP Server: 192.168.0.1 assigned 192.168.0.203 to remote access client
4	2022-08-11 16:48:55	192.168.0.1	<133>Aug 11 16:48:55 bai-lb01 L2TP/IPsec: watcharee/180.183.103.247 disconnected (192.168.0.203)
5	2022-08-11 16:45:38	192.168.0.1	<133>Aug 11 16:45:38 bai-lb01 DHCP Server: 192.168.0.1 assigned 192.168.0.204 to remote access client
6	2022-08-11 16:44:21	192.168.0.1	<133>Aug 11 16:44:21 bai-lb01 L2TP/IPsec: korawee/184.82.69.88 disconnected (192.168.0.204)
7	2022-08-11 16:28:05	192.168.0.1	<133>Aug 11 16:28:05 bai-lb01 L2TP/IPsec: korawee/184.82.69.88 connected (192.168.0.204)
8	2022-08-11 16:28:05	192.168.0.1	<133>Aug 11 16:28:05 bai-lb01 DHCP Server: 192.168.0.1 assigned 192.168.0.204 to remote access client
9	2022-08-11 16:09:51	192.168.0.1	<133>Aug 11 16:09:50 bai-lb01 L2TP/IPsec: warisara/119.76.5.32 connected (192.168.0.201)
10	2022-08-11 16:09:51	192.168.0.1	<133>Aug 11 16:09:50 bai-lb01 DHCP Server: 192.168.0.1 assigned 192.168.0.201 to remote access client
11	2022-08-11 16:01:57	192.168.0.1	<133>Aug 11 16:01:56 bai-lb01 L2TP/IPsec: warisara/119.76.5.32 disconnected (192.168.0.201)
12	2022-08-11 15:48:28	192.168.0.1	<133>Aug 11 15:48:27 bai-lb01 Admin: admin (192.168.21.194) login successful
13	2022-08-11 15:17:28	192.168.0.1	<133>Aug 11 15:17:27 bai-lb01 L2TP/IPsec: kiet/184.22.122.115 connected (192.168.0.202)

ประวัติการการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	19 เมษายน 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา
2	2.0	ปรับปรุงระบบการจัดเก็บ Log และให้เก็บได้ 180วัน	1 กันยายน 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา

ผู้อนุมัติ

ลงชื่อ วรวุฒิ เทพหัสดิน

(วรวุฒิ เทพหัสดิน ณ อยุธยา)

ผู้รับผิดชอบ

วันที่ 1 ก.ย. 2565

ลงชื่อ ธนิสร ธนวงศ์เกษม

(ธนิสร ธนวงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 1 ก.ย. 2565

BANGKOK ASSET INTERGROUP	คู่มือกระบวนการปฏิบัติงาน (Procedure Manual)	IT-Procedure-031	
	ขั้นตอนการจัดการ NDA	ฉบับที่ : 1.0	แผ่นที่ : 1/1
	Non-Disclosure Agreement Process Procedure	เริ่มใช้ : 3 พ.ค 65	

1. วัตถุประสงค์
   1.1. เพื่อเป็นมาตรฐานการรักษาความลับและความปลอดภัยของบริษัท
   1.2. เพื่อเป็นการสร้างความมั่นใจ และป้องกันการรั่วไหลของข้อมูลของบริษัท
   1.3. เพื่อเป็นไปตามกฎหมาย
2. ขั้นตอนการจัดการ
   2.1. ผู้จัดการแผนก IT ทำการรวบรวมรายชื่อผู้ให้บริการภายนอกที่เกี่ยวกับระบบสารสนเทศ
   2.2. ผู้จัดการแผนก IT จะดำเนินการทบทวนเอกสารสัญญารักษาความลับโดยพิจารณาวันที่หมดอายุของสัญญารักษาความลับ ในเดือนมกราคมของทุกปี
   2.3. หากมีสัญญาฉบับไหนที่จะหมดอายุภายในปีนั้นๆ ผู้จัดการแผนก IT จะดำเนินการส่งเอกสารสัญญารักษาความลับเพื่อส่งถึงผู้ให้บริการลงนามกลับมา ภายใน เดือน พฤษภาคมของทุกปี
   2.4. ในกรณีที่ผู้ให้บริการเป็นนิติบุคคล จะต้องแนบเอกสารหนังสือรับรองบริษัท และ สำเนาบัตรประชาชนกรรมการผู้มีอำนาจลงนาม พร้อมเซ็นสำเนาถูกต้อง
   2.5. เมื่อผู้จัดการแผนก IT ได้รับเอกสารสัญญารักษาความลับจากผู้ให้บริการเรียบร้อยแล้ว จะนำเอกสารสัญญารักษาความลับเสนอให้ผู้มีอำนาจลงนามของบริษัท ลงนามในสัญญารักษาความลับเสร็จเรียบร้อยแล้ว
   2.6. ผู้จัดการแผนก IT จะนำเอกสารสัญญารักษาความลับไปสแกน และจัดเก็บเอกสารในรูปแบบของอิเล็กทรอนิกส์เอาไว้ใน storage folder ชื่อว่าIT\สัญญารักษาความลับ
   2.7. แล้วนำเอกสารสัญญารักษาความลับที่มีรูปแบบกระดาษ ใส่ซองและเก็บรักษาไว้ในห้องทำงานของแผนกสารสนเทศต่อไป

	ผู้อนุมัติ
ลงชื่อ ณัฐชิดา สิงห์คง	ลงชื่อ ธนิศร ธนมศักดิ์เกษม
(น.ส. ณัฐชิดา สิงห์คง)	(ธนิศร ธนมศักดิ์เกษม)
ผู้รับผิดชอบ	ผู้บริหารฝ่ายคอมพิวเตอร์
วันที่ 27 เม.ย 65	วันที่ 27 เม.ย 65

ขั้นตอนการจัดการความเสี่ยงเทคโนโลยีสารสนเทศ

วัตถุประสงค์ เพื่อสร้างแนวทางปฏิบัติเกี่ยวกับการบริหารและการจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

1. แนวทางการกำหนดเหตุการณ์ความเสี่ยง (Risk Factor) ที่จะเกิดขึ้นกับฝ่ายเทคโนโลยีสารสนเทศเป็นหมวดหมู่ดังนี้

ความเสี่ยงแต่ละด้าน	ประเภทของเหตุการณ์	ปัจจัยความเสี่ยง
ด้านบุคลากร (Personnel)	ความรู้ความสามารถทางด้านเทคโนโลยีสารสนเทศ	● เทคโนโลยีสารสนเทศมีการพัฒนาและเปลี่ยนแปลงที่รวดเร็ว ● บุคลากรทางเทคโนโลยีสารสนเทศหาได้ค่อยข้างยาก
ด้านระบบปฏิบัติการด้านสารสนเทศ (Information Technology)	การโจรกรรม และทำลายสาธารณูปโภคด้านเทคโนโลยีสารสนเทศ	● ไวรัสคอมพิวเตอร์/Malware ● การบุกรุกโจมตีระบบ (Hacking) หรือการคุกคามทางไซเบอร์ ● Phishing Attack ข้อมูลรั่วไหลจากการหลอกลวงข้อมูล ● ศูนย์คอมพิวเตอร์ถูกทำลาย
	ระบบงานสารสนเทศ	● ปัญหาระบบไม่สามารถทำงานได้ตามที่ต้อง ● ปัญหาระบบที่มากเกินไปและทับซ้อนกัน ● ปัญหาการใช้โปรแกรมเก่าที่ไม่ได้การสนับสนุนจากผู้ผลิตแล้ว ● ปัญหาที่เกิดจากระบบใหม่ๆ ยังไม่เสถียร ● ปัญหาที่เกิดจากระบบมีความล้าสมัย ● ปัญหาการเข้าถึงข้อมูล
ด้านสิ่งที่เกิดขึ้นไม่คาดคิด (Environment)	ภัยธรรมชาติ	● น้ำท่วม ● พายุ ● แผ่นดินไหว

	อัคคีภัย	• ความร้อน • ไฟฟ้าลัดวงจร
	เหตุการณ์ทำให้หยุดชะงัก	• การประท้วงต่างๆ • การเมือง • สงคราม
ด้านการบริหาร (Management)	การลงทุน หรือการพัฒนาทางด้านเทคโนโลยีสารสนเทศ	• กลยุทธ์ขึ้นอยู่กับระดับความสำคัญทางธุรกิจ • งบประมาณทางด้านเทคโนโลยีที่สูง
	การบริหารจัดการระบบโครงการด้านเทคโนโลยีสารสนเทศ	• การบริหารโครงการไม่สำเร็จ ล่าช้า หรือหยุดชะงัก • โครงการใช้ทรัพยากรไม่เหมาะสม เช่น ต้นทุนมากเกินไป หรือ ใช้บุคลากรก่อนมากเกินไป
	การบริหารจัดการผู้ให้บริการภายนอก	• มีโอกาสที่เกิดข้อมูลรั่ว • โอกาสในการเปลี่ยนผู้ให้บริการภายนอกได้น้อย

2. การประเมินความเสี่ยง (Risk Assessment) หมายถึงกระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และการจัดลำดับความเสี่ยง เป็น 5 ระดับ ดังนี้

ระดับของโอกาสเกิด	โอกาสที่จะเกิด	ความถี่ที่เกิดขึ้น (เฉลี่ย)	เปอร์เซ็นต์ โอกาสที่เกิดขึ้น
1	น้อยมาก	ในระยะเวลามากกว่า 1 ปี เกิด 1 ครั้ง	น้อยกว่า 10%
2	น้อย	ในระยะเวลามากกว่า 6-12 เดือน เกิด 1 ครั้ง	10-25%
3	ขึ้นปานกลาง	ในระยะเวลามากกว่า 3-6 เดือน เกิด 1 ครั้ง	26-50%
4	สูง	ในระยะเวลามากกว่า 1-3 เดือน เกิด 1 ครั้ง	51-75%
5	สูงมาก	ในระยะเวลา 1 เดือน เกิด 1 ครั้งหรือมากกว่า	มากกว่า 75%

3. ความรุนแรงของผลกระทบของความเสี่ยง (Impact) หมายถึง ความรุนแรงของเหตุการณ์ความเสี่ยงที่หากเกิดขึ้นแล้วจะส่งผลกระทบในด้านต่างๆ ซึ่งผลกระทบนั้นพิจารณาได้ทั้ง ด้านการเงิน ผลกระทบด้านการดำเนินงาน และผลกระทบเชิงคุณภาพ ผลกระทบด้านความปลอดภัยในชีวิตและทรัพย์สินของบุคลากร และประสิทธิผลของการทำงาน ซึ่งสามารถแบ่งเป็น 5 ระดับ โดยกำหนดนิยามในแต่ละระดับดังนี้

ระดับความรุนแรงของผลกระทบของเสี่ยง		
ระดับ	ผลกระทบ	ความสูญเสีย
1	น้อยมาก	ระบบคอมพิวเตอร์ ที่รองรับธุรกรรมสำคัญหรือกระบวนงานหลัก หยุดชะงักไม่เกิน 4 ชั่วโมง หรือไม่ส่งผลต่อการให้บริการใด ๆ หยุดชะงัก
2	น้อย	ระบบคอมพิวเตอร์ ที่รองรับธุรกรรมสำคัญหรือกระบวนงานหลัก หยุดชะงักมากกว่า 4-24 ชั่วโมง
3	ปานกลาง	ระบบคอมพิวเตอร์ ที่รองรับธุรกรรมสำคัญหรือกระบวนงานหลัก หยุดชะงักมากกว่า 1-3 วัน
4	สูง	ระบบคอมพิวเตอร์ที่รองรับธุรกรรมสำคัญหรือกระบวนงานหลัก หยุดชะงักมากกว่า 3-7 วัน
5	สูงมาก	ระบบคอมพิวเตอร์ที่รองรับธุรกรรมสำคัญหรือกระบวนงานหลัก หยุดชะงักมากกว่า 7 วัน

4. จัดลำดับความเสี่ยง (Prioritizes Risk) เป็นการเลือกมาตรการตอบสนองความเสี่ยงที่เหมาะสมกับแต่ละความเสี่ยงและสภาวะแวดล้อม โดยพิจารณาความเสี่ยงภายใต้มิติของโอกาสเกิดและผลกระทบ ซึ่งการประเมินผลกระทบควรพิจารณาผลกระทบในทุกด้าน แล้วเลือกผลกระทบที่สอดคล้องกับวัตถุประสงค์ขององค์กร เพื่อจัดลำดับความสำคัญและใช้ในการตัดสินใจว่าความเสี่ยงใดควรเร่งจัดการก่อน โดยตารางจัดลำดับความเสี่ยงจะคิดคำนวณจากผลคูณระดับคะแนนระหว่างโอกาสที่จะเกิดกับความรุนแรงของผลกระทบของความเสี่ยง ซึ่งตารางจัดลำดับความเสี่ยง จะแสดงให้เห็นถึงขอบเขตความรุนแรงที่บริษัทยอมรับได้ เพื่อกำหนดเป็นเป้าหมายในภาพรวมว่าจะต้องบริหารความเสี่ยงจนมีระดับความรุนแรงที่ลดลงมาอยู่ในระดับที่ยอมรับได้

ระดับของโอกาสเกิดความเสี่ยง	ระดับความรุนแรงของผลกระทบของความเสี่ยง				
	1 = น้อยมาก	2 = น้อย	3 = ปานกลาง	4 = สูง	5 = สูงมาก
1 = น้อยมาก	1	2	3	4	5
2 = น้อย	2	4	6	8	10
3 = ปานกลาง	3	6	9	12	15
4 = สูง	4	8	12	16	20
5 = สูงมาก	5	10	15	20	25

5. ความเสี่ยงที่สามารถยอมรับได้ (Risk Appetite) หมายถึงปริมาณความเสี่ยงที่องค์กรสามารถยอมรับได้เมื่อมีความเสี่ยงเกิดขึ้น ดังแสดงในตารางดังนี้

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	แนวทางการดำเนินการ
1 – 3	ต่ำ	ระดับความเสี่ยงที่สามารถยอมรับได้โดยไม่ต้องมีการควบคุมหรือไม่ต้องมีการจัดการความเสี่ยงเพิ่มเติม
4 – 9	ปานกลาง	ระดับความเสี่ยงที่สามารถยอมรับได้ แต่ต้องมีการควบคุมและติดตามความเสี่ยงอย่างสม่ำเสมอ เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
10 – 16	สูง	ระดับความเสี่ยงที่ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้
17 – 25	สูงมาก	ระดับความเสี่ยงที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งรัดจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทันที โดยการหยุด เลิก ลดการดำเนินการกิจกรรม/โครงการที่เป็นความเสี่ยง

6. ดำเนินการตอบสนองต่อความเสี่ยง (Implements Risk Responses) เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดย

6.1. การยอมรับความเสี่ยง (Risk Acceptance) เป็นการกำหนดระดับของผลกระทบที่ยอมรับได้

6.2. การลด/ควบคุมความเสี่ยง (Risk Reduction/Control) เป็นการป้องกันหรือจำกัดผลกระทบ และโอกาสเกิดความเสียหาย

6.3. การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) เป็นการหยุดหรือเปลี่ยนแปลงสิ่งที่เป็นความเสี่ยง

6.4. การกระจาย/โอนความเสี่ยง (Risk Sharing/Spreading) เป็นการกระจายทรัพย์สิน หรือกระบวนการต่างๆ เพื่อลดความเสี่ยงจากการสูญเสีย

7. การรายงานผลการวิเคราะห์ความเสี่ยง (Risk Reporting) เมื่อประเมินความเสี่ยงเสร็จแล้ว และได้พิจารณาการทบทวนจากฝ่ายบริหารเรียบร้อยและ ให้นำเสนอต่อคณะกรรมการผู้บริหารความเสี่ยงของฝ่ายเทคโนโลยีสารสนเทศ เพื่อพิจารณากลั่นกรอง และนำเสนอต่อคณะกรรมการบริษัท อย่างน้อยปีละ 1ครั้ง เพื่อพิจารณาอนุมัติ

รายการการปรับปรุง		
วันที่	เรื่อง	ผู้แก้ไข
25 กรกฎาคม 2565	ปรับปรุงให้สอดคล้องกับนโยบายการบริหารความเสี่ยงของบริษัท ตามการรายงานตรวจสอบภายในครั้งที่ 1 ปี 2565 ของ บริษัท สอบบัญชี ไอวีแอล จำกัด	น.ส.ธนิศร ธนวงศ์เกษม

ผู้อนุมัติ

ลงชื่อ ธนิศร ธนวงศ์เกษม

(ธนิศร ธนวงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 1 สิงหาคม 2565

ลงชื่อ วรกฤต เทพหัสดิน ณ อยุธยา

(วรกฤต เทพหัสดิน ณ อยุธยา)

ผู้รับผิดชอบ

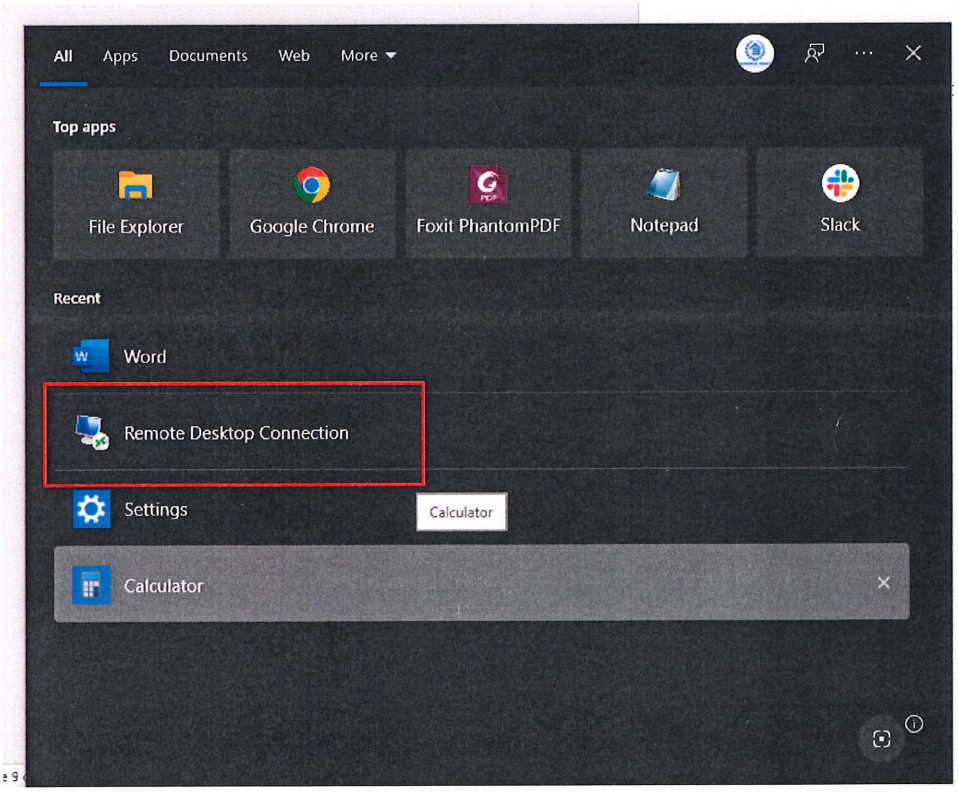
วันที่ 1 ส.ค. 2565

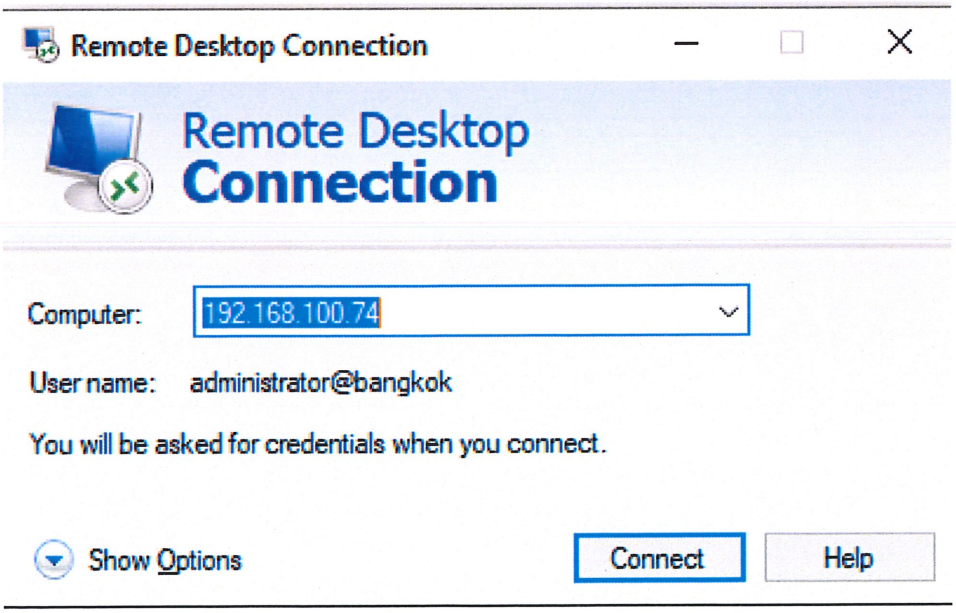
คู่มือสำหรับการใช้งานของ Admin AD (Active Directory)

วัตถุประสงค์ เพื่อเป็นมาตรฐานในการใช้งาน User Administrator ภายในบริษัทให้ได้มีประสิทธิภาพ

ขั้นตอนการใช้งาน Administration ของ AD

1. เลือก Remote Desktop Connection





2. ใส่ IP Address

   2.1. IP: 192.168.100.74

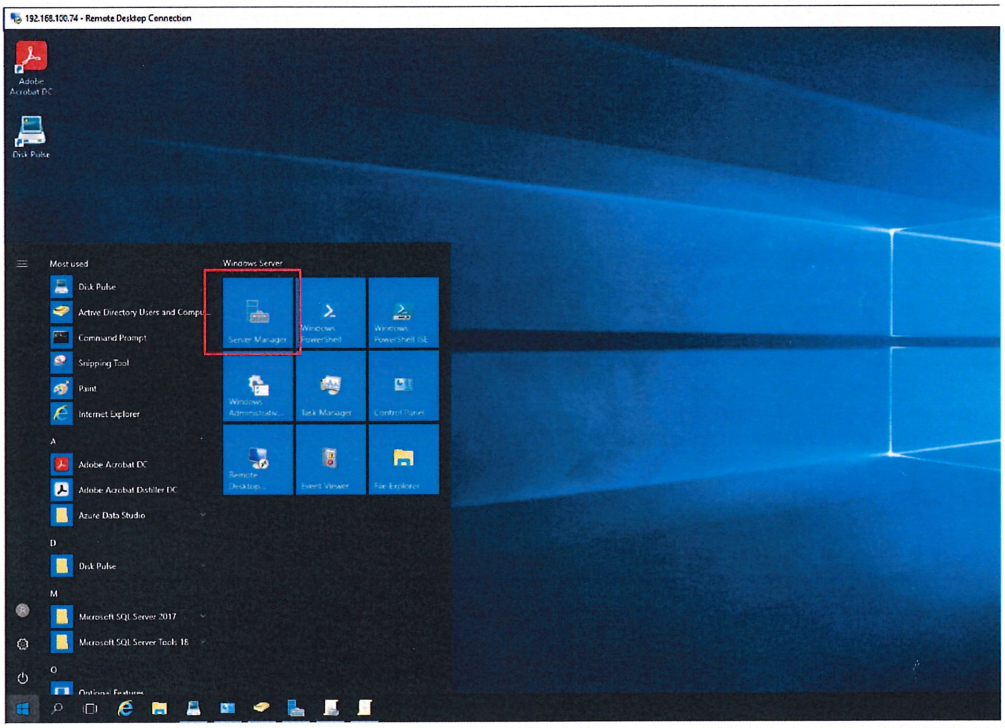
3. Login

   3.1. User: Administrator

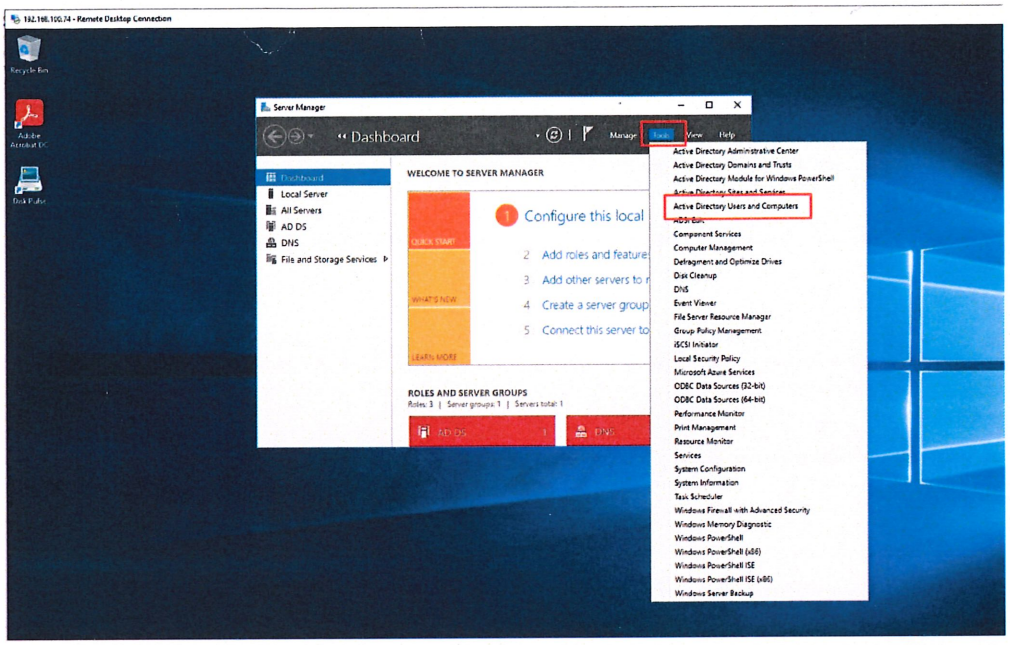
   3.2. Password: (เฉพาะผู้ดูแลระบบเท่านั้น)

4. การสร้างแผนก และผู้ใช้งาน (Organizations and Users)

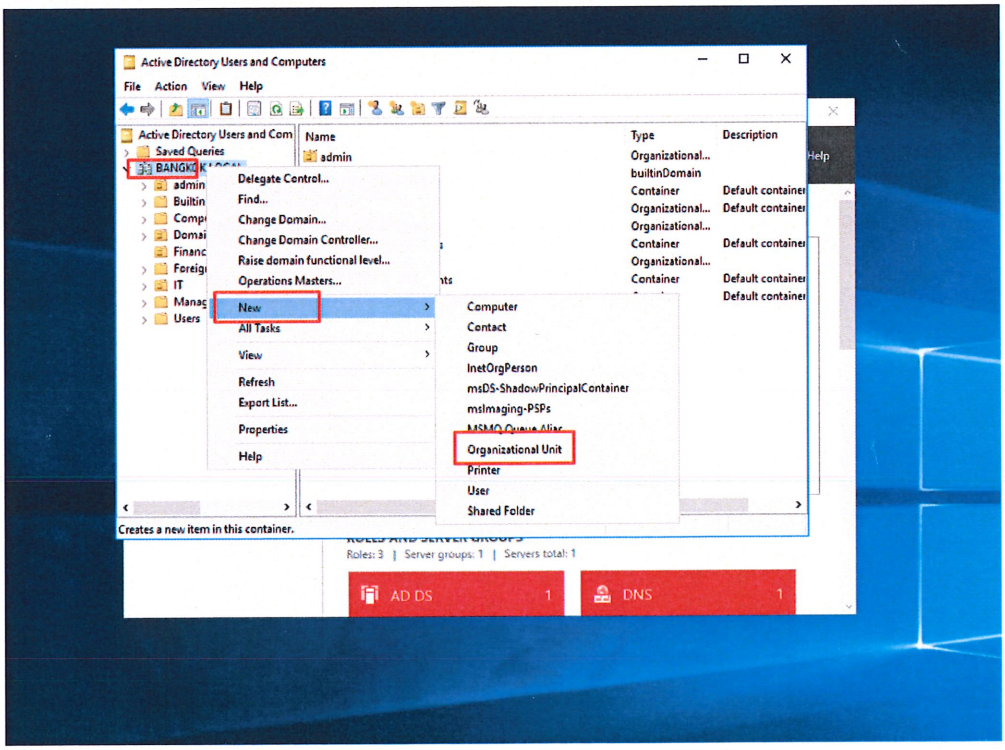
   4.1. เลือก Server Manager

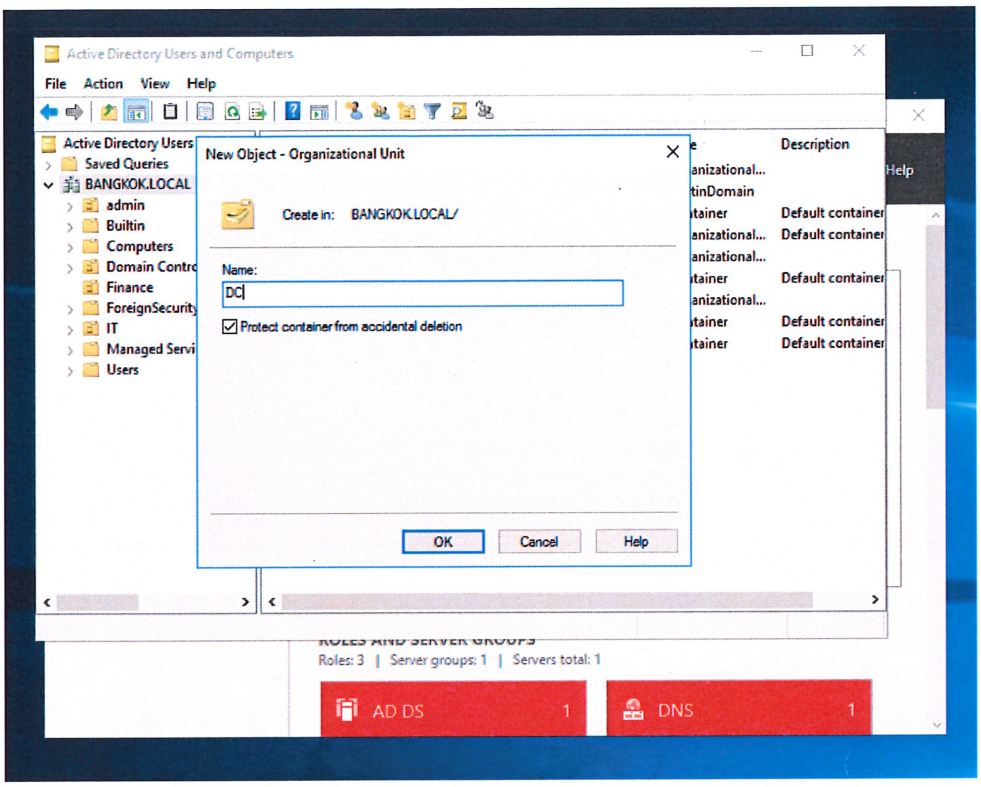


4.2. หน้า Dashboard เลือก Tools และ Active Directory Users and Computers

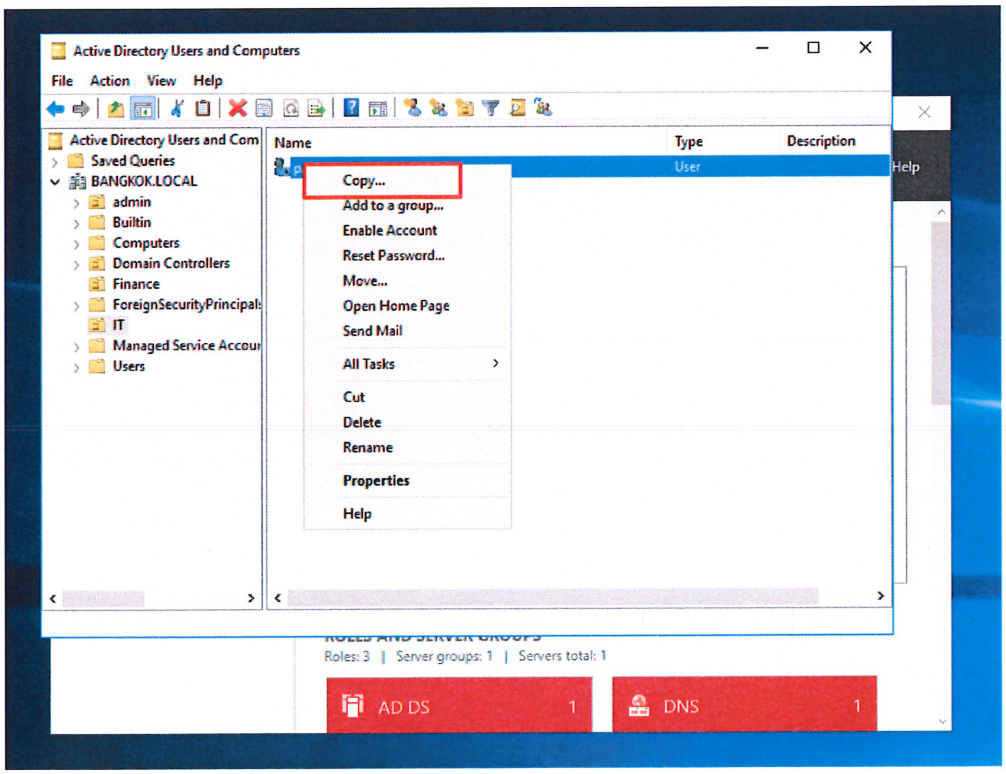


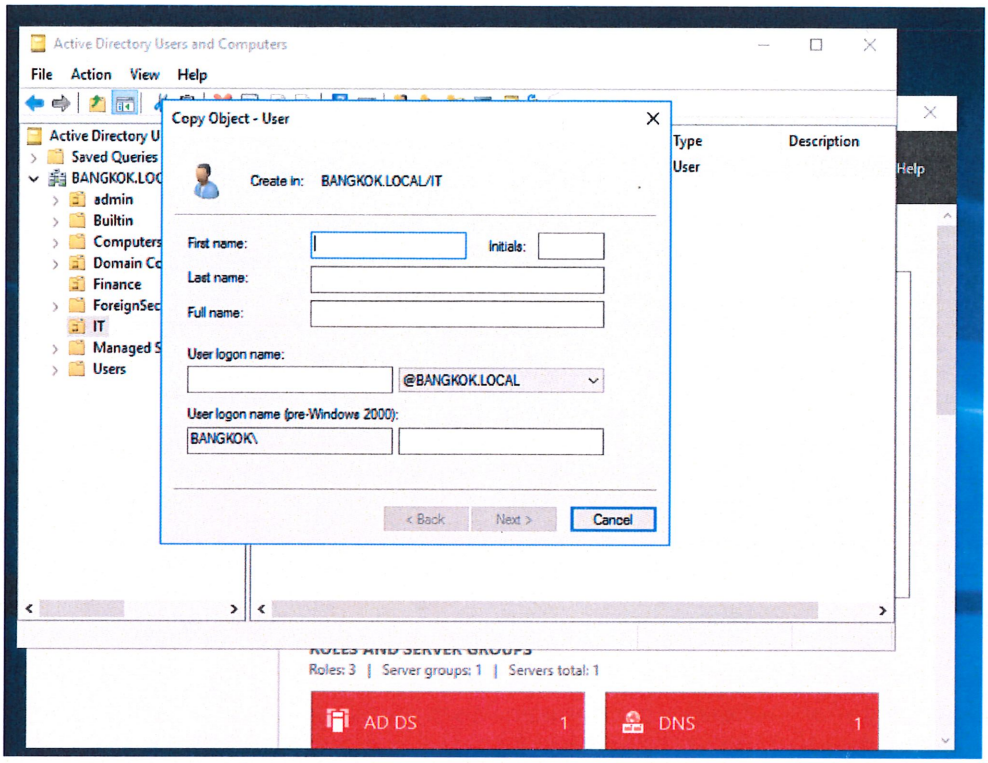
4.3. กรณีสร้างแผนกขึ้นใหม่ให้คลิกขวาที่ Domain และเลือก News Organizational Unit

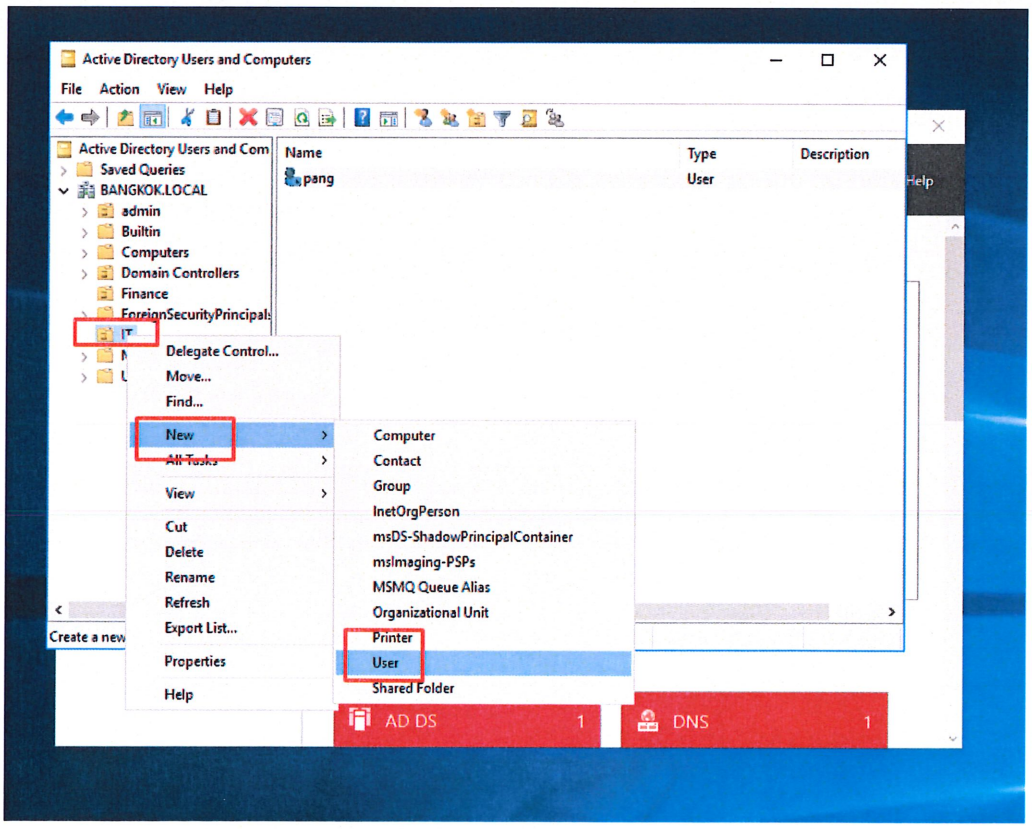




4.4. กรณีสร้าง User ภายในแผนกให้คลิกเลือกที่แผนก และ Copy User เดิม แล้วเปลี่ยนรายละเอียด หรือ New User ขึ้นมาใส่รายละเอียด

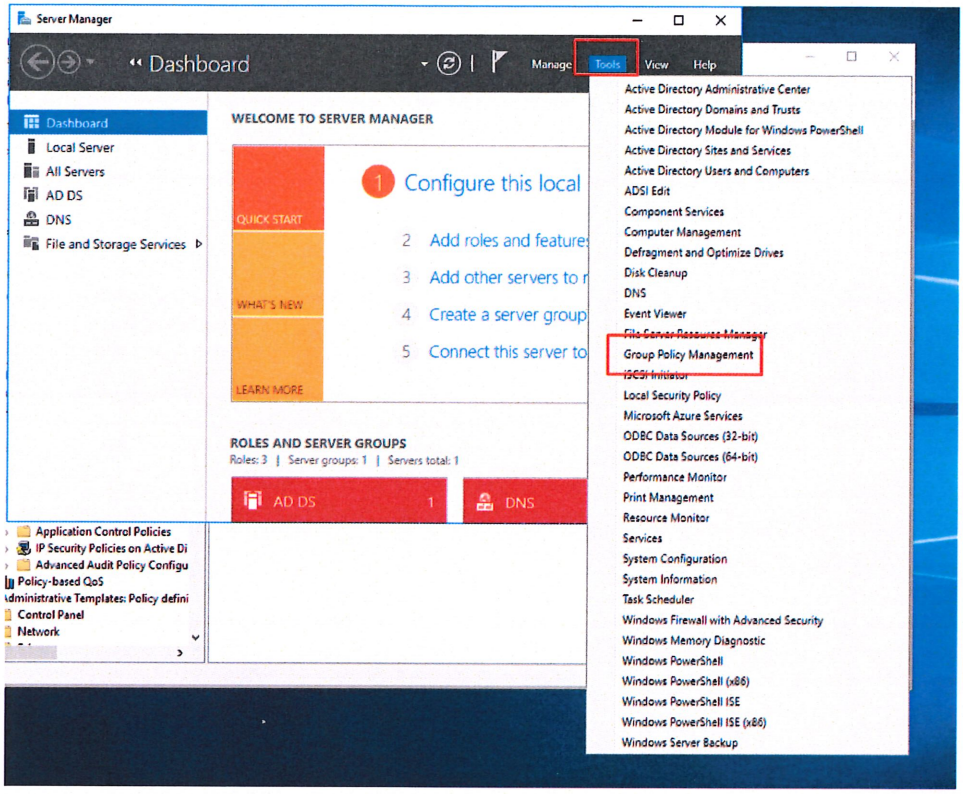



Active Directory Users and Computers
File Action View Help
Copy Object - User
Create in: BANGKOK.LOCAL/IT
First name:
Initials:
Last name:
Full name:
User logon name:
@BANGKOK.LOCAL
User logon name (pre-Windows 2000):
BANGKOK\
< Back
Next >
Cancel
Type
Description
User
Roles: 3 | Server groups: 1 | Servers total: 1
AD DS 1
DNS 1

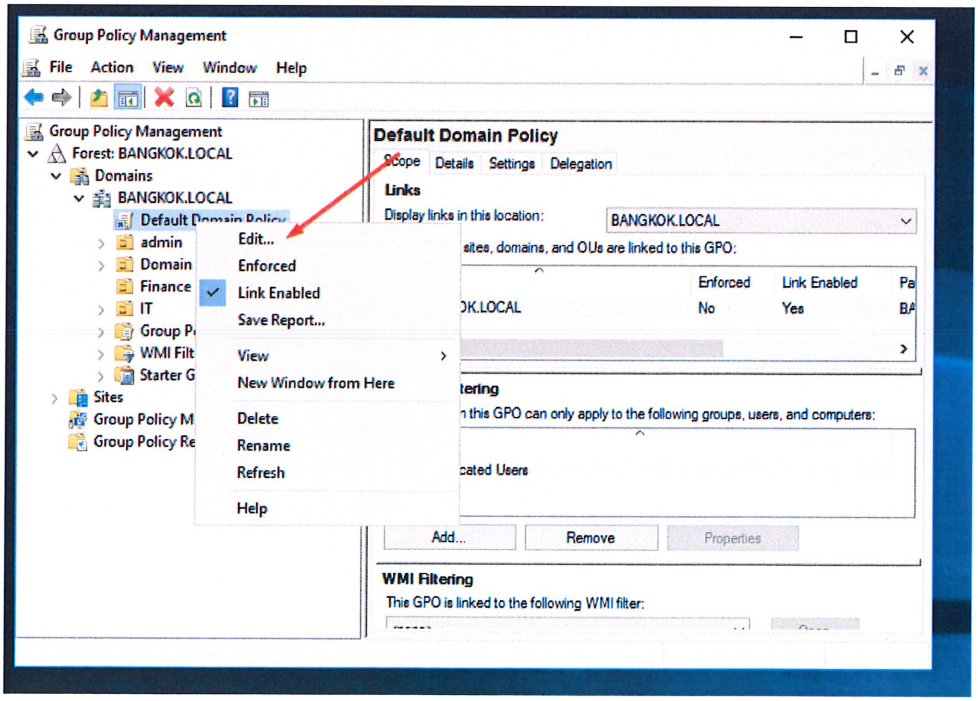

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
BANGKOK.LOCAL
admin
Builtin
Computers
Domain Controllers
Finance
ForeignSecurityPrincipals
IT
Name
Type
Description
pang
User
Delegate Control...
Move...
Find...
New
All Tasks
View
Cut
Delete
Rename
Refresh
Export List...
Properties
Help
Computer
Contact
Group
InetOrgPerson
msDS-ShadowPrincipalContainer
msImaging-PSPs
MSMQ Queue Alias
Organizational Unit
Printer
User
Shared Folder
Create a new
AD DS 1
DNS 1

5. การสร้าง Users Policy

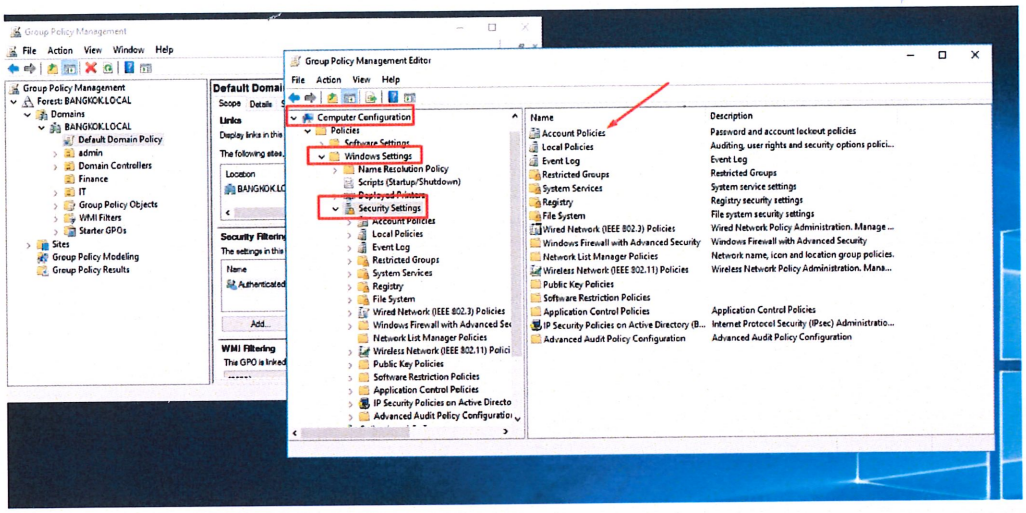
5.1. เข้าที่ Server Manager คลิก Tools และเลือก Group Policy Management



5.2. คลิกขวาที่ Default Domain Policy เลือก Edit



5.3. ที่ Computer Configuration _Policies _Security Settings _Account Policies



5.4. ตั้งค่าตามที่ (อ้างถึง "Standard Operating Procedure" เรื่อง User Account Standard) สามารถดูการตั้งค่าการใช้งานได้ที่เอกสาร "หลักเกณฑ์และการตั้งค่าต่างๆ ในระบบเทคโนโลยีสารสนเทศ"

ผู้อนุมัติ

ลงชื่อ วรวุฒิ เทพทัสสิน

(วรวุฒิ เทพทัสสิน ณ อยุธยา)

ผู้รับผิดชอบ

วันที่ 27 เม.ย 65

ลงชื่อ ชนิศร ธนวงศ์เกษม

(ชนิศร ธนวงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

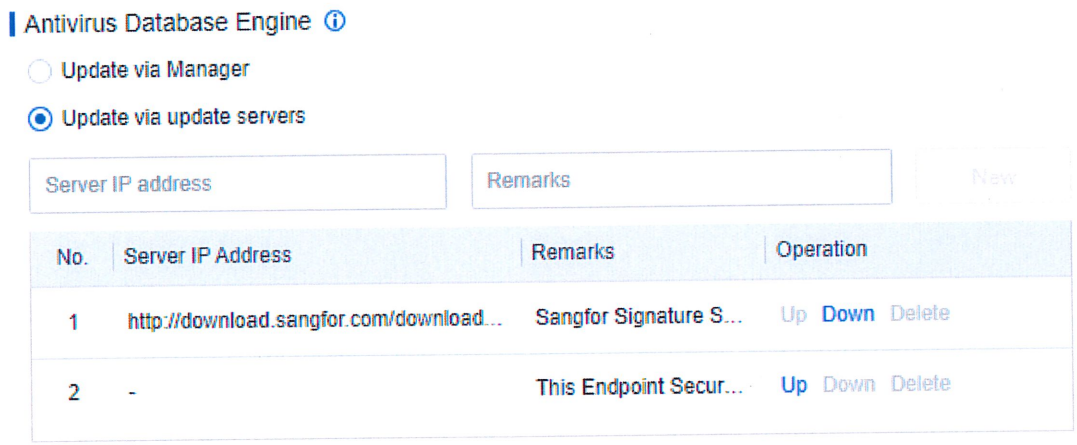
วันที่ 27 เม.ย 65

ขั้นตอนการตั้งค่าโปรแกรม Anti-Virus

1. Antivirus Database Engine

   1.1. Update from sangfor

   1.2. Update from endpoint in local networks

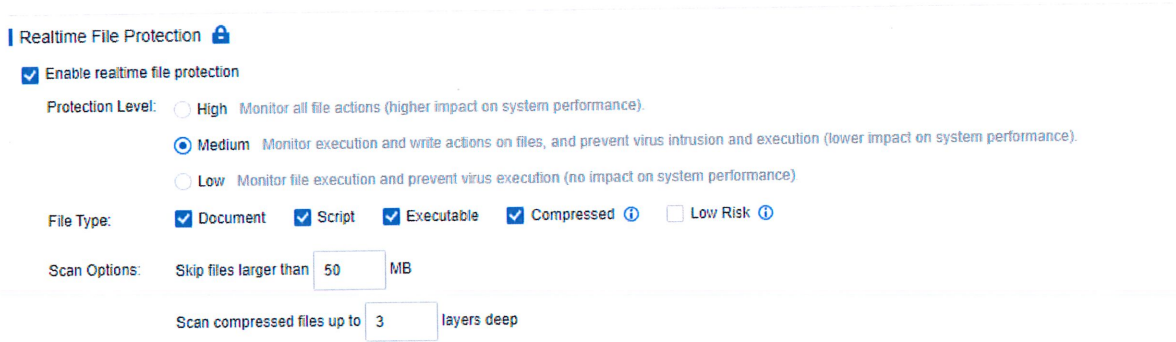


2. Realtime Protection

   2.1. Enable realtime protection level : medium

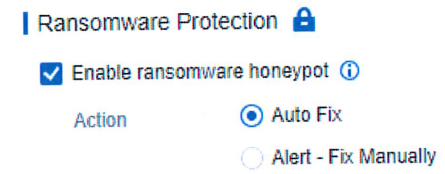
   2.2. File type : Document, Script, Executable, Compressed

   2.3. Scan Option : Skip files larger than 50 mb and 3 layer

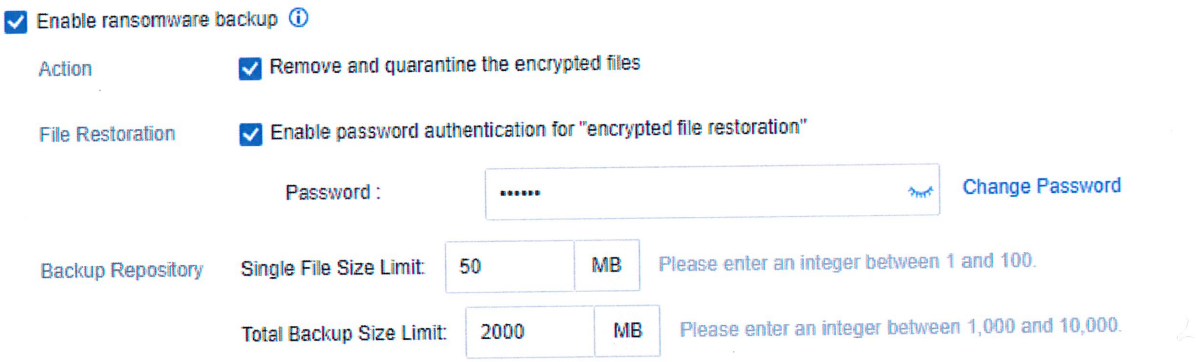


3. Anti-Ransomware

3.1. Ransomware Protection : Auto Fix

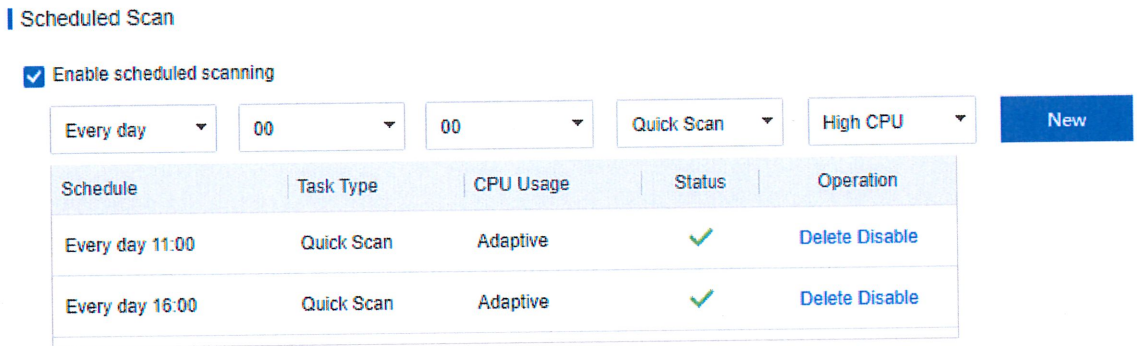


3.2. Enable ransomware backup

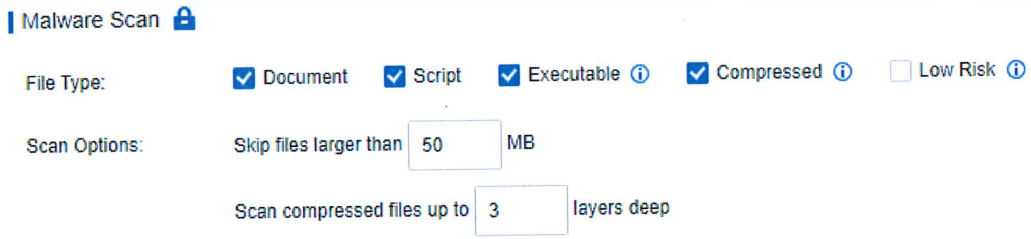


4. Anti-Malware

4.1. Scheduled Scan : Every day 11:00AM and 16:00PM quick scan.

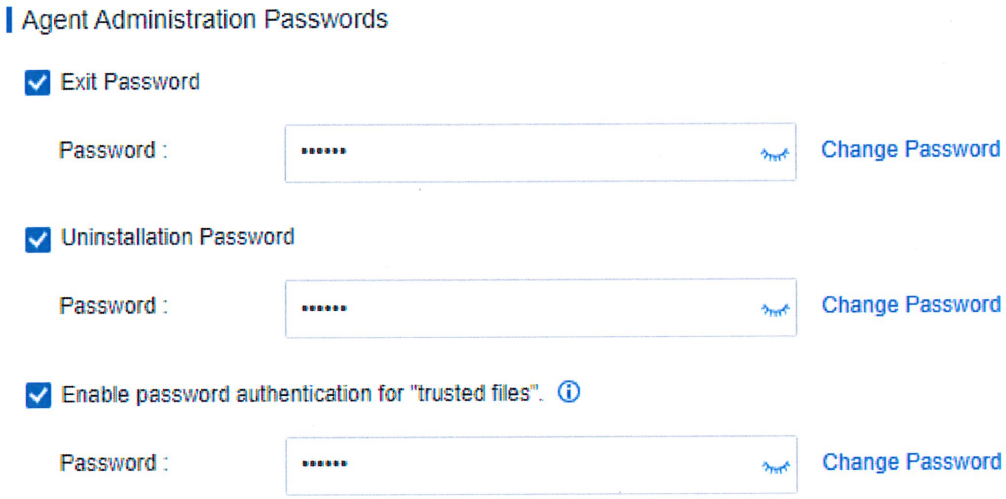


4.2. Malware Scan : scan file type document, script, executable, compressed.



5. Basic Configuration

5.1. Agent Administration Passwords for exit, uninstall and trusted files



ประวัติการปรับปรุงเอกสาร				
ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 พฤษภาคม 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา
2	2.0	ปรับปรุงขั้นตอนการตั้งค่า	11 พฤศจิกายน 2567	ชาญยุทธ วัฒนาศักดิกุล

ลงชื่อ _____

(นาย ชาญยุทธ วัฒนาศักดิกุล)

ผู้รับผิดชอบ

วันที่ 11/11/67

ผู้อนุมัติ

ลงชื่อ _____

(นางสาว ธนิศร ธนวงศ์เกษม)

ประธานเจ้าหน้าที่เทคโนโลยีสารสนเทศ

วันที่ 11/11/67

ขั้นตอนการใช้ User หรือ Administrator จากหน่วยงานภายนอก

วัตถุประสงค์ เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร ให้เป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางในการคัดเลือก ควบคุมการปฏิบัติงานของหน่วยงานภายนอก

แนวทางปฏิบัติ

1. บุคคลที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรด้วย User หรือ Administrator จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้บริหารฝ่ายเทคโนโลยีสารสนเทศโดยให้ทางผู้ขอรับบริการเขียนเป็น E-Mail ส่งถึงผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ และ cc. ผู้บริหารโดยตรงของผู้ขอ และผู้บริหารหน่วยงานที่รับผิดชอบโดยตรง (หน่วยงานที่ติดต่อผู้ขอ)
2. รายละเอียดที่ต้องแจ้งการขอเข้าใช้ผ่าน E-Mail
   2.1. ชื่อนามสกุลของผู้ขอใช้
   2.2. เหตุผลในการขอใช้
   2.3. ระยะเวลาในการใช้
3. หน่วยงานนั้น หรือ บุคคลนั้นจะต้องมีการลงนามในสัญญาห้ามเปิดเผยข้อมูล (Non-disclosure Agreement) เรียบร้อยแล้ว
4. หน่วยงานนั้น หรือ บุคคลนั้นจะต้องมีการลงนามในนโยบายการใช้งานระบบคอมพิวเตอร์ (Computer Usage Policy) และ Software and Hardware Policy
5. ฝ่ายเทคโนโลยีสารสนเทศทำการบันทึกการขอเข้าใช้งาน ผ่านระบบ Kintone
6. หลังจากเสร็จสิ้นการใช้งานตามระยะเวลาที่กำหนด ทางฝ่ายเทคโนโลยีสารสนเทศ จะทำการเปลี่ยนรหัสผ่านของ User Administrator ของระบบที่ทางผู้ขอใช้ ถ้าเป็น User ทั่วไปจะทำการ ลบทันทีที่หมดอายุ หากจะขอใช้อีกครั้ง ให้ทำเรื่องขออนุญาตเข้ามาใหม่ให้ปฏิบัติตามข้อ 1 และ 2 ใหม่อีกครั้ง
7. ฝ่ายเทคโนโลยีสารสนเทศมีสิทธิ์ที่จะงับการใช้งานได้ตลอดเวลา หากผู้ใช้มีการใช้งานที่ผิดวัตถุประสงค์ นอกเหนือขอบเขตงานที่ได้รับอนุมัติ
8. บริษัทมีสิทธิ์ในการตรวจสอบดูข้อมูลย้อนหลังการใช้งาน ได้ถูกต้องตามกฎหมาย

ผู้อนุมัติ

ลงชื่อ วรวุฒิ

(วรวุฒิ เทพทัสดิน ณ อยุธยา)

ผู้รับผิดชอบ

วันที่ 25/06/65

ลงชื่อ ชนิดร ชนวงศ์เกษม

(ชนิดร ชนวงศ์เกษม)

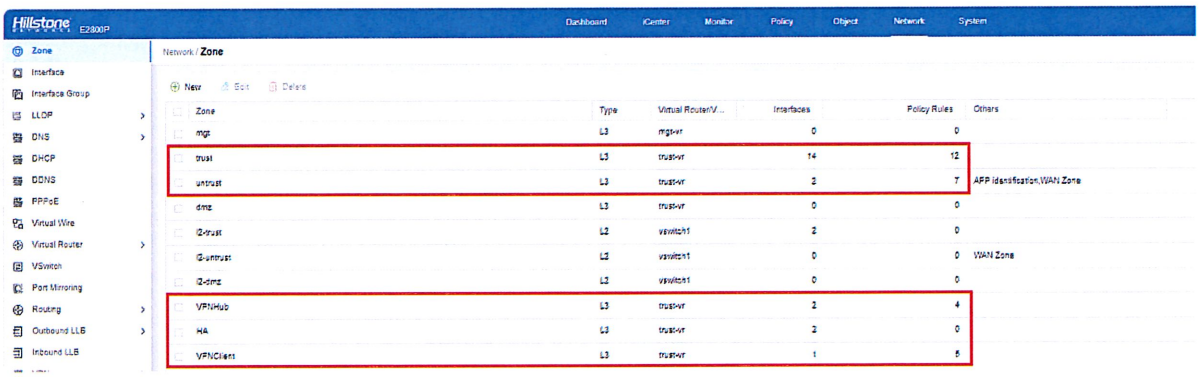
ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 25-06-65

ขั้นตอนการตั้งค่า Firewall

วัตถุประสงค์ เพื่อให้เป็นมาตรฐานการควบคุมการตั้งค่าระบบ Firewall และการตั้งค่า HA ให้มั่นคงปลอดภัยและใช้งานได้อย่างมีประสิทธิภาพได้มีการตั้งค่าดังนี้

1. **การทำ zoning แบ่งออกเป็น 5 ประเภทดังนี้**
   - 1.1. Trust คือ Zone Internal Member คือ VLAN 10,99,101-110,115-116,200
   - 1.2. Untrust คือ Zone Internet Member คือ interface 0/1, interface 0/3
   - 1.3. VPNHub คือ Zone Cloud Member คือ 192.168.100.74
   - 1.4. VPNClient คือ Zone ที่ใช้เชื่อมต่อผ่าน Virtual Private Network (VPN)
   - 1.5. HA คือ Zone ที่ใช้ Sync Configuration Firewall Master และ Slave



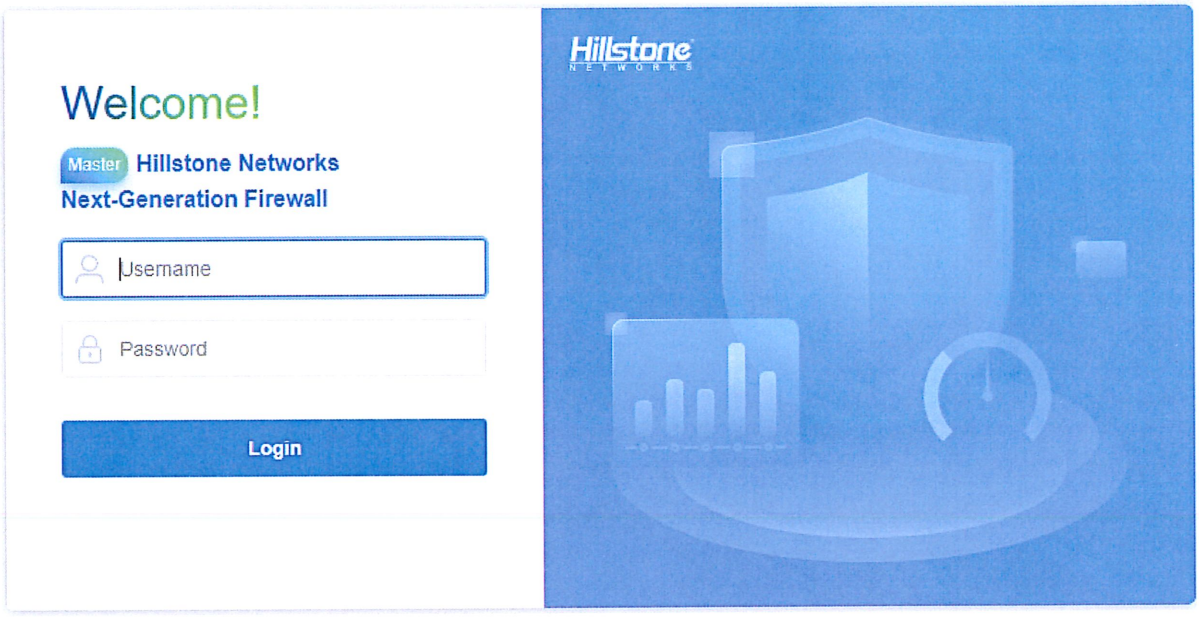
2. **การทำ VLAN โดยแบ่งได้ ดังนี้**

VLAN	VLAN Name	IP Address
200	VPN	192.168.200.0/24
10	Server	192.168.10.0/24
99	Network Management	192.168.99.0/24
101	Outlet ,Printer	192.168.101.0/24
102	Acc ,Fin	192.168.102.0/24
103	IT	192.168.103.0/24
104	DC,AGENT	192.168.104.0/24

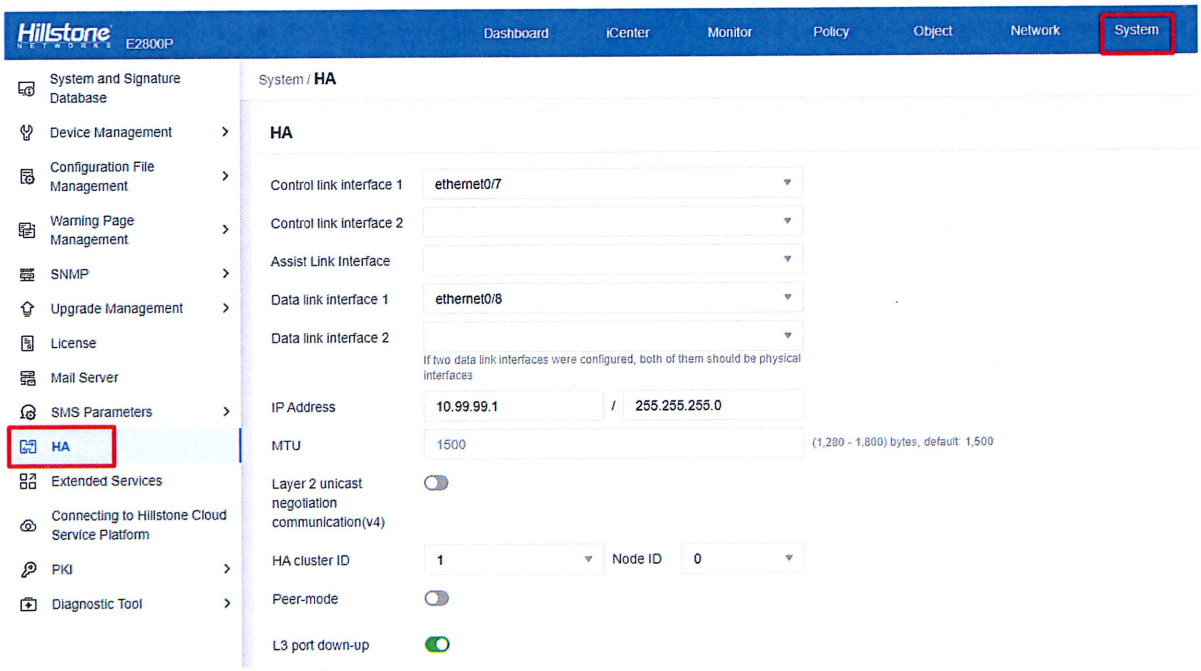
VLAN	VLAN Name	IP address
105	COMSEC,BOD,HR	192.168.106.0/24
106	MK	192.168.106.0/24
107	LIST,SALE	192.168.107.0/24
108	REN,DESIGN,PUR	192.168.108.0/24
109	<Stand by>	192.168.109.0/24
110	<Stand by>	192.168.110.0/24
115	Guest-WiFi	192.168.115.0/24
116	CCTV	192.168.116.0/24

3. การตั้งค่า HA

3.1 Login เข้าใช้งาน Firewall



3.2 เลือกเมนู System > เลือกเมนู HA



3.3 ที่เมนู HA กำหนดค่าตามนี้

3.3.1 Control link interface 1 = Firewall ทั้ง 2 เครื่อง เลือก Port 7 เหมือนกัน

3.3.2 Data link interface 1 = Firewall ทั้ง 2 เครื่อง เลือก Port 8 เหมือนกัน

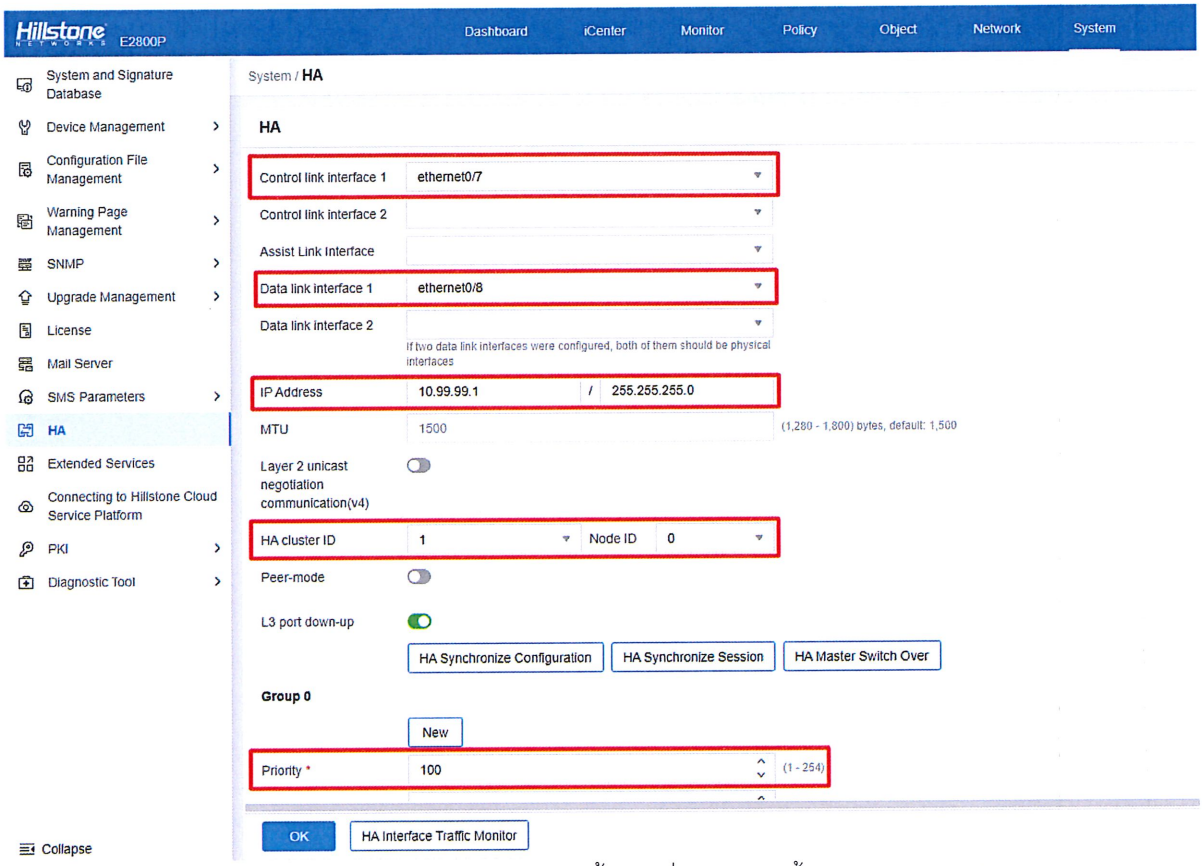
3.3.3 IP Address = กำหนด IP ให้กับ Firewall ทั้ง 2 เครื่อง โดยใช้ IP ต้องอยู่ Network เดียวกัน

3.3.4 HA Cluster ID = Firewall ทั้ง 2 เครื่อง เลือก HA Cluster ID เดียว

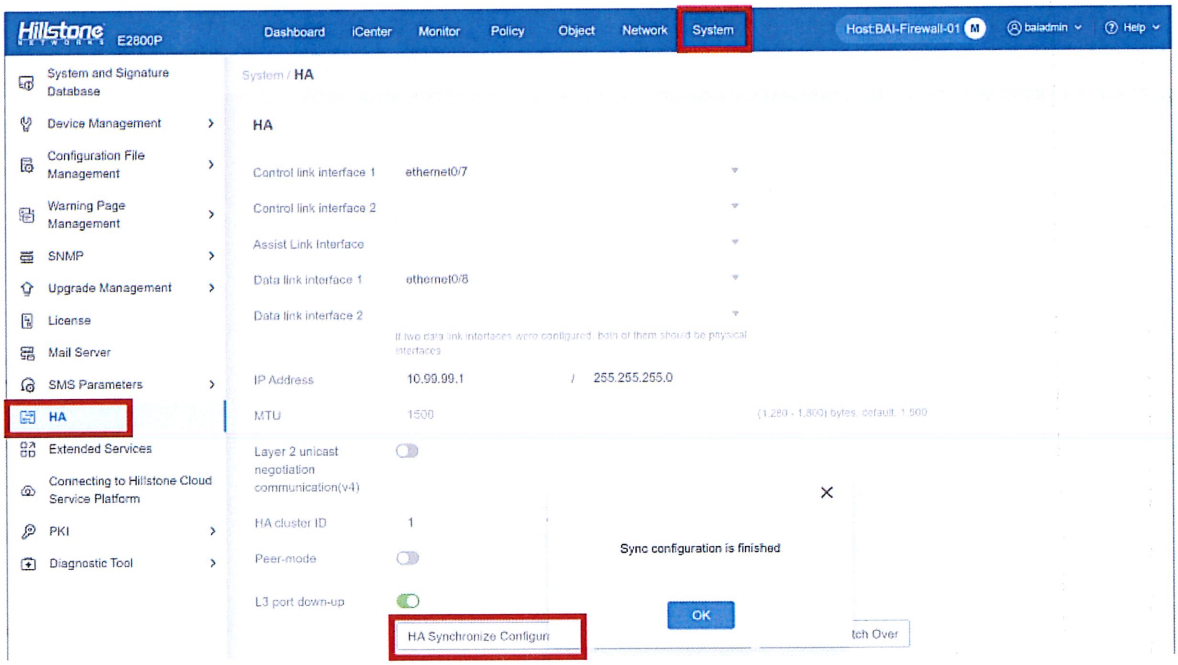
3.3.5 Node ID = Firewall ทั้ง 2 เครื่อง เลือก Hode ID (0,1) ต่างกัน

3.3.6 Priority = Firewall ทั้ง 2 เครื่อง เลือก Priority ต่างกัน โดย Firewall ที่มีค่า Priority มากกว่าจะทำหน้าที่ Standby

3.3.7 >เลือก OK

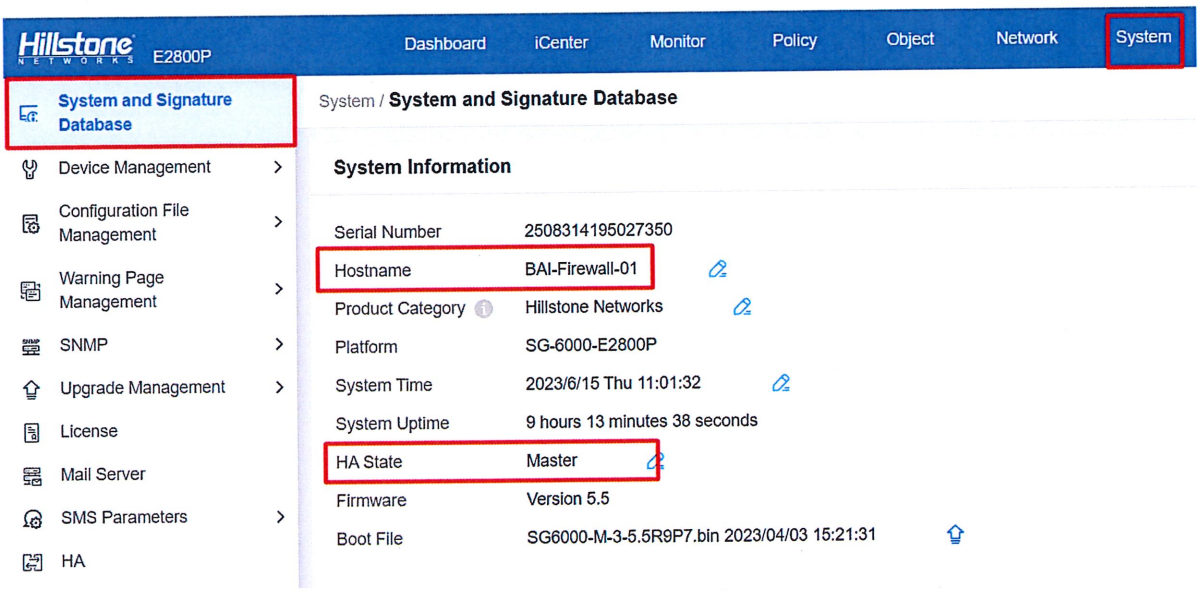


3.4 ตรวจสอบการ Synchronize ข้อมูลระหว่าง Firewall ทั้ง 2 เครื่องหลังจากตั้งค่า HA เสร็จ >เลือกเมนู System >เลือก HA > เลือก HA Synchronize Configuration

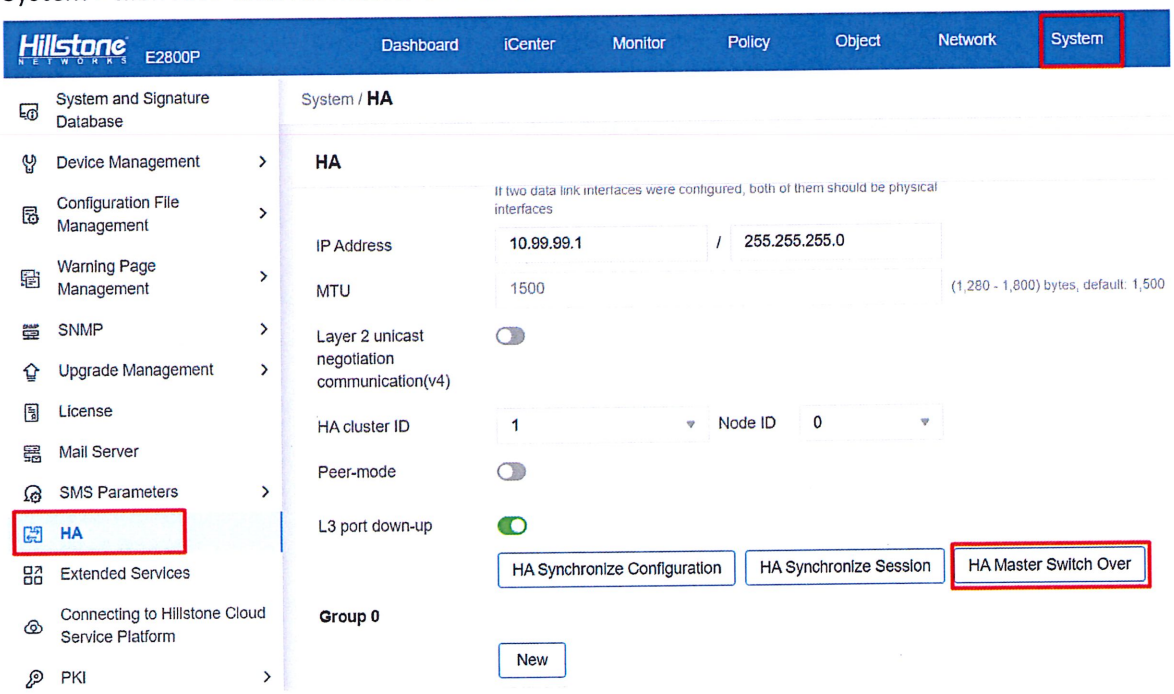


4. ทดสอบใช้งาน HA

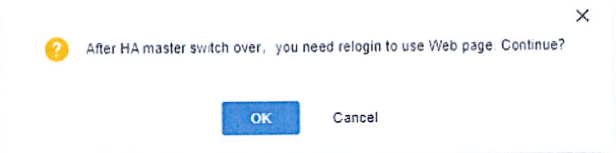
4.1 ตรวจสอบ Firewall ที่ทำหน้าที่เป็นตัวหลัก (Master) >เลือกเมนู System > เลือกเมนู System and Signature Database



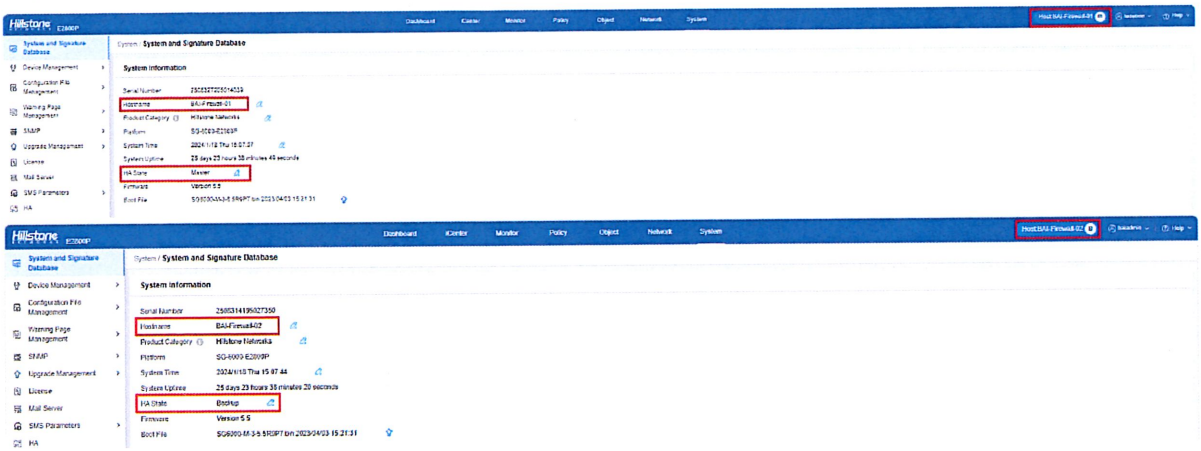
4.2 ทำการสลับ Firewall ตัวหลัก (Master) จาก BAI-Firewall-01 เปลี่ยนเป็น BAI-Firewall-02 > เลือก เมนู System > เลือก HA > เลือก HA Master Switch Over



4.3 เลือก OK



4.4 ตรวจสอบ Firewall ที่ทำหนHAที่เป็นตัวหลัก (Master) > เลือกเมนู System > เลือก System and Signature Database > เลือก HA State

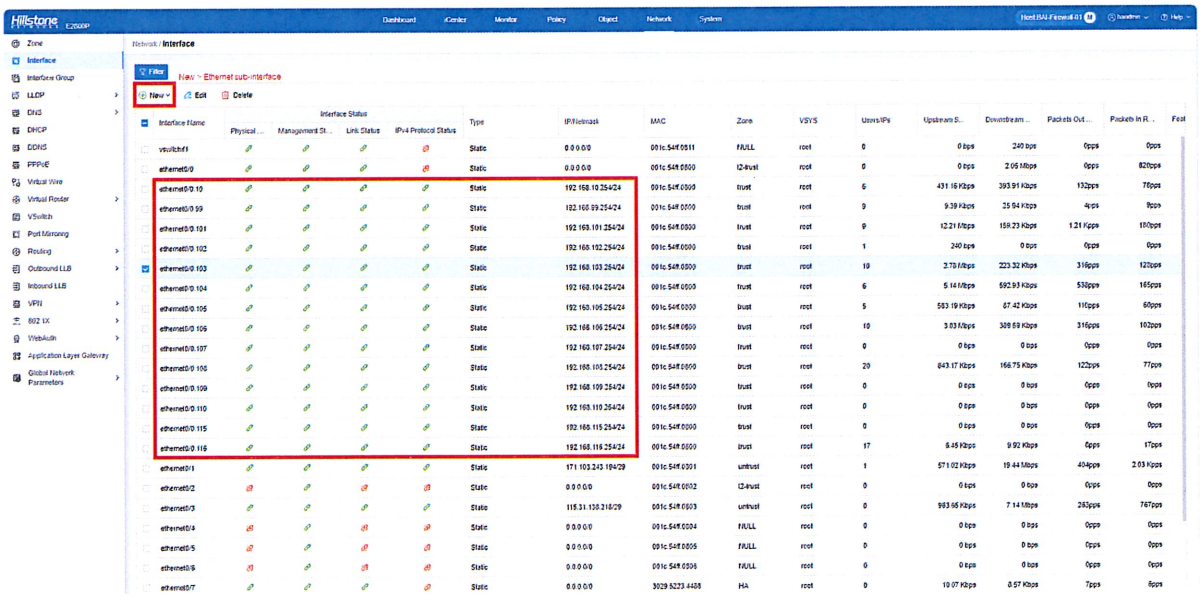


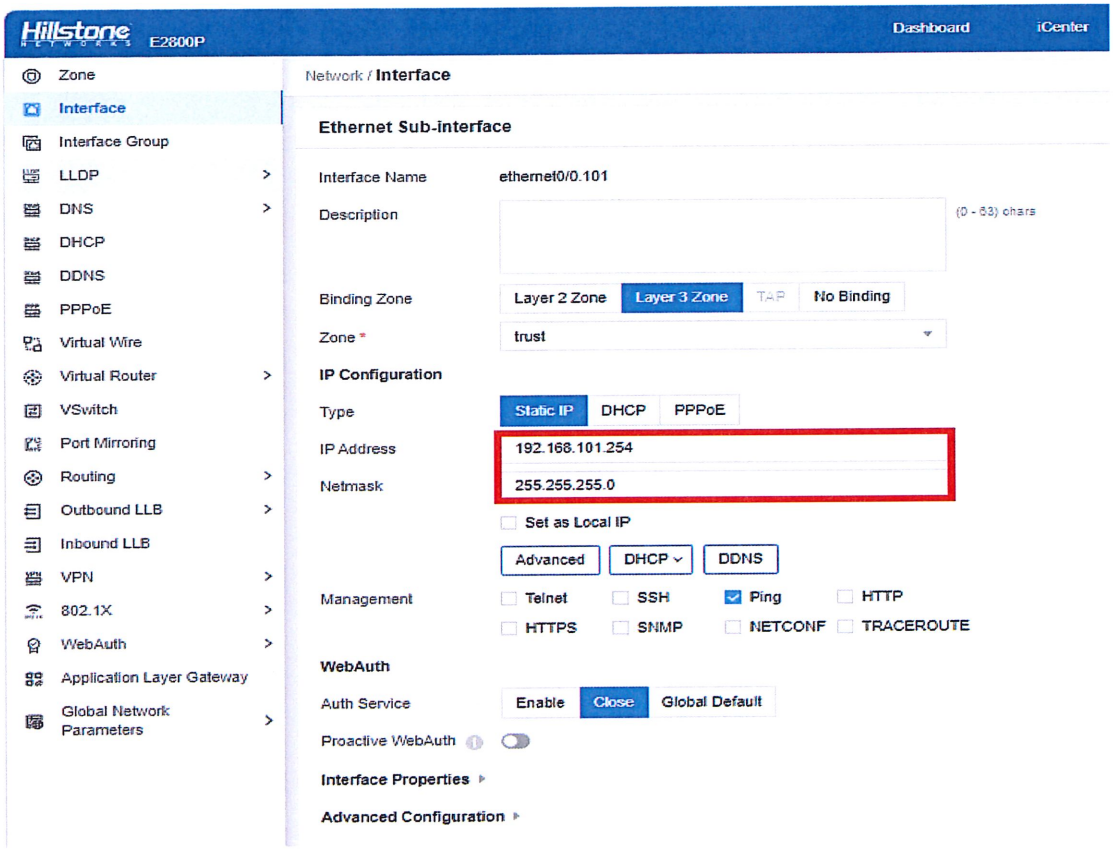
4.5 ทดสอบการเข้าเครือข่าย หลังจากทำการสลับ Firewall ตัวหลัก (Master) จาก BAI-Firewall-01 เปลี่ยนเป็น BAI-Firewall-02 จะเห็นว่าสามารถเข้าถึงเครือข่ายได้ปกติ

```
Pinging bangkokasset.co.th [203.150.20.210] with 32 bytes of data:
Reply from 203.150.20.210: bytes=32 time=14ms TTL=118
Reply from 203.150.20.210: bytes=32 time=19ms TTL=118
Reply from 203.150.20.210: bytes=32 time=14ms TTL=118
Reply from 203.150.20.210: bytes=32 time=77ms TTL=118

Ping statistics for 203.150.20.210:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 77ms, Average = 31ms

C:\Users\chanyut.w>ping 192.168.100.74

Pinging 192.168.100.74 with 32 bytes of data:
Reply from 192.168.100.74: bytes=32 time=13ms TTL=126
Reply from 192.168.100.74: bytes=32 time=12ms TTL=126
Reply from 192.168.100.74: bytes=32 time=12ms TTL=126
Reply from 192.168.100.74: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.100.74:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 13ms, Average = 12ms

C:\Users\chanyut.w>ping 192.168.10.224

Pinging 192.168.10.224 with 32 bytes of data:
Reply from 192.168.10.224: bytes=32 time=10ms TTL=63
Reply from 192.168.10.224: bytes=32 time=12ms TTL=63
Reply from 192.168.10.224: bytes=32 time=9ms TTL=63
Reply from 192.168.10.224: bytes=32 time=10ms TTL=63

Ping statistics for 192.168.10.224:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 12ms, Average = 10ms
```

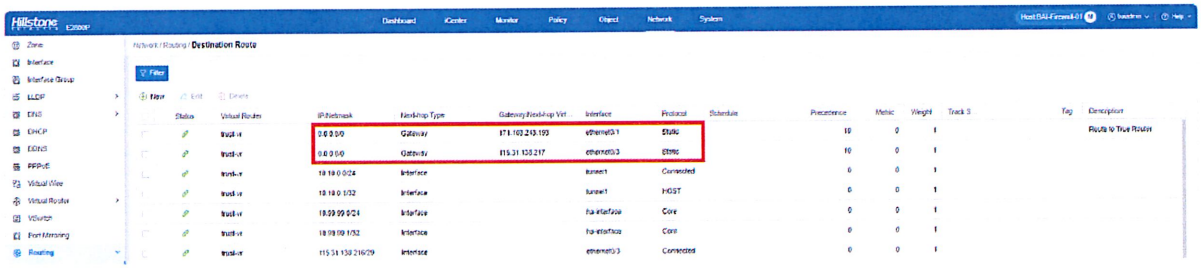
5. การตั้งค่า Default Gateway

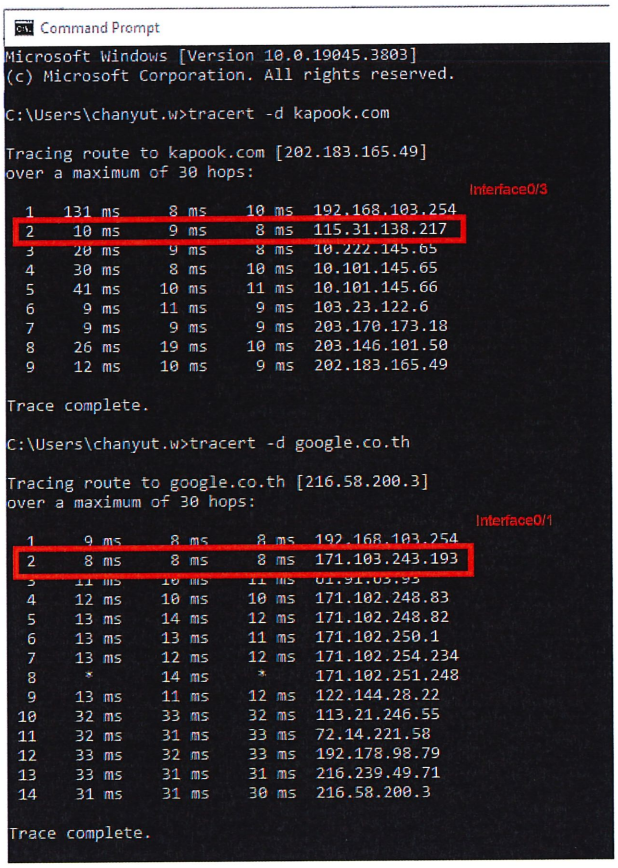
5.1. VLAN 10 IP 192.168.10.254/24
5.2. VLAN 99 IP 192.168.99.254/24
5.3. VLAN 101 IP 192.168.101.254/24
5.4. VLAN 102 IP 192.168.102.254/24
5.5. VLAN 103 IP 192.168.103.254/24
5.6. VLAN 104 IP 192.168.104.254/24
5.7. VLAN 105 IP 192.168.105.254/24
5.8. VLAN 106 IP 192.168.106.254/24
5.9. VLAN 107 IP 192.168.107.254/24
5.10. VLAN 108 IP 192.168.108.254/24
5.11. VLAN 109 IP 192.168.109.254/24
5.12. VLAN 110 IP 192.168.110.254/24
5.13. VLAN 115 IP 192.168.115.254/24
5.14. VLAN 116 IP 192.168.116.254/24
5.15. VLAN 200 IP 192.168.200.254/24



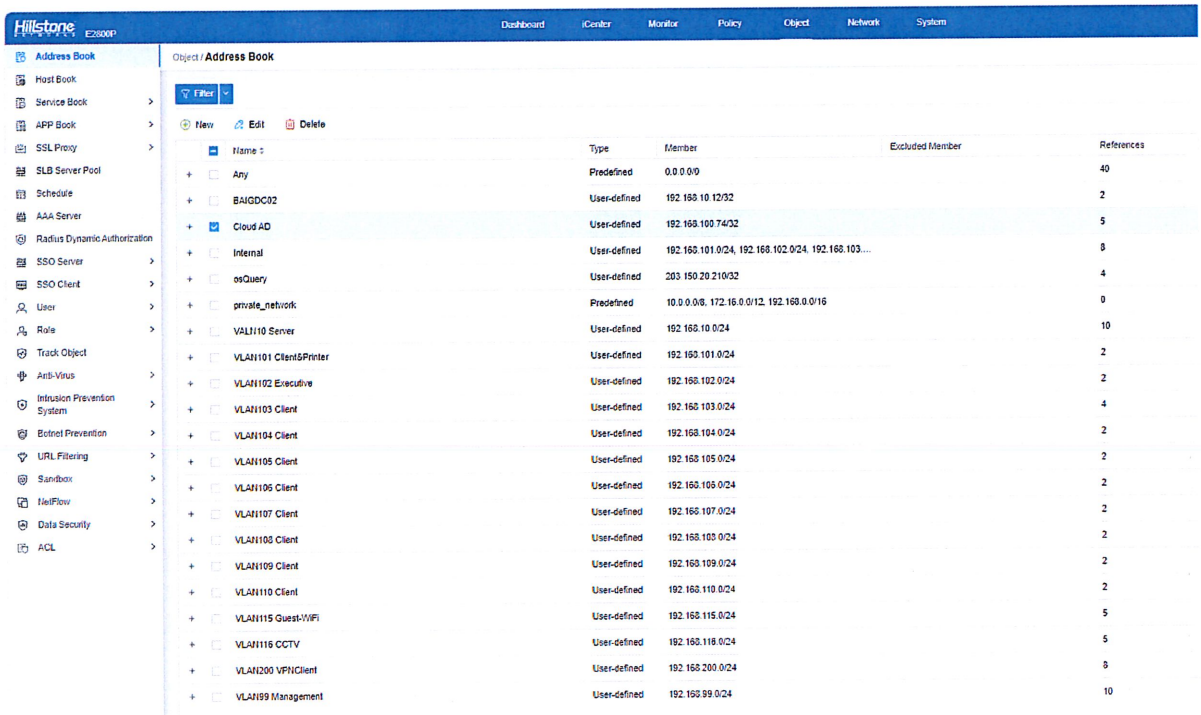


6. ตั้งค่า Load Balancing โดยใช้ Bandwidth ของ Interface0/1 และ Interface0/3 พร้อมกัน





7. ตั้ง Address Book แต่ละ VLAN



ประวัติการการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 สิงหาคม 2566	วรวุฒิ เทพหัสดิน ณ อยุธยา
2	2.0	ปรับปรุงเพิ่มเติม ขั้นตอนการตั้งค่า HA	15 มิถุนายน 2566	วรวุฒิ เทพหัสดิน ณ อยุธยา
3	2.1	ปรับปรุงเพิ่มข้อมูล VLAN 11 สำหรับ Server และนำ VLAN 0-1 ออกเพราะว่าเป็น Management ของอุปกรณ์	21 กรกฎาคม 2566	วรวุฒิ เทพหัสดิน ณ อยุธยา
4	3.0	ปรับปรุงโครงสร้างหลังย้ายสำนักงาน	1 กุมภาพันธ์ 2567	ชาญยุทธ วัฒนาศักดิกุล

ลงชื่อ_____

(นาย ชาญยุทธ วัฒนาศักดิกุล)

ผู้รับผิดชอบ

วันที่ 1/02/67

ผู้อนุมัติ

ลงชื่อ_____

(นางสาว ธนิศร ธนวงศ์เกษม)

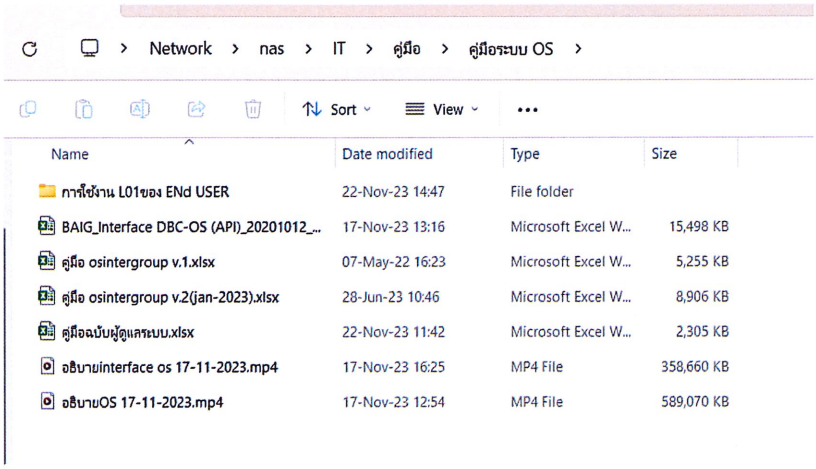
ประธานเจ้าหน้าที่เทคโนโลยีสารสนเทศ

วันที่ 01/02/67

คู่มือ และเอกสารประกอบการพัฒนาโปรแกรม

คู่มือระบบ OS มีดังนี้

\\nas\IT\คู่มือ\คู่มือระบบ OS



เอกสารประกอบการพัฒนาโปรแกรม

จัดเก็บเป็น วีดีโอ

การสร้าง BOQและ PR TEMPLATE :

https://drive.google.com/file/d/1pae1hkpGKhYOsMhqCqfwbFDxADQhcq-Y/view?usp=sharing

https://drive.google.com/file/d/1cXUlPcYys-2nE8c5qBJqN3v7f-YF0_7E/view?usp=sharing

https://drive.google.com/file/d/11HcBZM85s8vP8Lfv_GB8VE-b2dSBQj4J/view?usp=sharing

https://drive.google.com/file/d/1IyGW0SIQIj_EsWEjTSWiWrRXGdL6w9zN/view?usp=sharing

OS pahse3 :

https://www.dropbox.com/s/cr7ommuqznn0zug/OS%20Phase3.mp4?dl=0

BANGKOK ASSET INTERGROUP	คู่มือกระบวนการปฏิบัติงาน (Procedure/Manual)	IT-Procedure-037	
	คู่มือ และเอกสารประกอบการพัฒนาโปรแกรม OS	ฉบับที่ : 1.1	แผ่นที่ : 2/2
	OS Manual Procedure	เริ่มใช้ :1 กุมภาพันธ์ 2567	

ประวัติการการปรับปรุงเอกสาร				
ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 กรกฎาคม 2565	ธนิศร ธนวงศ์เกษม
2	1.1	แก้ไข IP	1 กุมภาพันธ์ 2567	ชาญยุทธ วัฒนาศักดิกุล

ลงชื่อ_____

(นาย ชาญยุทธ วัฒนาศักดิกุล)

ผู้รับผิดชอบ

วันที่ 1/02/67

ผู้อนุมัติ

ลงชื่อ_____

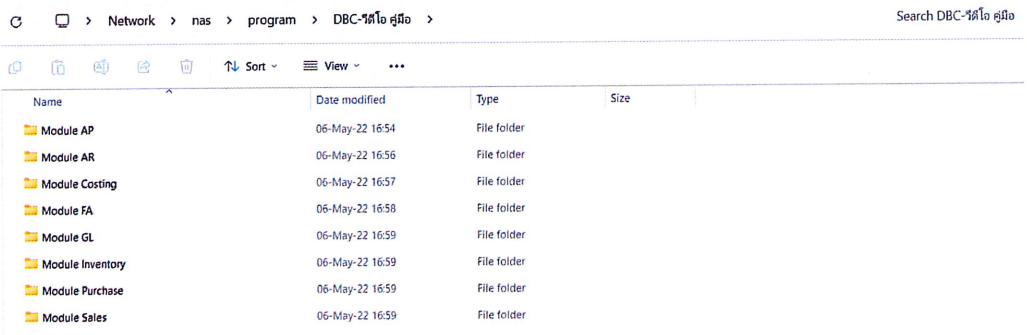
(นางสาว ธนิศร ธนวงศ์เกษม)

ประธานเจ้าหน้าที่เทคโนโลยีสารสนเทศ

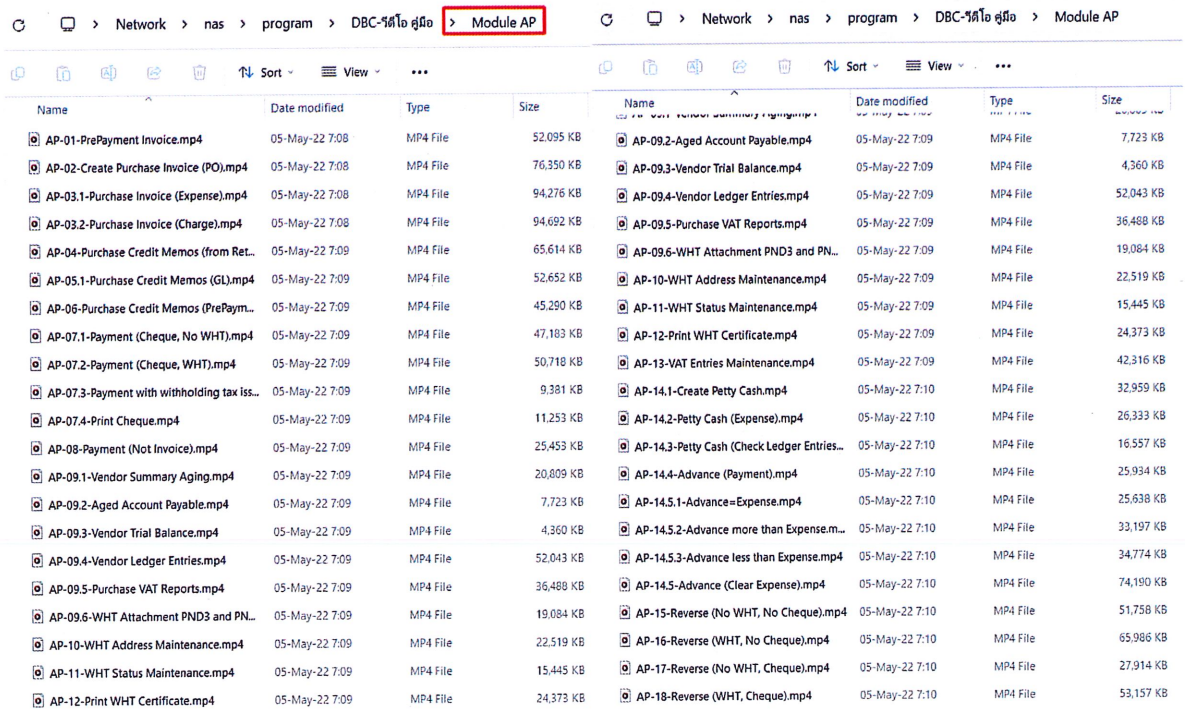
วันที่ 1/02/67

คู่มือการใช้งาน DBC

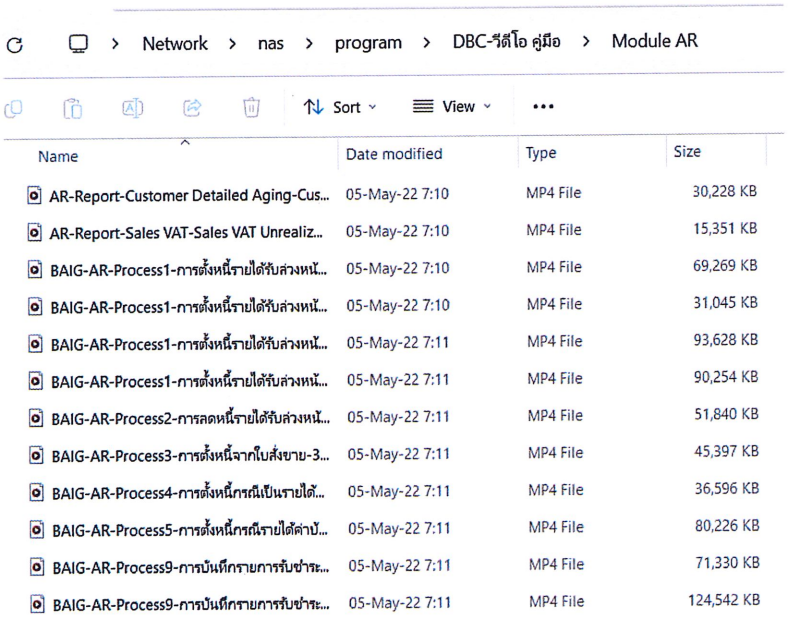
จากวีดีโอ สามารถเข้าศึกษาได้จาก วีดีโอการสอนได้ที่ \\nas\program\DBC-วีดีโอ ตาม Module ตามรูป



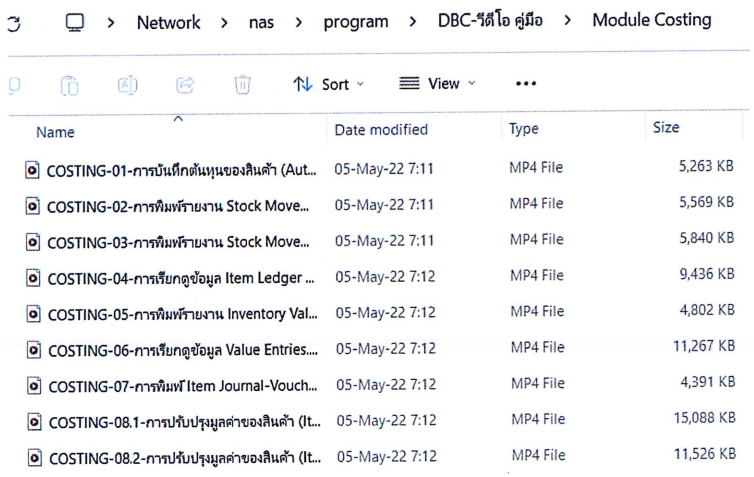
1. Module AP ประกอบไปด้วย



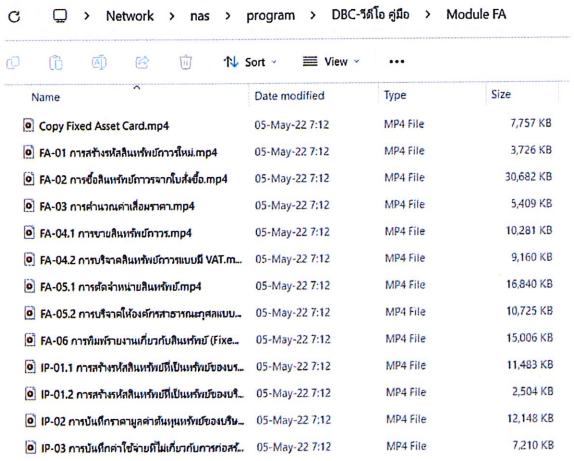
2. Module AR ประกอบไปด้วย



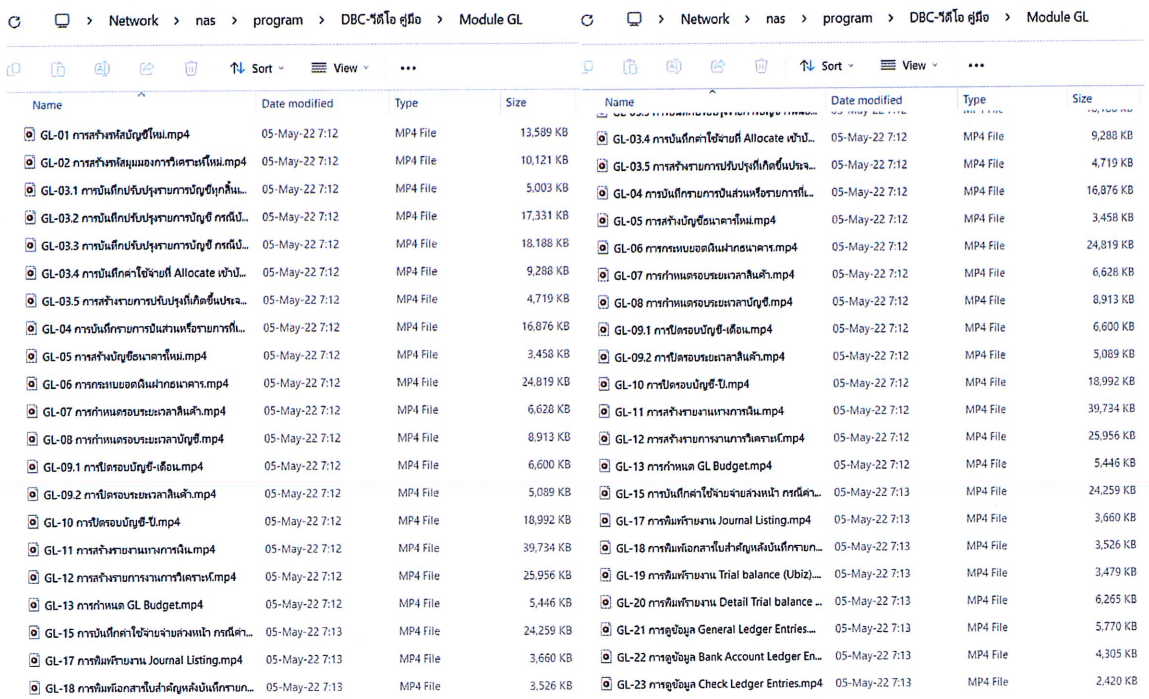
3. Module Costing ประกอบไปด้วย



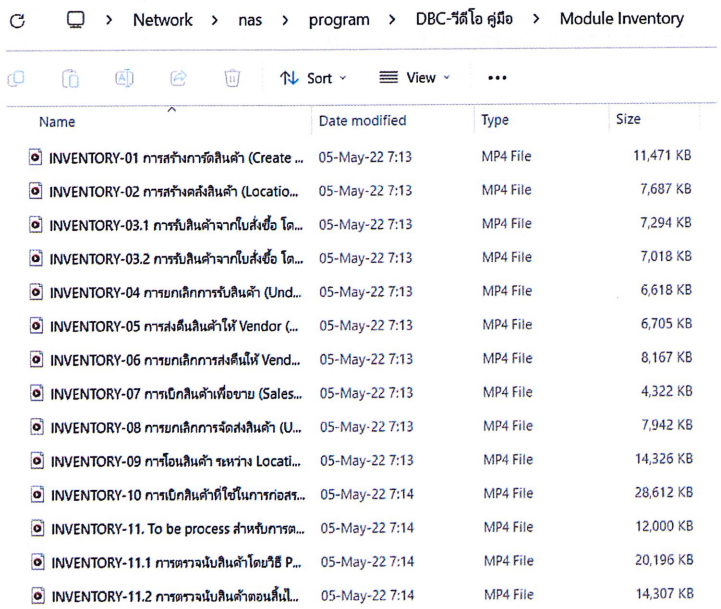
4. Module FA ประกอบไปด้วย



5. Module GL ประกอบไปด้วย



6. Module Inventory ประกอบไปด้วย

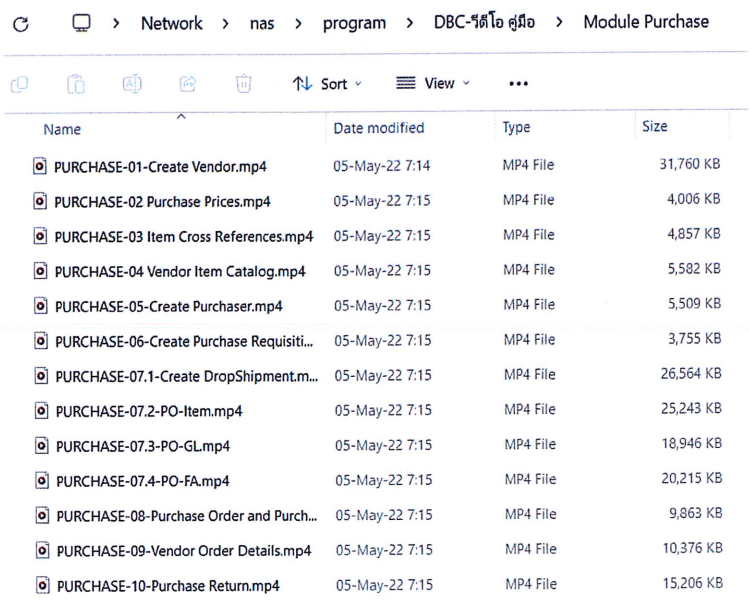


Network › nas › program › DBC-วีดีโอ คู่มือ › Module Inventory

Sort · View · ...

Name	Date modified	Type	Size
INVENTORY-01 การสร้างการ์ดสินค้า (Create ...	05-May-22 7:13	MP4 File	11,471 KB
INVENTORY-02 การสร้างคลังสินค้า (Locatio...	05-May-22 7:13	MP4 File	7,687 KB
INVENTORY-03.1 การรับสินค้าจากใบสั่งซื้อ โด...	05-May-22 7:13	MP4 File	7,294 KB
INVENTORY-03.2 การรับสินค้าจากใบสั่งซื้อ โด...	05-May-22 7:13	MP4 File	7,018 KB
INVENTORY-04 การยกเลิกการรับสินค้า (Und...	05-May-22 7:13	MP4 File	6,618 KB
INVENTORY-05 การส่งคืนสินค้าให้ Vendor (...	05-May-22 7:13	MP4 File	6,705 KB
INVENTORY-06 การยกเลิกการส่งคืนให้ Vend...	05-May-22 7:13	MP4 File	8,167 KB
INVENTORY-07 การเบิกสินค้าเพื่อขาย (Sales...	05-May-22 7:13	MP4 File	4,322 KB
INVENTORY-08 การยกเลิกการจัดส่งสินค้า (U...	05-May-22 7:13	MP4 File	7,942 KB
INVENTORY-09 การโอนสินค้า ระหว่าง Locati...	05-May-22 7:13	MP4 File	14,326 KB
INVENTORY-10 การเบิกสินค้าที่ใช้ในการก่อสร...	05-May-22 7:14	MP4 File	28,612 KB
INVENTORY-11. To be process สำหรับการต...	05-May-22 7:14	MP4 File	12,000 KB
INVENTORY-11.1 การตรวจนับสินค้าโดยวิธี P...	05-May-22 7:14	MP4 File	20,196 KB
INVENTORY-11.2 การตรวจนับสินค้าตอนสิ้นไ...	05-May-22 7:14	MP4 File	14,307 KB

7. Module Purchase ประกอบไปด้วย

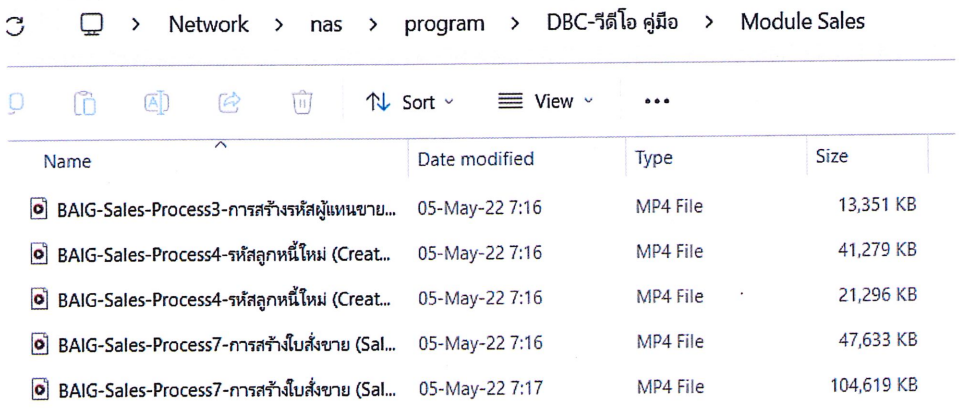


Network › nas › program › DBC-วีดีโอ คู่มือ › Module Purchase

Sort · View · ...

Name	Date modified	Type	Size
PURCHASE-01-Create Vendor.mp4	05-May-22 7:14	MP4 File	31,760 KB
PURCHASE-02 Purchase Prices.mp4	05-May-22 7:15	MP4 File	4,006 KB
PURCHASE-03 Item Cross References.mp4	05-May-22 7:15	MP4 File	4,857 KB
PURCHASE-04 Vendor Item Catalog.mp4	05-May-22 7:15	MP4 File	5,582 KB
PURCHASE-05-Create Purchaser.mp4	05-May-22 7:15	MP4 File	5,509 KB
PURCHASE-06-Create Purchase Requisiti...	05-May-22 7:15	MP4 File	3,755 KB
PURCHASE-07.1-Create DropShipment.m...	05-May-22 7:15	MP4 File	26,564 KB
PURCHASE-07.2-PO-Item.mp4	05-May-22 7:15	MP4 File	25,243 KB
PURCHASE-07.3-PO-GL.mp4	05-May-22 7:15	MP4 File	18,946 KB
PURCHASE-07.4-PO-FA.mp4	05-May-22 7:15	MP4 File	20,215 KB
PURCHASE-08-Purchase Order and Purch...	05-May-22 7:15	MP4 File	9,863 KB
PURCHASE-09-Vendor Order Details.mp4	05-May-22 7:15	MP4 File	10,376 KB
PURCHASE-10-Purchase Return.mp4	05-May-22 7:15	MP4 File	15,206 KB

8. Module Sale ประกอบไปด้วย



ประวัติการการปรับปรุงเอกสาร				
ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 กรกฎาคม 2565	ธนิศร ธนวงศ์เกษม
2	1.1	แก้ไข IP	1 กุมภาพันธ์ 2567	ชาญยุทธ วัฒนาศักดิกุล

ลงชื่อ_____

(นาย ชาญยุทธ วัฒนาศักดิกุล)

ผู้รับผิดชอบ

วันที่ 01/02/67

ผู้อนุมัติ

ลงชื่อ_____

(นางสาว ธนิศร ธนวงศ์เกษม)

ประธานเจ้าหน้าที่เทคโนโลยีสารสนเทศ

วันที่ 01/02/67

ทะเบียนโปรแกรมและระบบ

วัตถุประสงค์

1. เพื่อเป็นมาตรฐานในการใช้งานโปรแกรมและระบบในบริษัท
2. เพื่อเป็นควบคุมการใช้งานโปรแกรมและระบบให้ถูกต้องตามกฎหมาย หรือ พรบ.คอมพิวเตอร์

Software/System					
Standard			Requisition		
System	Application	Freeware	System	Application	Freeware
MS Windows	MS Office/ 365 (Excel, Word, PowerPoint, Onedrive, OneNote)	Adobe Reader	Linux	Adobe Aftereffect	Beger
Android	Zoom	I Love pdf		Adobe Photoshop	TOA
IOS	OS	Openoffice		Adobe Premier Pro	RD prep
	Kintone	Google Chrome (Sheet, Drive, Meet, Calendar)		Adobe Lightroom	Filezilla
	DBC	MS Edge		Adobe Cloud	Advanced IP scan
	EDR Sangfor	Opera		AutoCad	Putty
	SV	FireFox		Sketchup	SQL Server
	Slack	Vlc media		Dropbox	OBS
	MS Team	Ccleaner		MS Visio	MS PowerBI

Software/System					
Standard			Requisition		
Application	Freeware	System	System	Application	Freeware
	Fastinspect	Lightshot		MS Project	Github
	Rustdesk	Line		Adobe Acrobat Pro	Tiktok
		Trello		Visual Studio	Fastimageresizer
		Winrar		Foxit PDF	Owasp Zap
		MirrorOp		Dev express	Media Encoder
		Anydesk		Server express	Prtg monitoring
		Tight VNC		Osquery	Pdf Exchang Viewer
		UltraVNC Viewer		UiPath	Tiktok live studio
				Selenium	Microsoft report Builder
				Python	xampp
				QuickTime 7	G-log
				Maxon Cinema 4D	Tableau
				Blackmagic RAW Common Components	Synology Drive
				Adobe InDesign	VM wareplayer
				Grammarly for Windows	Notepad++
				Hillstone Secure Connect	DWG Trueview
				7-zip	SketchUp Viewer

				WinSCP	HandBrake
				Postman	CapCut
				Canva	GNU IMAGE
				GIMP	Davinci Resolve 19

โปรแกรม	วัตถุประสงค์
MS Office/ 365	ใช้สำหรับพิมพ์เอกสารหรือทำสูตรคำนวณรวมถึงประชุมออนไลน์
Zoom	ใช้ประชุมออนไลน์
OS	ใช้สำหรับลงทะเบียนทรัพย์สินบ้านแต่ง ,บ้านฝาก
Kintone	ใช้สำหรับนำแบบฟอร์มที่เป็นกระดาษ ขึ้นไปเป็นไฟล์ อิเล็กทรอนิกส์ เพื่อลดการใช้กระดาษ
DBC	โปรแกรม ERP
Hunman OS	ใช้สำหรับลงเวลาเข้างาน
EDR Sangfor	เป็นโปรแกรม Anti-virus
ZOHO CRM	เป็นโปรแกรมเก็บ ข้อมูลติดต่อลูกค้า ประเมินลูกค้า
SV	เป็นโปรแกรม สำรวจบ้าน มือ 1 และ มือ 2
Slack	ใช้สำหรับสื่อสารภายในบริษัท
Anydesk	โปรแกรมแกรม Remote เข้าหน้าจอคอมพิวเตอร์
Ms team	ประชุมออนไลน์
Fastinspect	ใช้ตรวจ Defect
Rustdesk	โปรแกรมแกรม Remote เข้าหน้าจอคอมพิวเตอร์
Adobe Reader	อ่านไฟล์ PDF
I love pdf	อ่านไฟล์ PDF และแก้ไขไฟล์ PDF
Openoffice	อ่านไฟล์ ประเภท Office
Google Chrome	ใช้สำหรับเปิด เว็บไซต์

MS Edge	ใช้สำหรับเปิด เว็บไซต์
Opera	ใช้สำหรับเปิด เว็บไซต์
Firefox	ใช้สำหรับเปิด เว็บไซต์
Vlc media	ใช้เปิดไฟล์ วิดิโอ
Ccleaner	ใช้สำหรับกำจัดไฟล์ขยะภายในเครื่อง
Lightshot	ใช้สำหรับแคปหน้าจอ
Line	โปรแกรมสำหรับสื่อสาร
Trello	ใช้สำหรับทำบอร์ดต่างๆเพื่อ ดูแลจัดการงาน
WinRAR	ใช้สำหรับเปิดไฟล์ zip และสามารถทำการ รวมไฟล์ได้
Mirror op	ใช้สำหรับฉายภาพขึ้น โปรเจคเตอร์
Adobe Aftereffect	ทำกราฟฟิกภาพเคลื่อนไหว
Adobe Photoshop	ตัดต่อภาพ
Adobe Premier Pro	ตัดต่อวิดิโอ
Adobe Lightroom	แต่งภาพปรับโทนสี
Adobe Cloud	เป็นแอป สำหรับดาวโหลดโปรแกรม Adobe
AutoCad	โปรแกรมช่วยออกแบบผังบ้าน
Sketchup	ออกแบบสถาปัตยกรรม 3 มิติ
Dropbox	โปรแกรมเก็บไฟล์
MS Visio	ทำแผนผัง หรือ Flow งานต่างๆได้สะดวก
MS Project	ช่วยผู้จัดการโครงการในการพัฒนาหรือมอบหมายทรัพยากรให้กับงานนั้นๆ
Adobe Acrobat Pro	ใช้ในการแก้ไขไฟล์ PDF
Visual Studio	ใช้สำหรับอ่านโค้ด หรือเขียนโปรแกรมขึ้นมา
Foxit PDF	อ่านและแก้ไขไฟล์ PDF
Dev express	โปรแกรมสำหรับช่วยพัฒนาเว็บไซต์
Server express	ระบบจัดการฐานข้อมูล
Osquery	รายงานใน OS
Beger	ใช้ในการออกแบบสีบ้าน

TOA	ใช้ในการออกแบบสีบ้าน
RD prep	โปรแกรม ทำงานเกี่ยวกับภาษี
Filezilla	ใช้สำหรับอัปโหลด ดาวน์โหลด ไฟล์
Advanced IP scan	ตรวจสอบ IP
Putty	โปรแกรมเชื่อมต่ออุปกรณ์ช่วยโปรโตคอล SSH, Telnet
SQL Server	โปรแกรมจัดการ ฐานข้อมูล
OBS	โปรแกรม อัดวิดิโอหน้าจอ
MS PowerBI	ช่วยวิเคราะห์ข้อมูล
Github	เว็บไซต์ที่ให้บริการ Git
Tiktok	ช่วยในการศึกษา รวมไปถึงการลง Content
Fastimageresizer	ช่วยในการลดขนาดรูปภาพลง
Owasp Zap	โปรแกรมที่จะช่วยหาช่องโหว่ของระบบ
Media Encoder	ช่วยให้เข้าทำงานระหว่าง Premiere pro กับ After Effects ดีขึ้น
Prtg monitoring	ช่วยในการตรวจสอบดูแลระบบเครือข่าย
Pdf Exchang Viewer	ช่วยอ่านไฟล์ pdf ที่มีเนื้อหาเกี่ยวกับ พื้นที่บ้านได้ดีขึ้น
Tiktok live studio	ช่วยในการ Live steam ผ่าน tiktok
Microsoft Report Builder	โปรแกรมสำหรับสร้างรายงาน
Xampp	โปรแกรมจำลองให้เครื่องตัวเองเป็น host
G-log	ไว้อ่าน log
Tableau	ช่วยในการจัดการข้อมูลภายในองกรค์
Synology Drive	ช่วยในการทำงานผ่าน Nas เร็วขึ้น
VM wareplayer	โปรแกรมในการจำลอง ระบบปฏิบัติขึ้นมาภายในเครื่องตัวเอง
Notepad++	ช่วยในการอ่านโค้ด และเขียนโค้ดขึ้นมา
DWG Trueview	ช่วยในการอ่านไฟล์ Auto cad
SketchUp Viewer	ช่วยในการอ่านไฟล์ Sketch up
Handbrake	ช่วยลดขนาดไฟล์ วีดีโอ ทำสื่อการเรียนการสอน และ Upload ขึ้นระบบ LMS
CapCut	ใช้ในการตัดต่อวีดีโอ

Tight VNC	โปรแกรม Remote เข้าควบคุม computer เพื่อ support user
GNU IMMAGE	เพื่อใช้ตกแต่งรูปภาพ
Davinci Resolve 19	เพื่อใช้ในการทำสี VDO ให้ดูน่าสนใจมากขึ้น
Python	โปรแกรมสำหรับ Developer
UiPath	โปรแกรมสำหรับสร้างการทำงานอัตโนมัติ
7-zip	บีบอัดไฟล์
QuickTime 7	ช่วยเล่นวิดิโอในระบบ IOS
Maxon Cinema 4D	ใช้ทำวัตถุ 4D หรือ 3D
Blackmagic RAW Common Components	ใช้เปิดรูปภาพไฟล์ Raw
Adobe InDesign	สร้างรูปภาพ เวกเตอร์
Grammarly for Windows	ใช้สำหรับในการจัดการ Gramma
Hillstone Secure Connect	ใช้สำหรับ VPN
WinSCP	ใช้สำหรับ โอนถ่ายข้อมูล Ftp Client
Postman	ใช้สำหรับ Test การยิง API
Canva	ใช้สำหรับการตกแต่งการ์ดหรือประกาศ
GIMP	ใช้สำหรับตกแต่งภาพ

ประวัติการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 สิงหาคม 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา
2	1.1	ปรับปรุงเพิ่มโปรแกรม MirrorOp	1 กันยายน 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา
3	1.2	ปรับปรุงเพิ่มโปรแกรม Tableau, Synology Drive	1 ธันวาคม 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา
4	1.3	ปรับปรุงเพิ่มโปรแกรม Rustdesk, Owasp Zap, Media Encoder, Prtg monitoring, Pdf Exchang	1 มีนาคม 2566	วรวุฒิ เทพหัสดิน ณ อยุธยา

		Viewer, Tiktok live Studio, Microsoft report Builder, Xampp, G-log		
5	1.4	ปรับปรุงเพิ่มโปรแกรม DWG Trueview, Vmwareplayer, Notepad++	30 มีนาคม 2566	วรวุฒิ เทพหัสดิน ณ อยุธยา
6	2.0	ปรับปรุงเพิ่มโปรแกรม Sketchup Viewer, และเพิ่มวัตถุประสงค์ของทุกโปรแกรม	26 เมษายน 2566	วรวุฒิ เทพหัสดิน ณ อยุธยา
7	2.1	ปรับปรุงเพิ่มโปรแกรม HandBrake	17 กรกฎาคม 2566	วรวุฒิ เทพหัสดิน ณ อยุธยา
8	2.2	ปรับปรุงเพิ่มโปรแกรม CapCut	29 มีนาคม 2567	ชาญยุทธ วัฒนาศักดิกุล
9	2.3	ปรับปรุงเพิ่มโปรแกรม Tight VNC , GNU IMAGE , Davinci Resolve 19	08 กรกฎาคม 2567	ชาญยุทธ วัฒนาศักดิกุล
10	2.4	ปรับปรุงเพิ่มโปรแกรม Sangfor EDR, UiPath, Python, QuickTime 7, Maxon Cinema 4D, Blackmagic RAW Common Components, Adobe InDesign, Grammarly for Windows, Hillstone Secure Connect, WinSCP, Postman, Canva, GIMP	11 พฤศจิกายน 2567	ชาญยุทธ วัฒนาศักดิกุล

ลงชื่อ_____

(นาย ชาญยุทธ วัฒนาศักดิกุล)

ผู้รับผิดชอบ

วันที่ 11/11/24

ผู้อนุมัติ

ลงชื่อ_____

(นางสาว ธนิศร ธนวงศ์เกษม)

ประธานเจ้าหน้าที่เทคโนโลยีสารสนเทศ

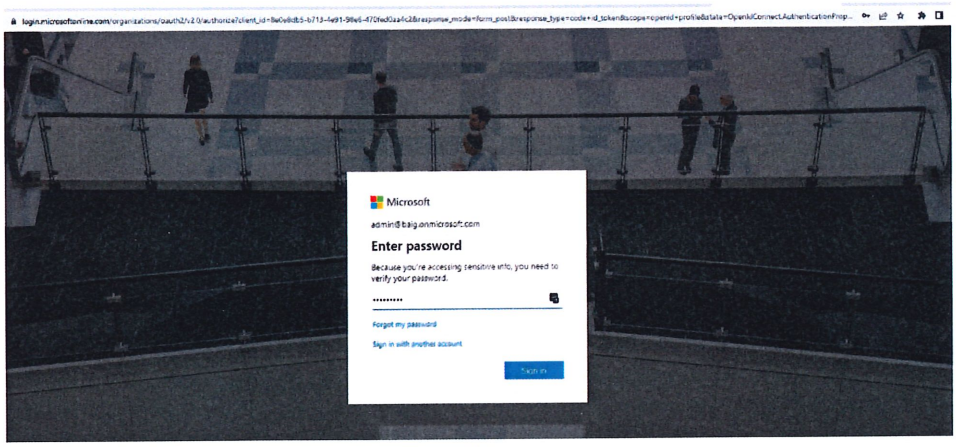
วันที่ 11/11/24

การสำรองข้อมูลระบบ DBC สำหรับแบบ Local Backup

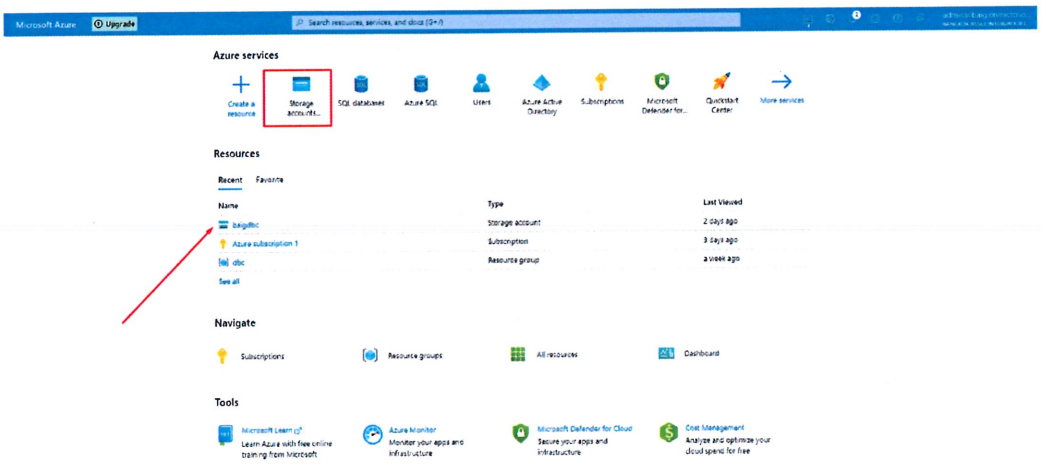
วัตถุประสงค์ เพื่อสำรองข้อมูลไว้ในกรณีฉุกเฉิน

ขั้นตอนการการสำรองข้อมูลระบบ DBC ไว้ที่ Local System

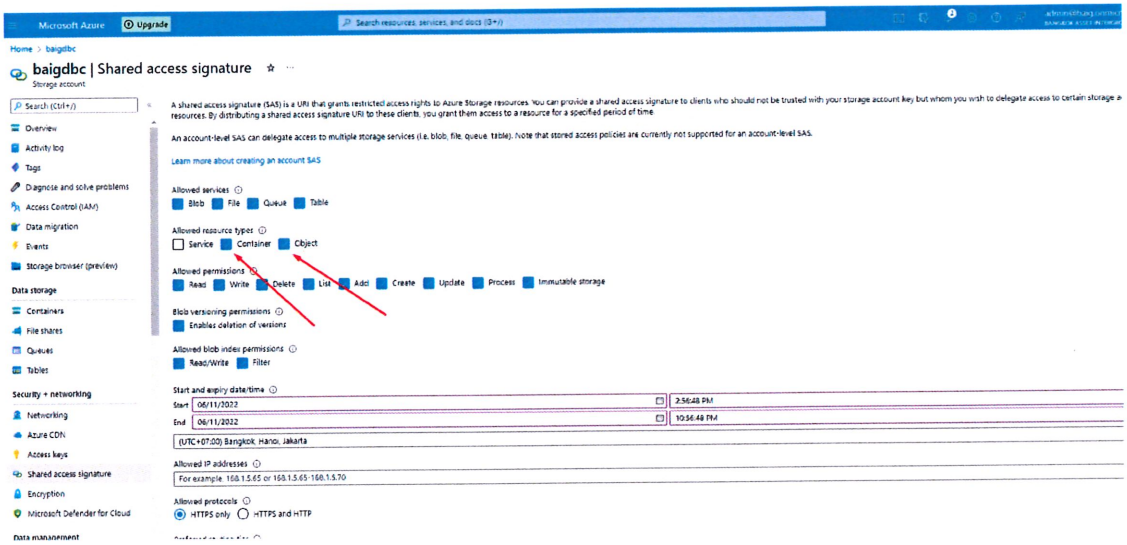
1. ให้เข้าหน้า Azure Portal คลิกที่ https://portal.azure.com/#home ด้วย User และ Password เดียวกับระบบ DBC



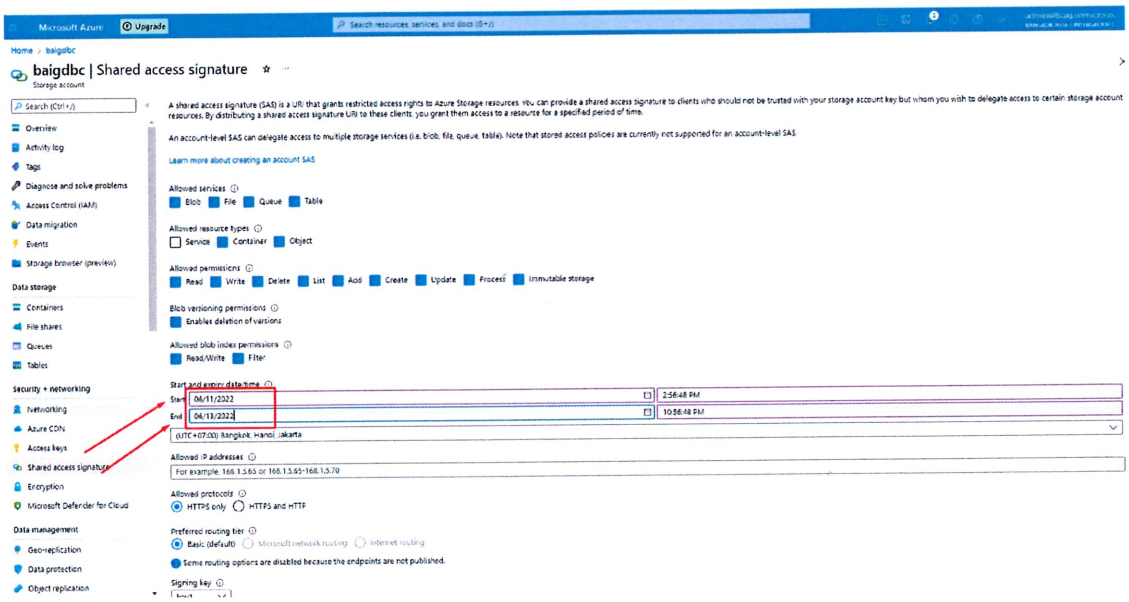
2. ให้สร้าง Storage Account เพื่อเก็บ DB ที่ export จาก DBC มาเก็บไว้ที่ baigdbc (สร้างไว้แล้ว)



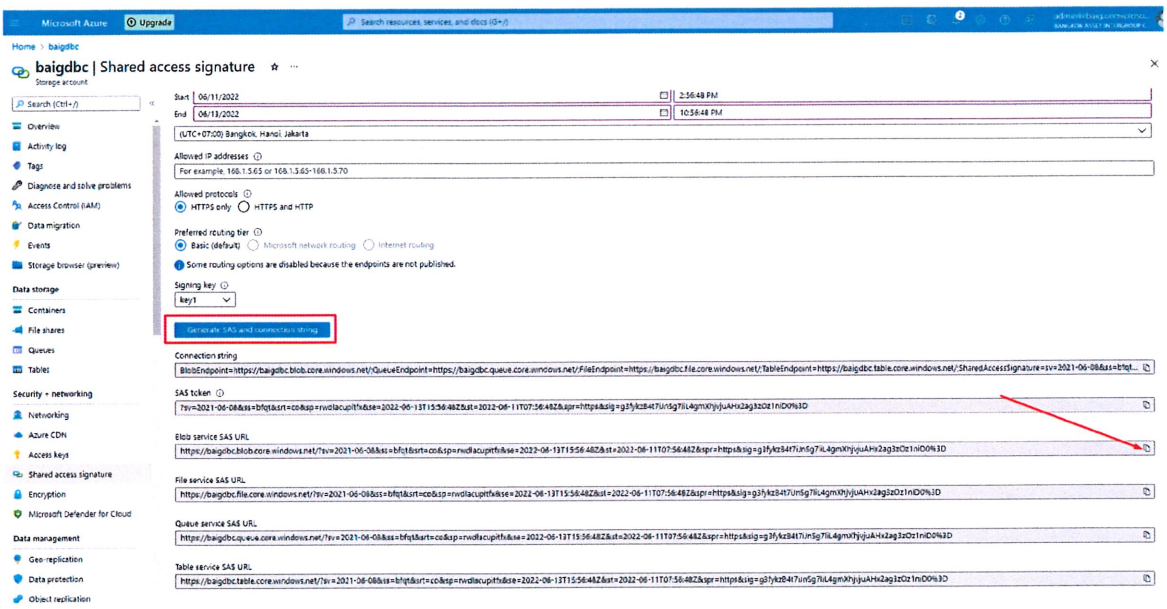
3. ทำการ Share Folder โดยเลือกที่ Container และ Object



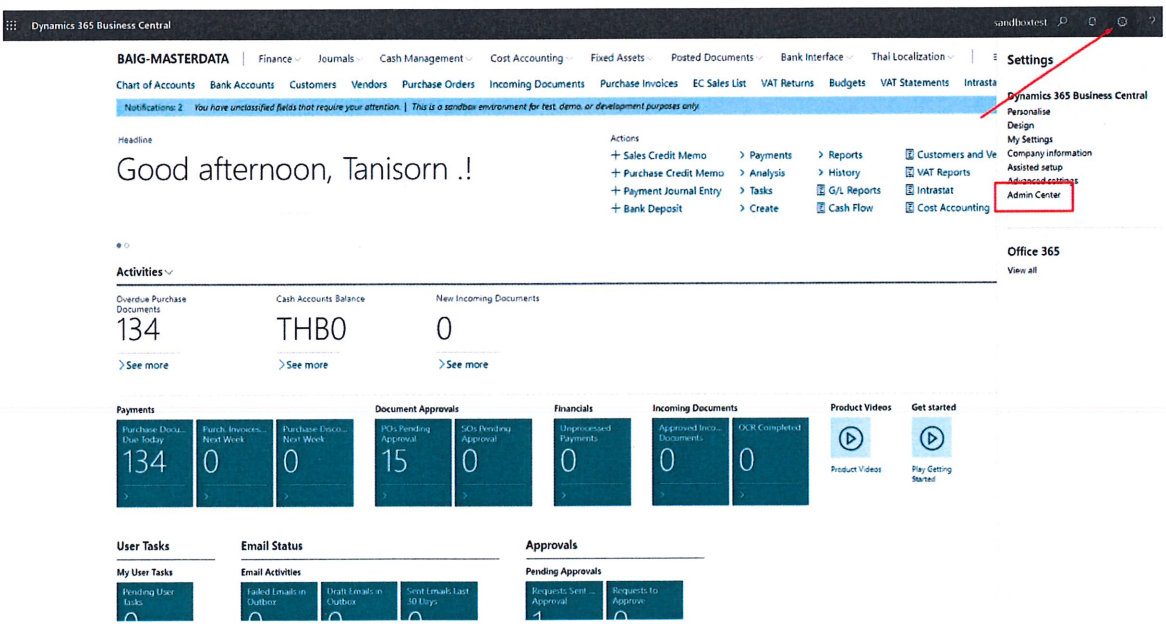
4. เลือกช่วงเวลาของการ Share โดยห้ามให้มีอายุการทำงานต่ำกว่า 24 ชม. มิฉะนั้นจะไม่สามารถ Export มาเก็บไว้ได้



5. Generate SAS และ Copy Blob service SAS URL



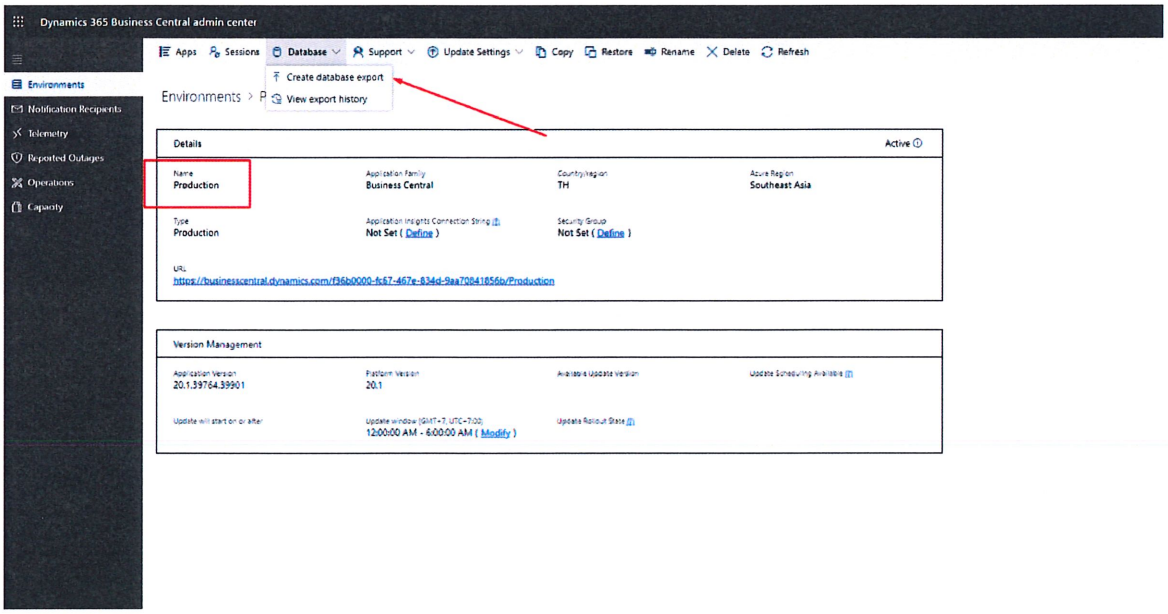
6. เปิดหน้า Admin Center บน DBC



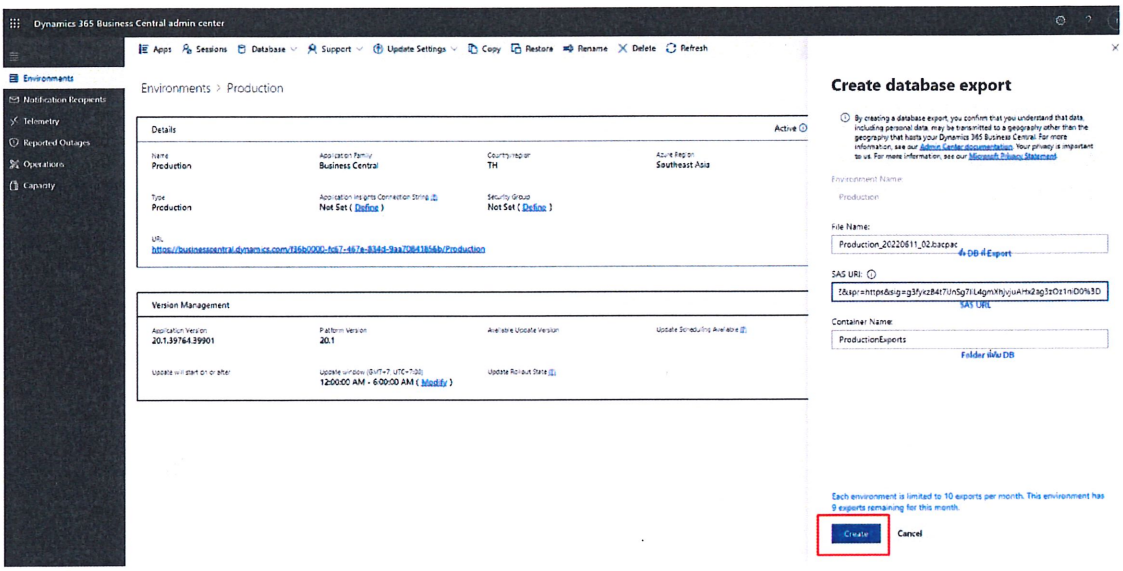
7. เลือก DB ที่จะ Backup



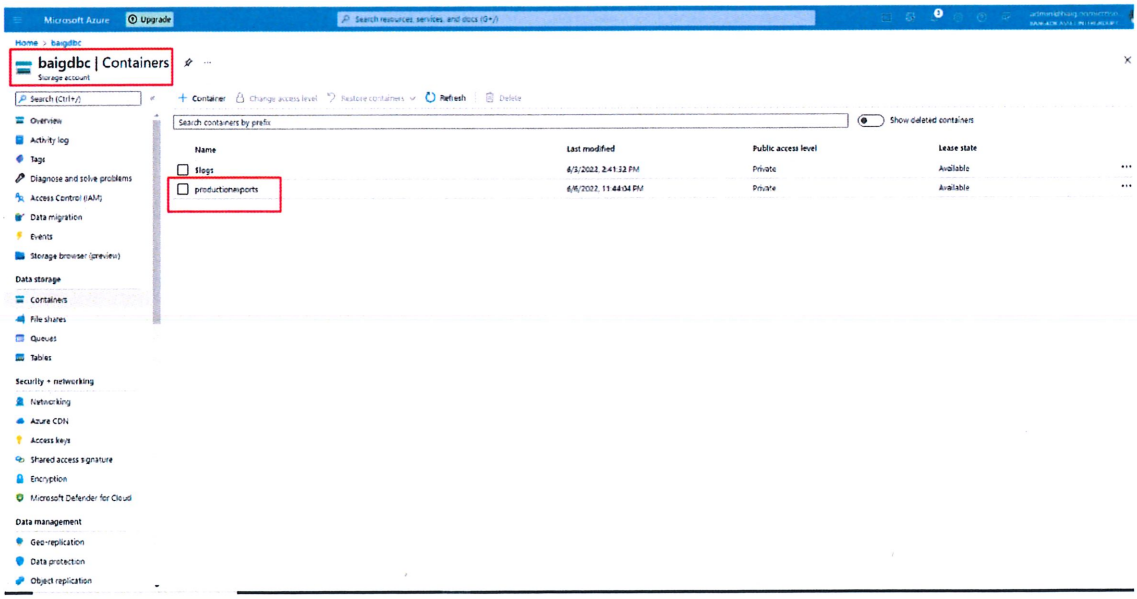
8. หลังจากเลือก DB แล้วให้ไปที่เมนู Database และเลือก Create Database Export

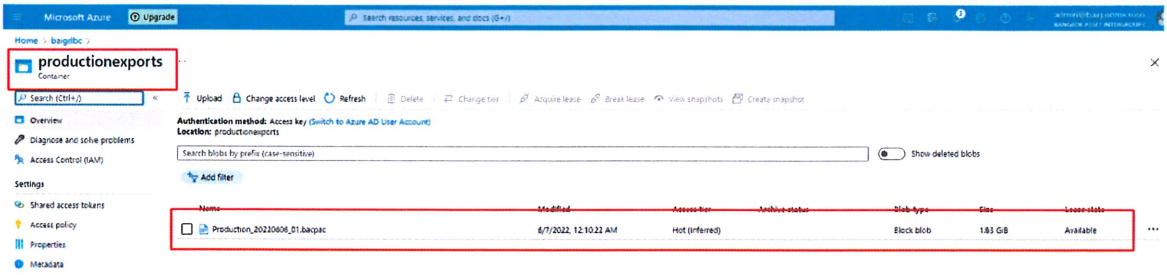


9. ตั้งชื่อ DB ที่จะ Export ใส่ SAS URL ที่ Copy มาจาก Azure Storage (ตามข้อที่ 5) ตั้งชื่อ Folder ของ DB ที่ Export ตามลำดับ และกด Create

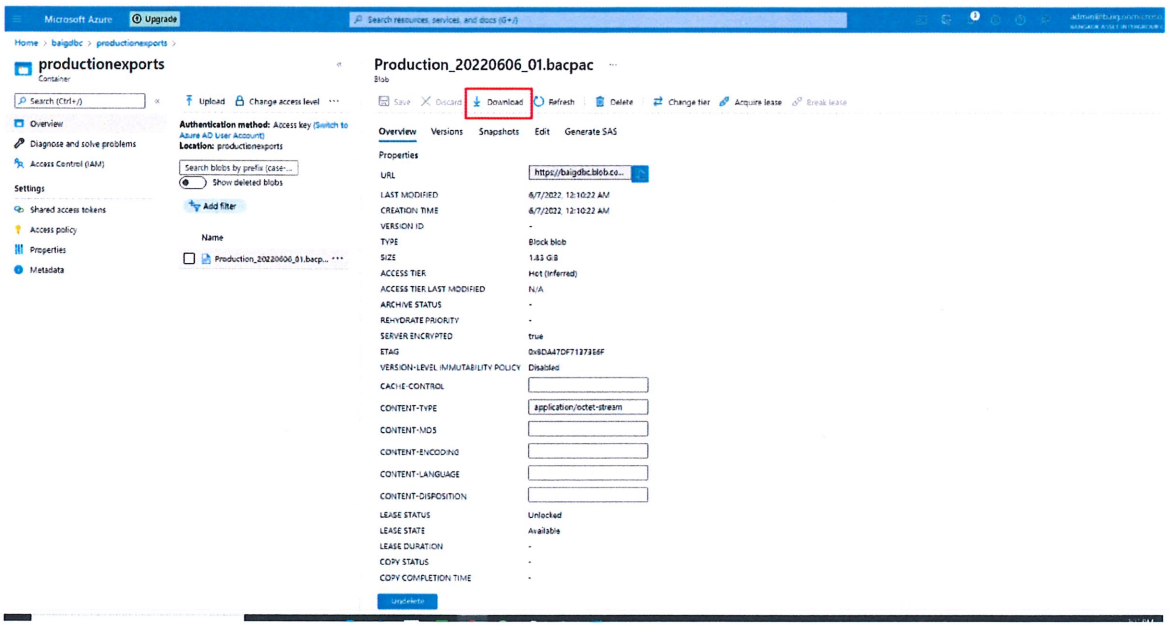


10. รอจนระบบ Create เสร็จเรียบร้อย (อาจจะใช้เวลา 2-3 ชม. แนะนำให้ทำช่วงเวลาที่ไม่มี User ใช้งาน) Folder จะปรากฏบน Azure Storage





11. ไปที่ Download เพื่อโหลดลงเครื่องของทางบริษัทได้เลย



ประวัติการการปรับปรุงเอกสาร				
ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 กันยายน 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา

ผู้อนุมัติ

ลงชื่อ วรวุฒิ เทพหัสดิน ณ

(วรวุฒิ เทพหัสดิน ณ อยุธยา)

ผู้รับผิดชอบ

วันที่ 1 ก.ย. 65

ลงชื่อ

(

)

ผู้บริหารฝ่ายคอมพิวเตอร์

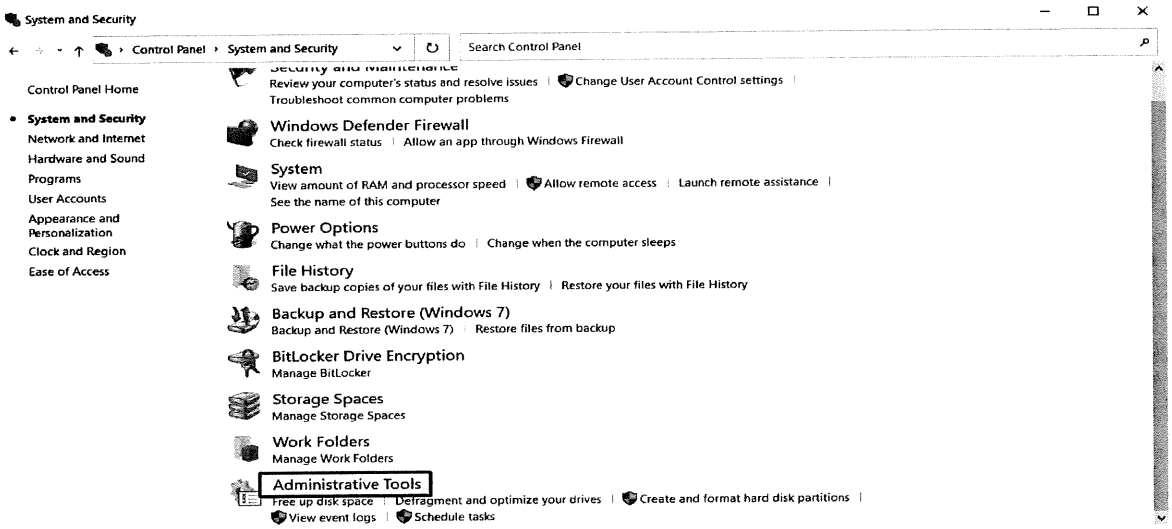
วันที่ 1 ก.ย. 65

วัตถุประสงค์ เพื่อเป็นไปตามมาตรการติดตั้งระบบ IIS

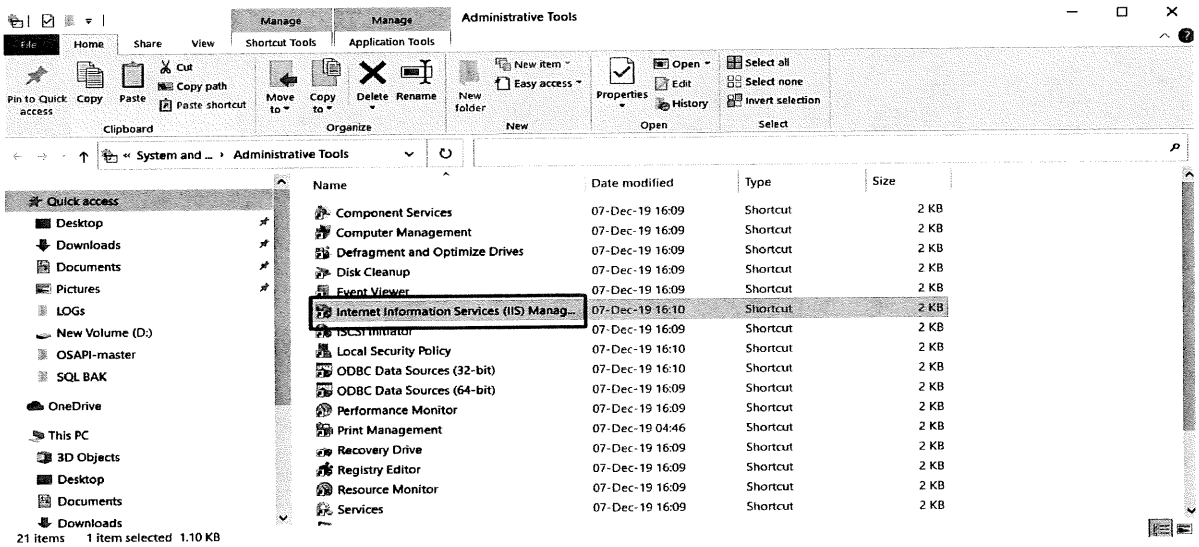
ขั้นตอนการติดตั้ง IIS

link : http://logandbak:8042/Account/Login

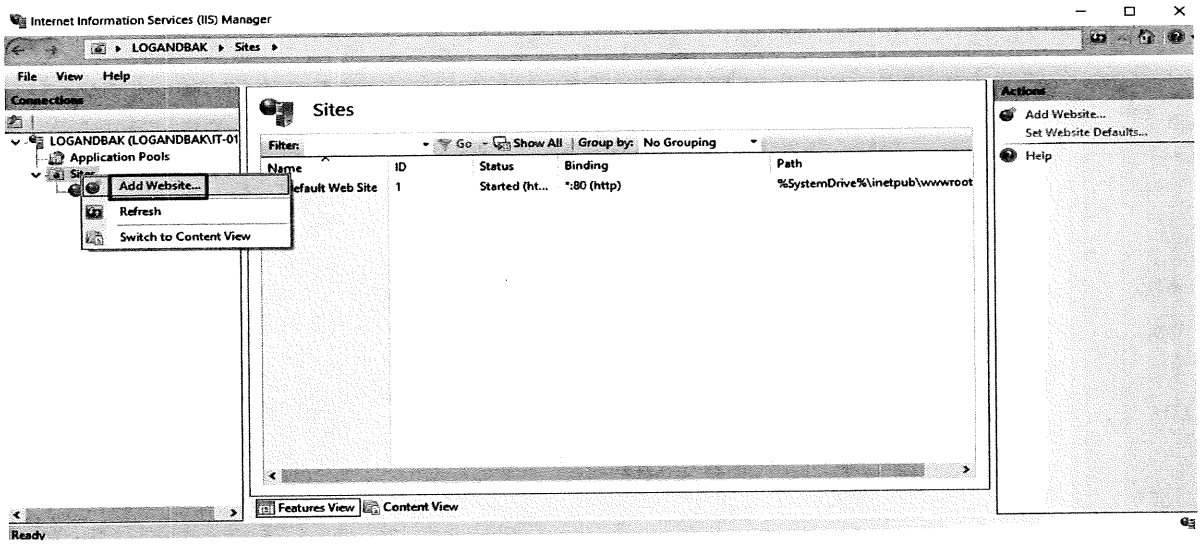
1. ไปที่ Control Panel => System and Security เลือกที่ Administrative Tools



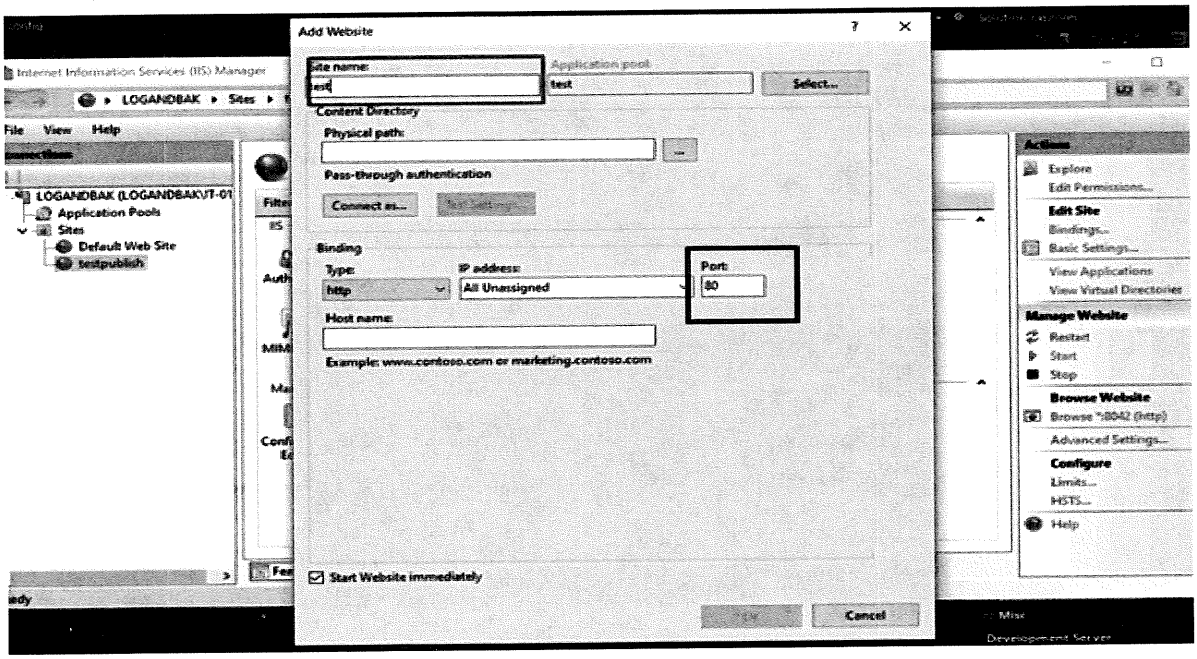
2. คลิกไปที่ Internet Information Services(IIS) Manager



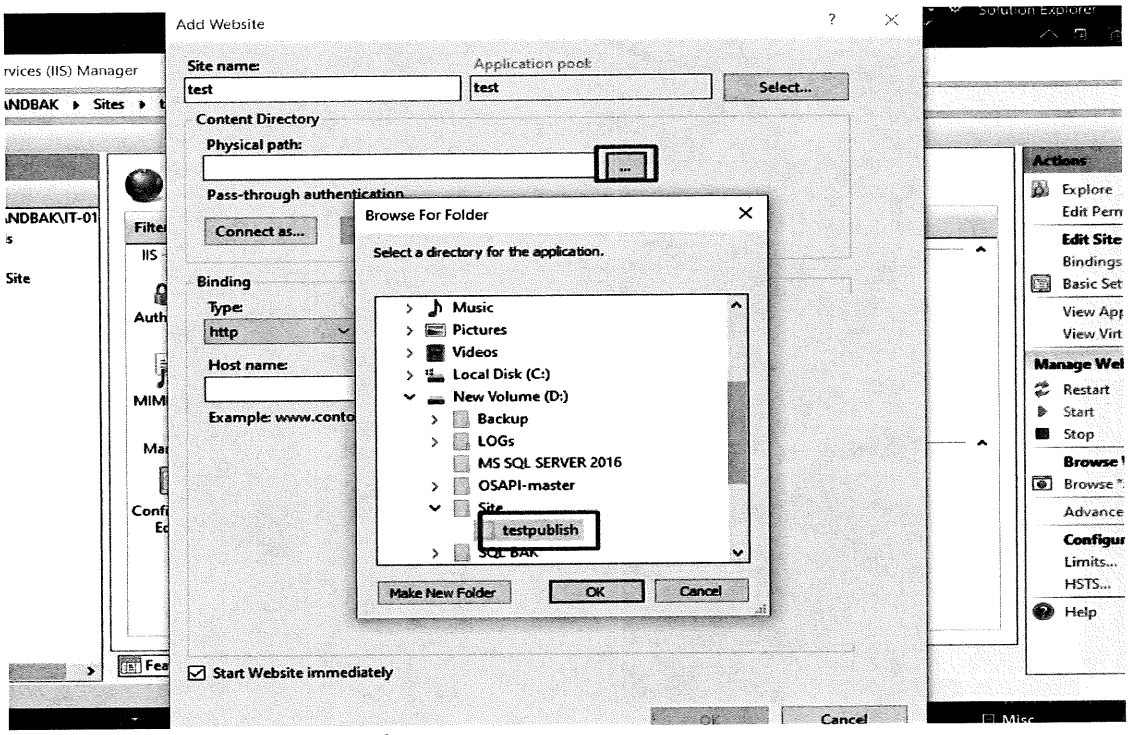
3. คลิกขวาที่ Site แล้วเลือก Add Website



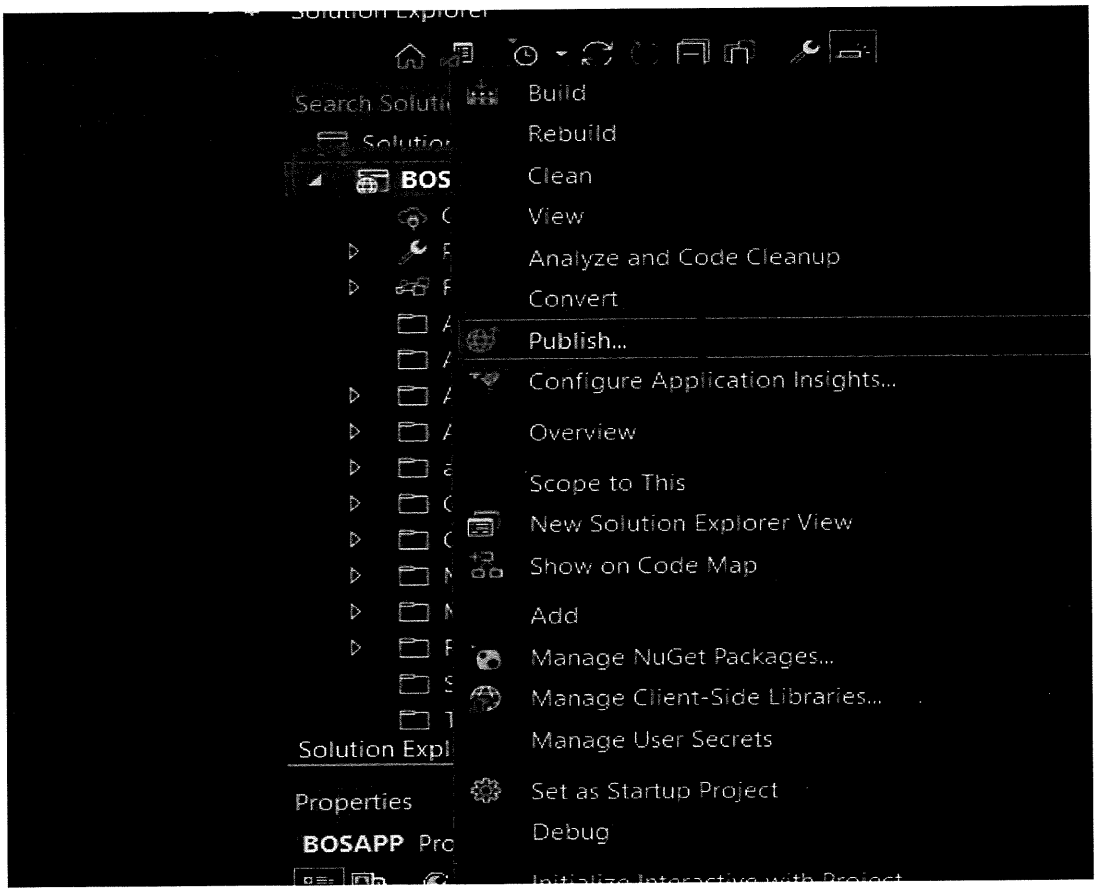
4. ระบุ Site name ระบุ Port



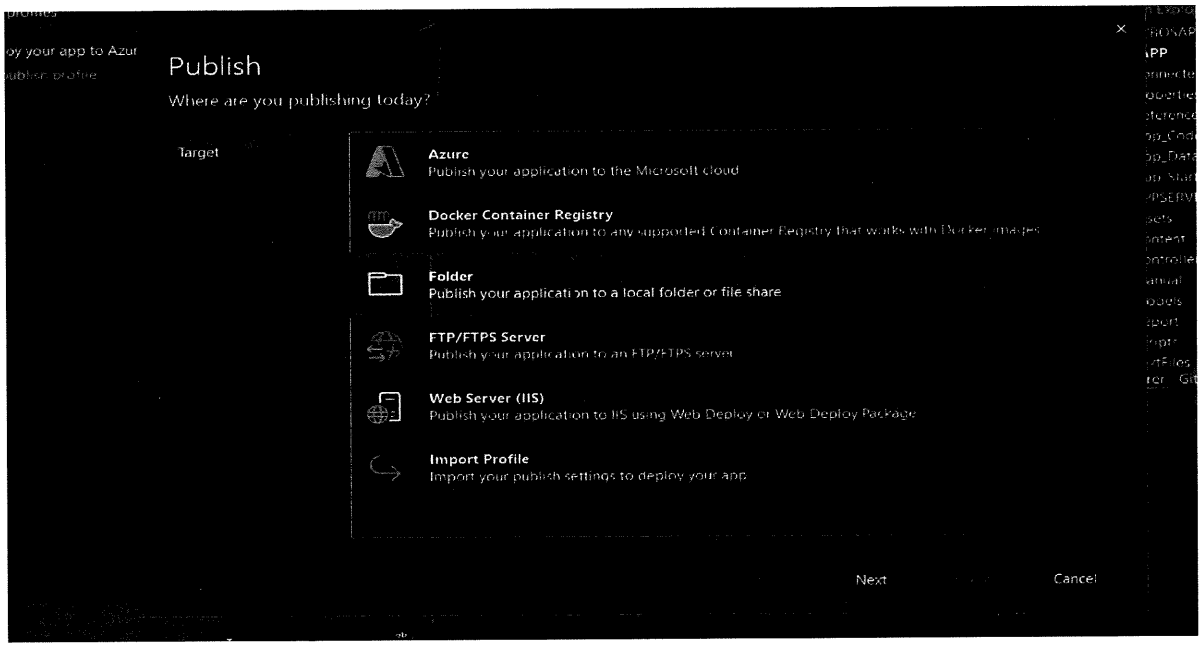
5. เลือก path ของ app



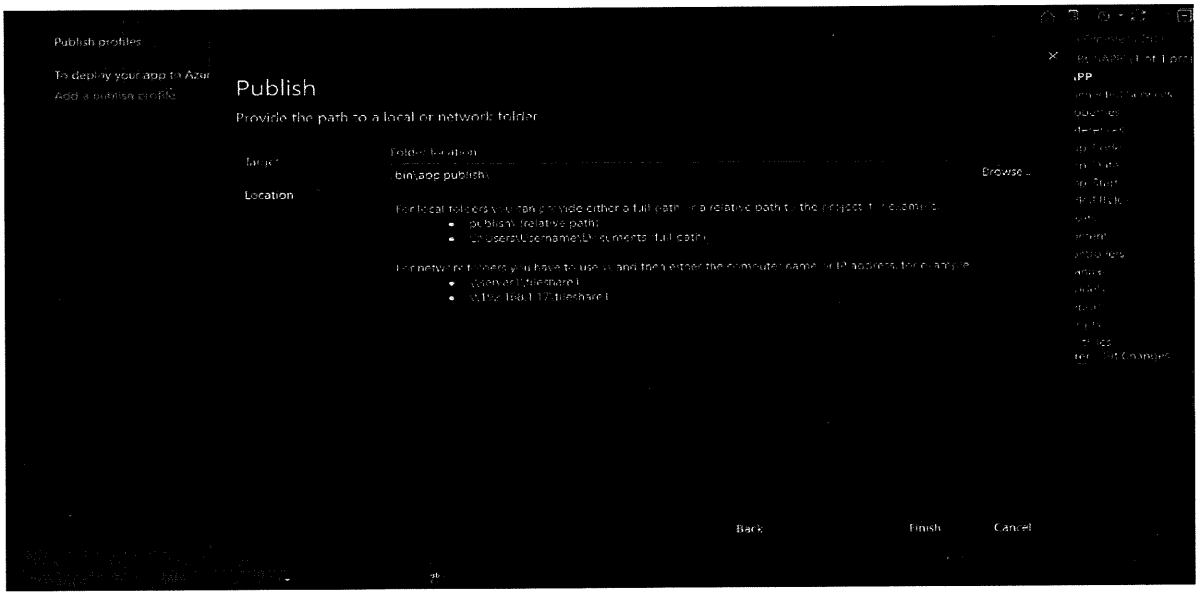
6. ไปที่โปรเจคโปรแกรม คลิกขวาที่โปรเจค เลือก Publish…



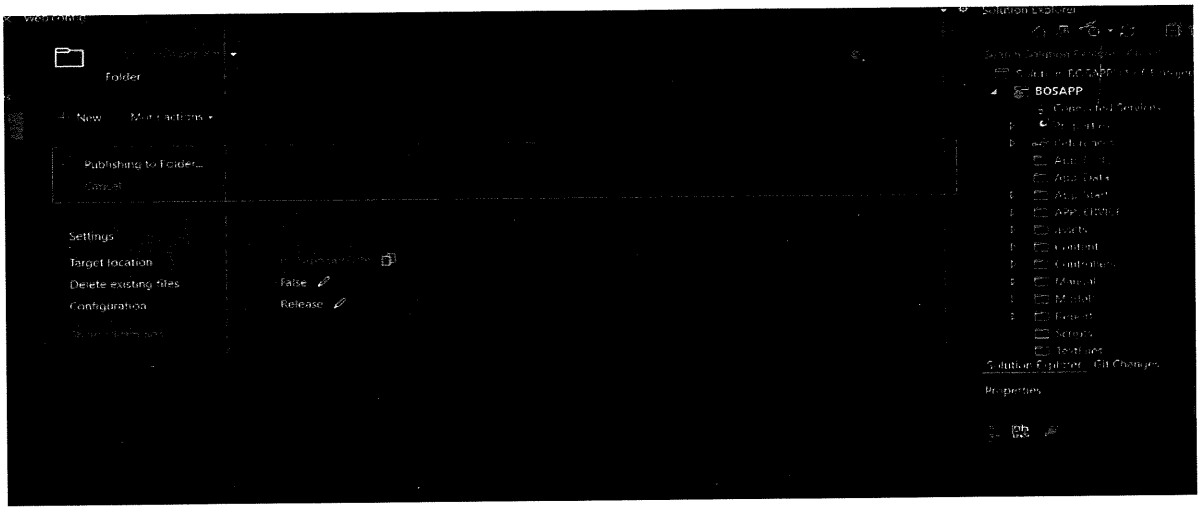
7. จากนั้นเลือก Folder กด Next



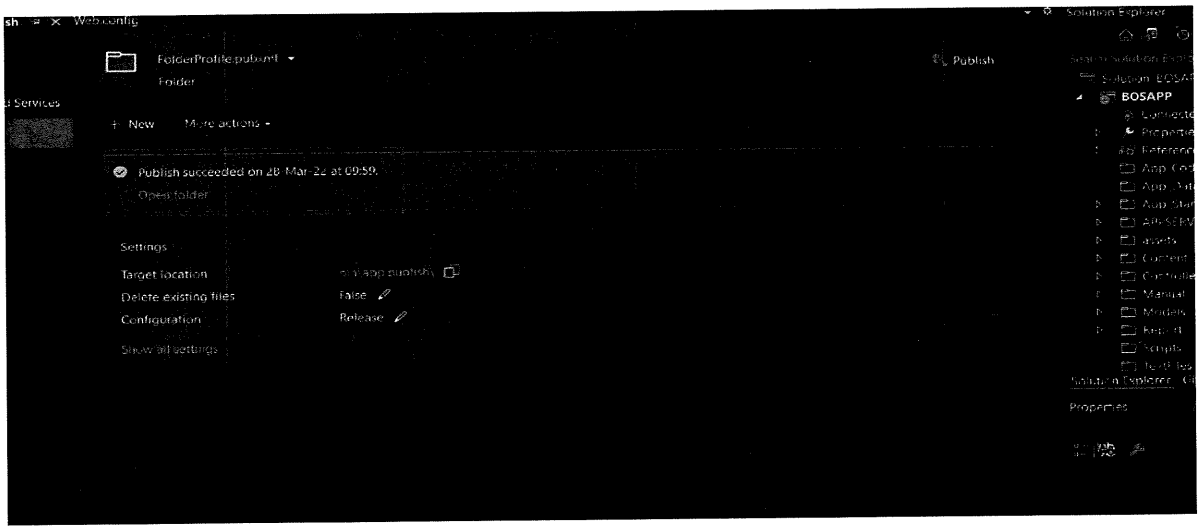
8. กด Finish



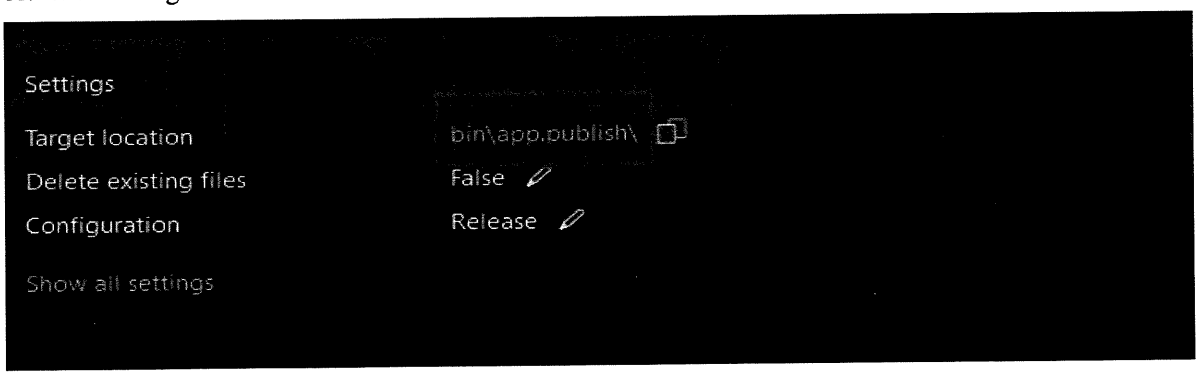
9. กด Publish



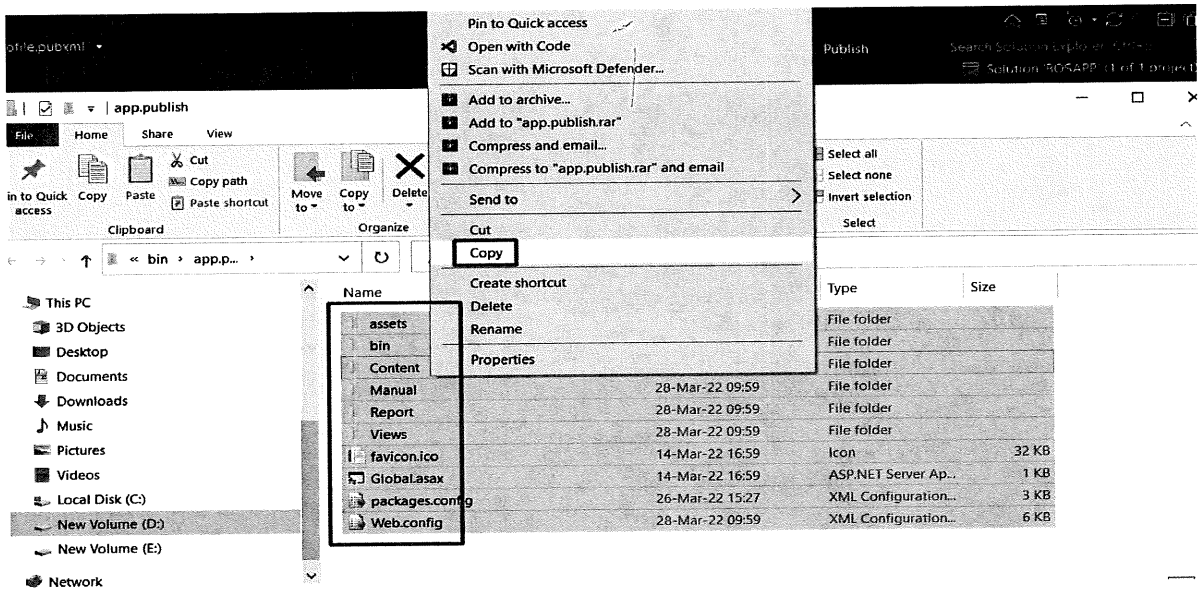
10. สำเร็จ



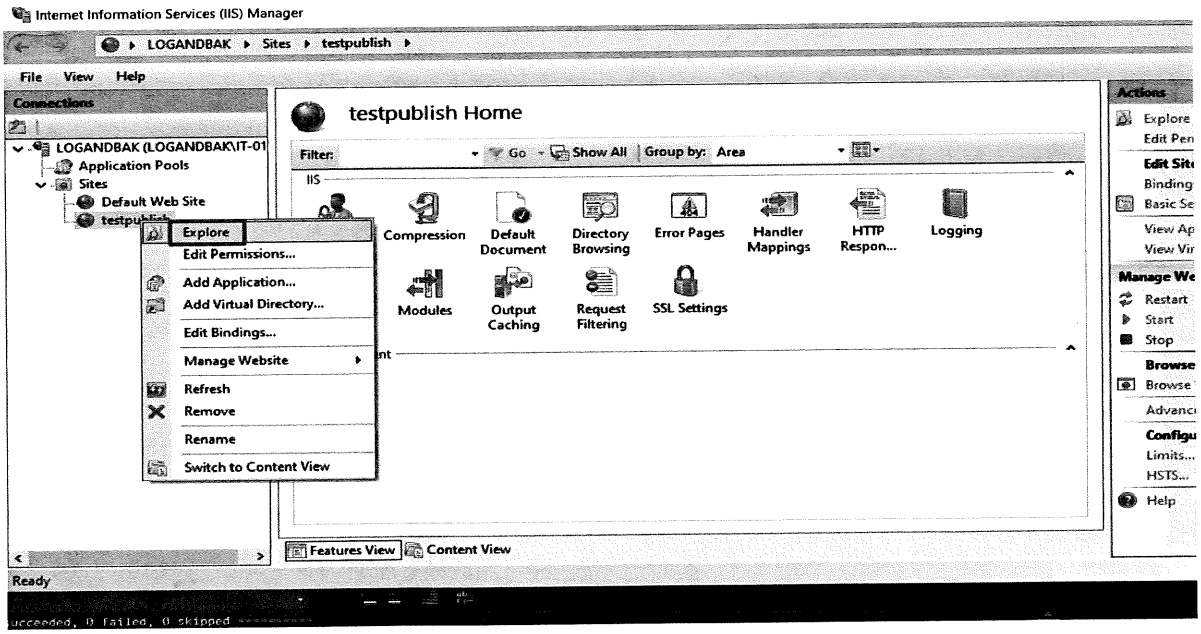
11. คลิกที่ Target location



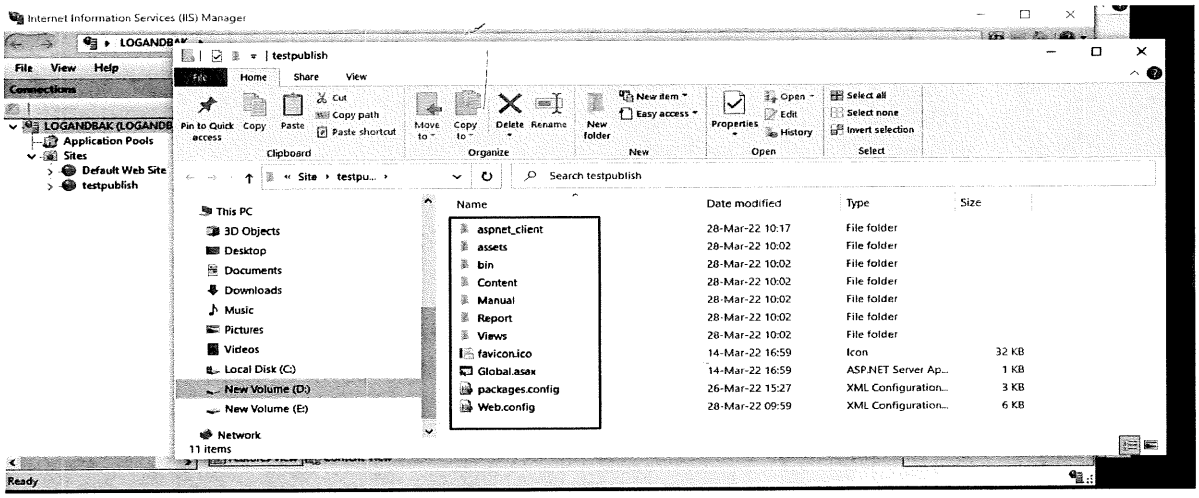
12. ก๊อปปี้ไฟล์ทั้งหมด



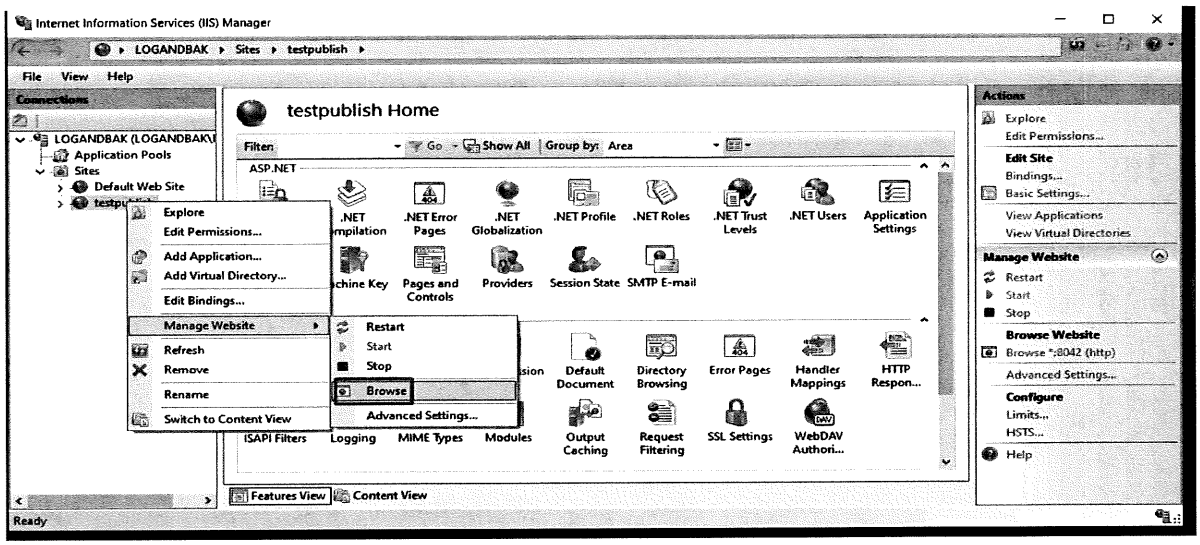
13. จากนั้นเปิดไปที่ Internet Information Services(IIS) Manager คลิกขวาที่ชื่อ Web Site ที่ทำไว้ เลือก Explore



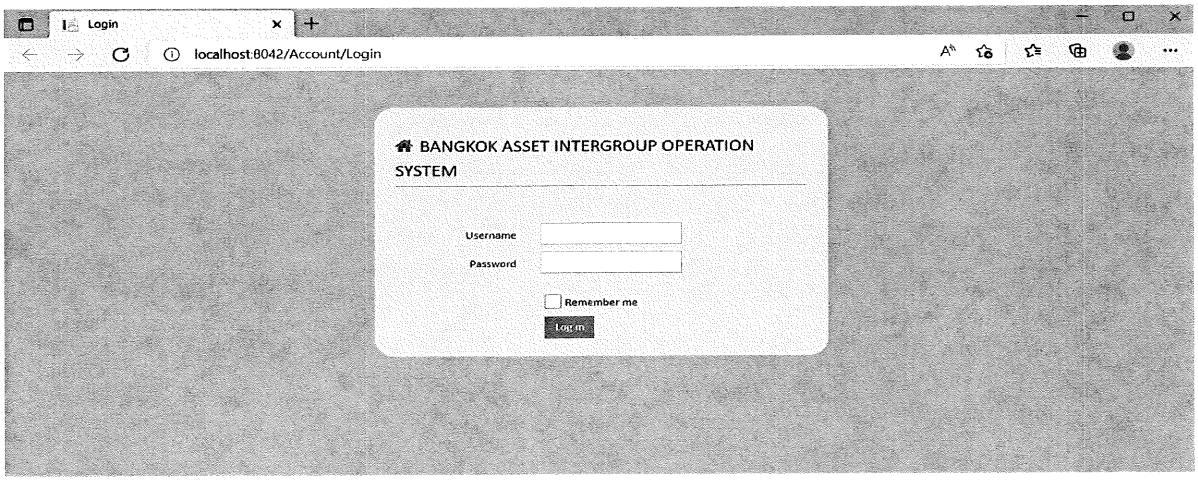
14. วางไฟล์ที่ก๊อปปี้มาจากการ Publish ลงไป



15. คลิกขวาที่ Site => Manage Website => Browse



16. แสดงผล



ประวัติการการปรับปรุงเอกสาร				
ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 กันยายน 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา

ผู้อนุมัติ

ลงชื่อ ธนัศร ธนวงศ์เกษม

(ธนัศร ธนวงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 1-09-2565

ลงชื่อ วรวุฒิ เทพหัสดิน ณ อยุธยา

(วรวุฒิ เทพหัสดิน ณ อยุธยา)

ผู้รับผิดชอบ

วันที่ 1 ก.ย 65

การแจ้งซ่อมอุปกรณ์คอมพิวเตอร์ประเภทไม่ใช่ทรัพย์สิน

1. ผู้ใช้งาน (User) จะทำการแจ้งซ่อมผ่านระบบ “สอบถาม-ปรึกษา-แจ้งปัญหา-IT” โดยระบุประเภทอุปกรณ์ที่จะซ่อม รายละเอียดปัญหาที่เกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ พร้อมแนบรูปภาพประกอบ
2. นำส่งอุปกรณ์ดังกล่าวให้กับเจ้าหน้าที่ IT Support
3. เจ้าหน้าที่ IT Support ตรวจสอบอุปกรณ์
4. บันทึกสถานะการซ่อมในระบบ “สอบถาม-ปรึกษา-แจ้งปัญหา-IT ”
   - 4.1. กรณีที่สามารถดำเนินการซ่อมเองได้
     - 4.1.1. ดำเนินการซ่อมอุปกรณ์คอมพิวเตอร์
     - 4.1.2. เมื่อดำเนินการซ่อมเรียบร้อยแล้ว เจ้าหน้าที่ IT Support จะบันทึกผลการซ่อม
     - 4.1.3. ปิดสถานะการแจ้งซ่อมผ่านระบบ “สอบถาม-ปรึกษา-แจ้งปัญหา-IT”
     - 4.1.4. เจ้าหน้าที่ IT Support ทำการแจ้งให้ผู้ใช้งาน (User) เข้ามารับอุปกรณ์ที่ส่งซ่อม
   - 4.2. กรณีไม่สามารถดำเนินการซ่อมเองได้
     - 4.2.1. เจ้าหน้าที่ IT Support จะทำการตรวจสอบข้อมูลการรับประกันของอุปกรณ์คอมพิวเตอร์
       - 4.2.1.1. นำ Serial Number จาก Stock อุปกรณ์คอมพิวเตอร์ ในระบบ Kintone ไปตรวจสอบการรับประกันในระบบ
         - 4.2.1.1.1. กรณีที่อยู่ในระยะเวลาการรับประกัน เจ้าหน้าที่ IT Support จะนำส่งอุปกรณ์คอมพิวเตอร์ให้กับบริษัทผู้รับประกันดำเนินการซ่อม/เคลมต่อไป
         - 4.2.1.1.2. กรณีหมดระยะเวลารับประกันแล้ว เจ้าหน้าที่ IT Support ทำการบันทึกสถานะการซ่อมเป็น “ยกเลิกการซ่อม” ผ่านระบบ แจ้งปัญหา IT (Repair) แล้วแจ้งให้ผู้ใช้งาน (User) ดำเนินการขอเบิกอุปกรณ์คอมพิวเตอร์ใหม่ผ่านระบบ Kintone (อ้างอิงขั้นตอนการปฏิบัติงานเรื่อง การขอเบิกอุปกรณ์คอมพิวเตอร์ประเภทไม่ใช่ทรัพย์สิน)
5. ระหว่างรอซ่อม/เคลมอุปกรณ์คอมพิวเตอร์
   - 5.1. เจ้าหน้าที่ IT Support จะทำการแจ้งผู้ใช้งาน (User) ให้ดำเนินการขอยืมอุปกรณ์คอมพิวเตอร์ทดแทนผ่านระบบ Kintone (อ้างอิงขั้นตอนการปฏิบัติงานเรื่องการขอยืมอุปกรณ์คอมพิวเตอร์)
6. เมื่ออุปกรณ์คอมพิวเตอร์ถูกซ่อมเรียบร้อยแล้ว เจ้าหน้าที่ IT Support ทำการบันทึกผลการซ่อมเป็น “ซ่อมสำเร็จ” เพื่อปิดสถานะการแจ้งซ่อมผ่านระบบ “สอบถาม-ปรึกษา-แจ้งปัญหา-IT”
7. แจ้งผู้ใช้งาน (User) ผ่านระบบ Slack เพื่อให้เข้ามารับอุปกรณ์ที่ส่งซ่อมกับเจ้าหน้าที่ IT Support พร้อมนำอุปกรณ์คอมพิวเตอร์ที่ยืมมาคืนให้กับเจ้าหน้าที่ IT Support แล้วทำการตรวจสอบอุปกรณ์คอมพิวเตอร์ ก่อนบันทึกวันที่คืนลงในแบบคำร้องขอยืมอุปกรณ์คอมพิวเตอร์ในระบบ Kintone

ประวัติการการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 กันยายน 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา

ผู้อนุมัติ

ลงชื่อ วรวุฒิ เทพหัสดิน ฯ

(วรวุฒิ เทพหัสดิน ณ อยุธยา)

ผู้รับผิดชอบ

วันที่ 1 ก.ย. 2565

ลงชื่อ ชนิดร ธนวงศ์เกษม

(ชนิดร ธนวงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 1 ก.ย. 2565

ขั้นตอนการขอเบิกอุปกรณ์คอมพิวเตอร์

1. ผู้ใช้งาน (User) จะขอเบิกอุปกรณ์คอมพิวเตอร์ ผ่านระบบ Kintone
2. ระบบจะแจ้งเตือนไปยังเจ้าหน้าที่ IT Support
3. เจ้าหน้าที่ IT Support จะทำการตรวจสอบอุปกรณ์คอมพิวเตอร์คงเหลือจากแบบฟอร์มเก็บสินทรัพย์ (IT) ในระบบ Kintone
4. เจ้าหน้าที่ IT Support ระบุผลการขอเบิกลงในแบบคำร้องขอเบิกอุปกรณ์คอมพิวเตอร์ก่อนนำเสนอผู้จัดการ IT ผ่านระบบ Kintone
5. เมื่อแบบคำร้องผ่านการอนุมัติแล้ว ระบบจะแจ้งเตือนไปยังผู้ร้องขอเพื่อแจ้งผลการเบิก
6. ผู้ร้องขอทำการกดยืนยันผลการเบิก เพื่อเป็นการปิดสถานะแบบคำร้อง
7. ผู้ร้องขอเข้ามารับอุปกรณ์คอมพิวเตอร์กับเจ้าหน้าที่ IT Support โดยผู้ร้องขอทำการแจ้งเบิกทรัพย์สินกับส่วนงานทรัพยากรบุคคล โดยจัดทำเอกสารการรับ-ส่งคืนทรัพย์สินของบริษัทฯ พร้อมลงนามผู้ขอเบิก และเจ้าหน้าที่ IT Support ลงนามผู้ส่งมอบ
8. ฝ่าย IT แจ้งอัปเดตทรัพย์สินในห้อง Slack เพื่อแจ้งให้ฝ่ายบัญชีและบุคคล รับทราบ

ขั้นตอนการนำส่งให้บริษัทภายนอกซ่อม

1. เมื่อผู้ใช้งาน (User) แจ้งซ่อมผ่านระบบ “Slack” โดยระบุประเภทอุปกรณ์ที่จะซ่อม รายละเอียดปัญหาที่เกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ พร้อมแนบรูปภาพประกอบ แล้วนำส่งอุปกรณ์ดังกล่าวให้กับเจ้าหน้าที่ IT Support
2. เจ้าหน้าที่ IT Support ตรวจสอบอุปกรณ์ที่ผู้ใช้งาน (User) ส่งซ่อม ก่อนบันทึกสถานะการซ่อมในระบบ “Kintone แบบฟอร์ม ขออนุมัติซ่อมอุปกรณ์คอมพิวเตอร์” แล้วจึงดำเนินการซ่อมอุปกรณ์คอมพิวเตอร์
   2.1. กรณีที่เจ้าหน้าที่ IT Support ไม่สามารถซ่อมอุปกรณ์คอมพิวเตอร์ได้เอง เจ้าหน้าที่ IT Support จะทำการตรวจสอบระยะเวลาการรับประกันของอุปกรณ์คอมพิวเตอร์
      2.1.1. กรณีอยู่ในระยะเวลาการรับประกันเจ้าหน้าที่ IT Support จะนำส่งอุปกรณ์คอมพิวเตอร์ให้กับบริษัทผู้รับประกันดำเนินการซ่อมต่อไป
      2.1.2. กรณีหมดระยะเวลารับประกันแล้ว เจ้าหน้าที่ IT Support จะนำส่งอุปกรณ์คอมพิวเตอร์ไปซ่อมกับบริษัทที่รับซ่อมคอมพิวเตอร์ จากนั้นนำใบแจ้งประเมินค่าบริการซ่อมที่ได้จากผู้ให้บริการมา

ใช้อ้างอิงการขออนุมัติซ่อมอุปกรณ์คอมพิวเตอร์ผ่านระบบ Kintone โดยนำเสนอผู้จัดการส่วนงาน IT เพื่อพิจารณาอนุมัติ (อ้างอิงตารางอำนาจอนุมัติ) เมื่อผู้จัดการส่วนงาน IT อนุมัติการซ่อมอุปกรณ์คอมพิวเตอร์แล้ว

2.1.2.1. เจ้าหน้าที่ IT Support ทำการเปิดใบขอซื้อ (PR) ในระบบ DBC โดยผู้จัดการ IT ดำเนินการอนุมัติใบขอซื้อ (PR)

2.1.2.2. เมื่อใบขอซื้อ (PR) ผ่านการอนุมัติแล้ว เจ้าหน้าที่ IT Support นำส่งใบแจ้งหนี้ให้กับเจ้าหน้าที่ธุรการจัดซื้อใช้อ้างอิงการจัดทำใบสั่งซื้อ (PO) เพื่อตั้งหนี้และทำจ่ายตามกระบวนการต่อไป

2.1.3. กรณีที่อุปกรณ์คอมพิวเตอร์ที่ส่งซ่อมไม่สามารถซ่อมได้ หรือบริษัทภายนอกที่ส่งอุปกรณ์คอมพิวเตอร์ไปซ่อมแจ้งว่าไม่สามารถซ่อมได้

2.1.3.1. เจ้าหน้าที่ IT Support ทำการบันทึกสถานะการซ่อมเป็น “ยกเลิกการซ่อม” ผ่านระบบ Kintone

2.1.3.2. ทำการแจ้งผู้ใช้งาน (User) ให้เข้ามารับอุปกรณ์คอมพิวเตอร์ที่ซ่อมรุด เพื่อใช้อ้างอิงการแจ้งคืนทรัพย์สินกับส่วนงานทรัพยากรบุคคล แล้วดำเนินการขอเบิกอุปกรณ์คอมพิวเตอร์ใหม่ผ่านระบบ Kintone *(อ้างอิงขั้นตอนการปฏิบัติงานเรื่องการขอเบิกอุปกรณ์คอมพิวเตอร์ที่เป็นทรัพย์สิน)*

2.1.3.3. เมื่อผู้ใช้งาน (User) ได้รับอุปกรณ์คอมพิวเตอร์ใหม่แล้ว จะดำเนินการแจ้งเปลี่ยนแปลงรายการทรัพย์สินผ่านห้องอัปเดตทรัพย์สินของบริษัทฯ กับเจ้าหน้าที่ส่วนงานทรัพยากรบุคคล-HR1 พร้อมกับเจ้าหน้าที่ บัญชี

3. ระหว่างรอซ่อมอุปกรณ์คอมพิวเตอร์

3.1. เจ้าหน้าที่ IT Support จะทำการแจ้งผู้ใช้งาน (User) ให้ดำเนินการขอยืมอุปกรณ์คอมพิวเตอร์ทดแทนผ่านระบบ Kintone *(อ้างอิงขั้นตอนการปฏิบัติงานเรื่องการขอยืมอุปกรณ์คอมพิวเตอร์)*

4. เมื่อผู้ให้บริการซ่อมอุปกรณ์คอมพิวเตอร์เรียบร้อยแล้ว จะนำส่งให้กับเจ้าหน้าที่ IT Support

4.1. เจ้าหน้าที่ IT Support ทำการบันทึกผลการซ่อมเป็น “ซ่อมสำเร็จ” เพื่อปิดสถานะการแจ้งซ่อมผ่านระบบ “Kintone แบบฟอร์ม ขออนุมัติซ่อมอุปกรณ์คอมพิวเตอร์”

4.2. แจ้งผู้ใช้งาน (User) ผ่านระบบ Slack เพื่อให้เข้ามารับอุปกรณ์ที่ส่งซ่อมกับเจ้าหน้าที่ IT Support และนำอุปกรณ์คอมพิวเตอร์ที่ยืมมาคืนให้กับเจ้าหน้าที่ IT Support โดยเจ้าหน้าที่ IT Support ทำการตรวจสอบอุปกรณ์คอมพิวเตอร์ ก่อนบันทึกวันที่คืนลงในแบบคำร้องขอยืมอุปกรณ์คอมพิวเตอร์ในระบบ Kintone

ประวัติการการปรับปรุงเอกสาร				
ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 กันยายน 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา
2	1.1	ลบขั้นตอนขอซ่อม Non-Asset	1 กุมภาพันธ์ 2566	วรวุฒิ เทพหัสดิน ณ อยุธยา

ผู้อนุมัติ

ลงชื่อ_____ ลงชื่อ_____

(วรวุฒิ เทพหัสดิน ณ อยุธยา) ( )

ผู้รับผิดชอบ ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 01/02/66 วันที่ 01/02/66

วัตถุประสงค์ เพื่อให้ทำงานเป็นระบบ และมีประสิทธิภาพ รวมทั้งตอบสนองความพึงพอใจของผู้ใช้งาน

ขั้นตอนการปฏิบัติการ

1. เมื่อผู้ใช้งาน (User) เกิดปัญหาในการใช้งานระบบต่างๆ ให้ทำการแจ้งส่วนงาน IT ผ่านระบบ “แจ้งปัญหา IT”
2. เจ้าหน้าที่ IT Support จะดำเนินการตรวจสอบและแก้ไขปัญหาที่เกิดขึ้น
3. เมื่อเจ้าหน้าที่ IT Support ดำเนินการแก้ปัญหาเรียบร้อยแล้ว จะทำการบันทึกผลการแก้ปัญหา และปิดสถานะการแจ้งปัญหาผ่านระบบ “แจ้งปัญหา IT”
4. กรณีที่ใช้เวลาหลายวัน จะมีเจ้าหน้าที่ IT Support ทำการติดตามสถานะการแก้ปัญหาว่าได้มีการดำเนินการเรียบร้อยแล้วหรือไม่ หากยังไม่มีการดำเนินการจะทำการแจ้งไปยังผู้รับผิดชอบ และแจ้งให้ผู้ใช้งานทราบเป็นระยะๆ จนกระทั่งทำการแก้ปัญหา และสถานะการแจ้งปัญหาผ่านระบบ “แจ้งปัญหา IT”
5. เจ้าหน้าที่ Support จะรวบรวมรายงานทั้งหมด ให้ผู้บริหารรับทราบ และนำมารายงานสรุปผลในที่ประชุมประจำเดือน
6. หากปัญหาเกิดขึ้นซ้ำๆ เป็นจำนวนมาก ให้พิจารณาเป็น “ปัญหา” ที่ต้องแก้ไขเร่งด่วน และดำเนินแก้ไขให้ลดน้อยลงในการรายงานครั้งต่อไป

ประวัติการการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 กันยายน 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา

ผู้อนุมัติ

ลงชื่อ วรวุฒิ เทพหัสดิน ฯ

(วรวุฒิ เทพหัสดิน ณ อยุธยา)

ผู้รับผิดชอบ

วันที่ 1/9/22

ลงชื่อ [illegible]

([illegible])

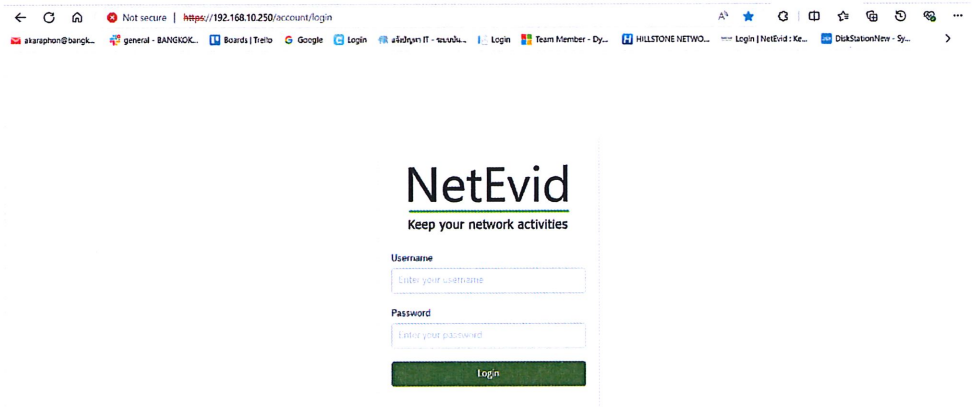
ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 1/9/22

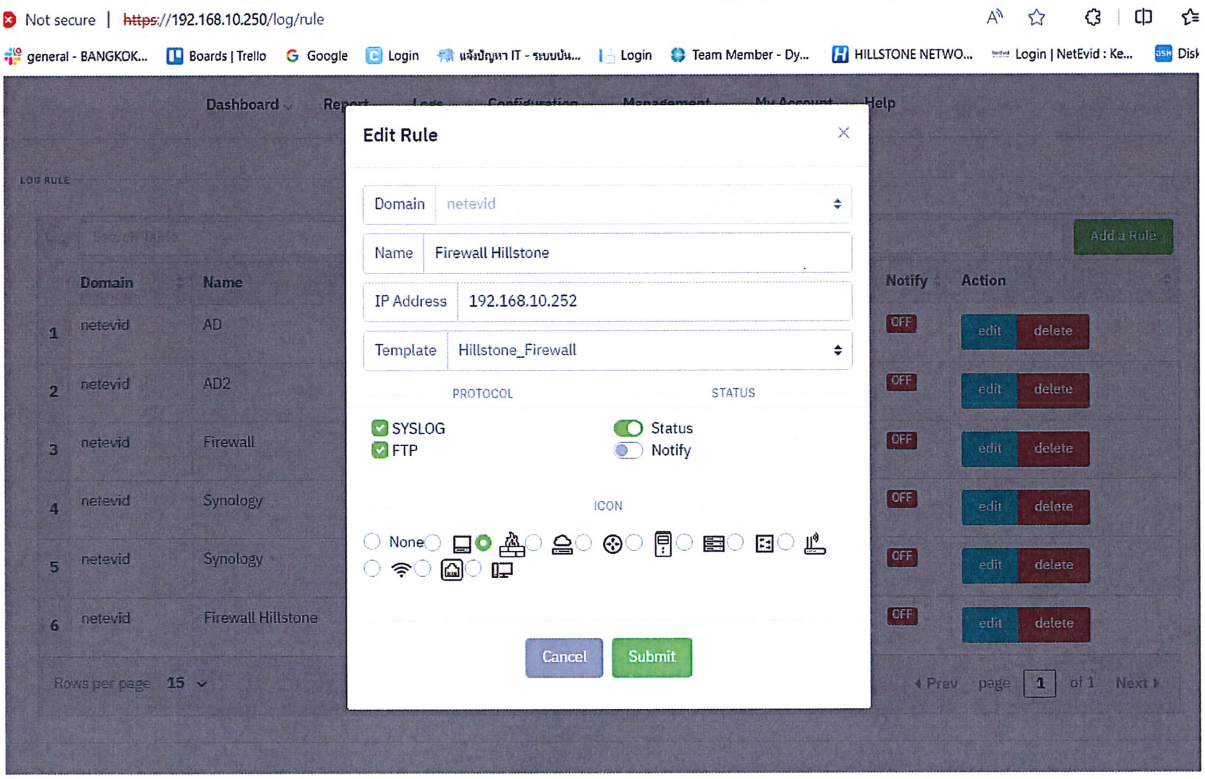
วัตถุประสงค์ เพื่อเป็นไปตามกฎหมาย และปฏิบัติตามพรบ.คอมพิวเตอร์ในการเก็บ Log

ขั้นตอนการเก็บ Log

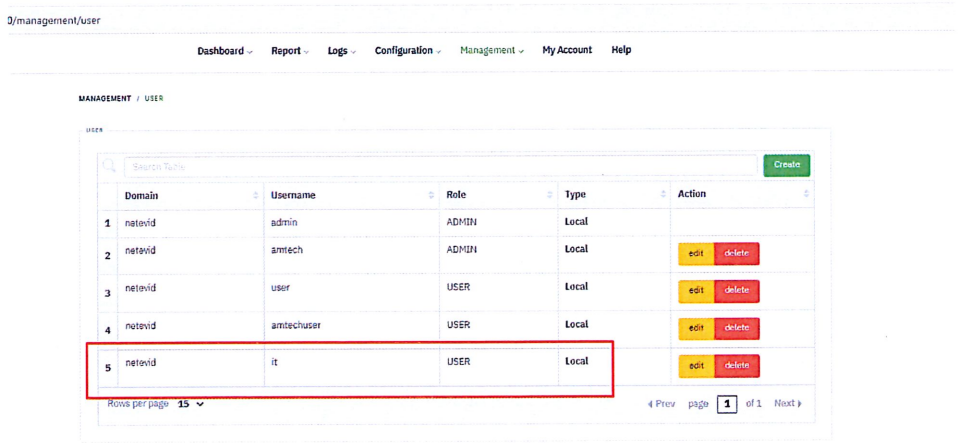
1. ไปที่ Logs Server (192.168.10.250)



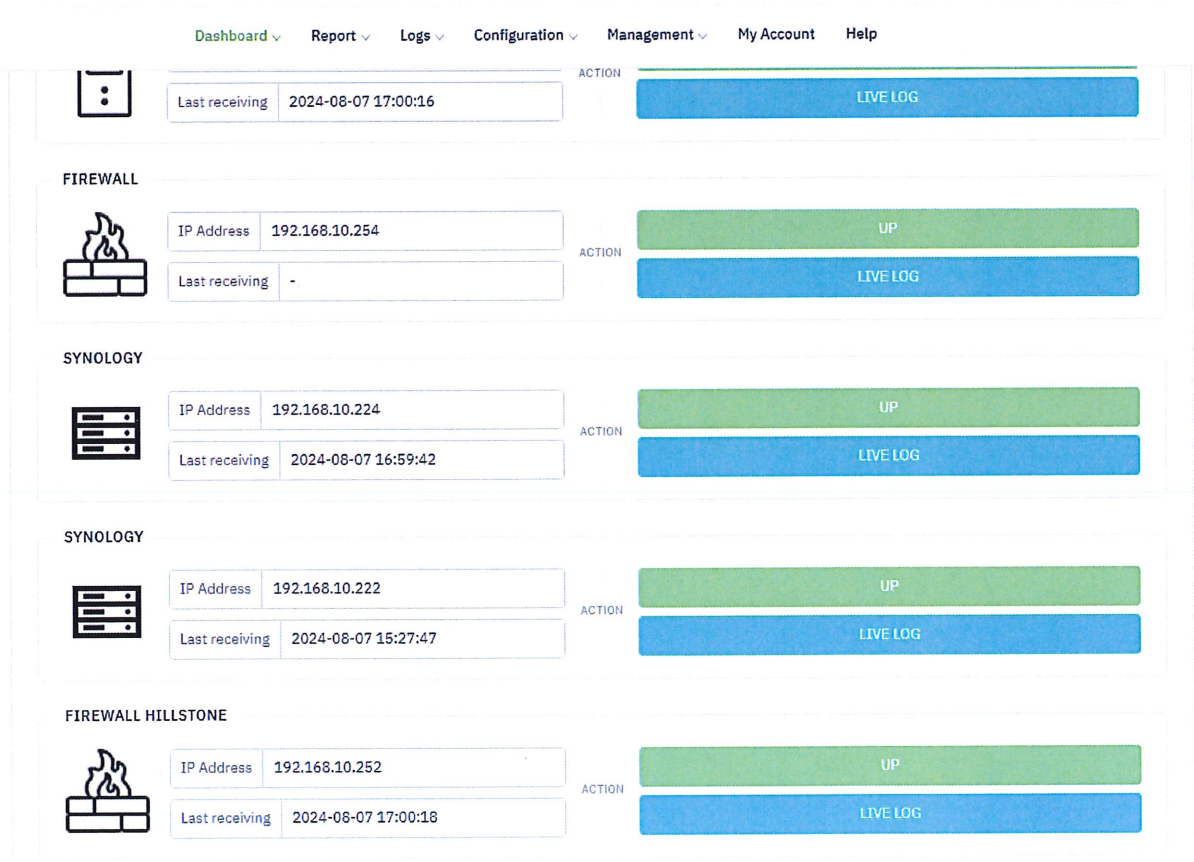
2. Login ด้วย User Administrator (จัดเก็บโดย IT Infrastructure)
3. ดูที่ Menu Logs (เลือก Logs Rules และตั้งค่า IP)



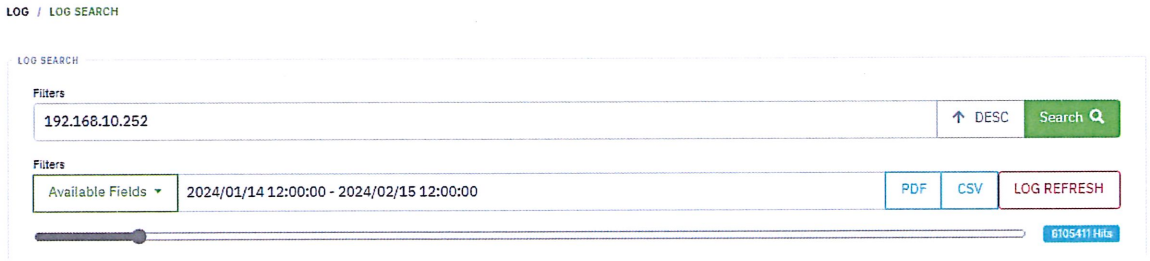
4. Login ด้วย User ที่เป็นสิทธิ์ User ทั่วไป (เนื่องจาก User Admin จะมีไว้ตั้งค่าเพียงอย่างเดียวไม่สามารถดูหรือเรียก Logs Report



5. ไปที่ Menu Dashboard เลือก Data Sources Status และเลือก HILLSTONE FIREWALL และเข้าไปที่ LIVE LOG



6. ให้ไปที่ Menu Report และเลือก Search เราจะทำการ Filter โดยพิม 192.168.10.252 และเลือกช่วงเวลา (สามารถเก็บ Logs ไว้ได้ 180 วัน) จะเห็นว่าสามารถ Export ได้ 2 แบบคือ PDF และ CSV



ประวัติการการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 กันยายน 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา
2	1.1	แก้ไขIP	15 กุมภาพันธ์ 2567	ชาญยุทธ วัฒนาศักดิกุล

ลงชื่อ _____

(นาย ชาญยุทธ วัฒนาศักดิกุล)

ผู้รับผิดชอบ

วันที่ 15/02/67

ผู้อนุมัติ

ลงชื่อ _____

(นางสาว ธนิศร ธนวงศ์เกษม)

ประธานเจ้าหน้าที่เทคโนโลยีสารสนเทศ

วันที่ 15/02/67.

วัตถุประสงค์ เพื่อที่ให้ทำงานเป็นระบบ และควบคุมในการปรับปรุงโปรแกรม หรือ Software ให้ทันสมัย และทำงานได้อย่างมีประสิทธิภาพ

ขั้นตอนการปฏิบัติการ

1. ผู้ใช้งานที่มีความประสงค์จะ Upgrade โปรแกรม/Software ต่างๆ ให้ทำการแจ้งมายังส่วนงาน IT ผ่าน Slack
2. เจ้าหน้าที่ IT Support จะตรวจสอบรายละเอียด ก่อนแจ้งไปยังผู้จัดการส่วนงาน IT /เจ้าหน้าที่ Infrastructure ตามระบบงานที่มีสิทธิ์ในการดำเนินงาน
3. ตรวจสอบ โปรแกรม/ Software
   - 3.1. หากโปรแกรม หรือ Software เวอร์ชันใหม่ที่ยังไม่เคย Upgrade มาก่อน
     - 3.1.1. ให้ทดลองก่อนเพื่อดูผลกระทบ
       - 3.1.1.1. ถ้ามีผลกระทบ เจ้าหน้าที่ IT Support จะแจ้งกับผู้ใช้งานถึงเหตุผล แล้วยกเลิกคำขอจากระบบ และรอการปรับปรุงแก้ไขให้เสร็จก่อน
       - 3.1.1.2. ถ้าไม่มีผลกระทบ ให้เจ้าหน้า IT Support ดำเนินการ Upgrade ได้
   - 3.2. โปรแกรม หรือ Software ที่ผ่านการทดสอบแล้ว
     - 3.2.1. ให้เจ้าหน้า IT Support ดำเนินการ Upgrade ได้
4. เมื่อเจ้าหน้าที่ IT Support ดำเนินการ Upgrade โปรแกรมเรียบร้อย จะทำการบันทึกในใบคำขอให้สถานะเป็น “ซ่อมสำเร็จ” ผ่านระบบ “แจ้งปัญหา IT (Repair)” เพื่อเป็นการปิดสถานะการแจ้ง

ประวัติการการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 กันยายน 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา

ผู้อนุมัติ

ลงชื่อ วรวุฒิ เทพหัสดิน 1

(วรวุฒิ เทพหัสดิน ณ อยุธยา)

ผู้รับผิดชอบ

วันที่ 1/09/2565

ลงชื่อ ธนัญร ธนวงศ์เกษม

(ธนัญร ธนวงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 1/09/2565

วัตถุประสงค์

1. เพื่อที่ให้ทำงานเป็นระบบ และทำงานได้อย่างมีประสิทธิภาพ
2. เพื่อให้ Software ถูกต้องตามมาตรฐานการใช้งานของบริษัท และถูกต้องตามกฎหมาย
3. เพื่อให้อุปกรณ์ สามารถใช้งานได้อย่างมีประสิทธิภาพ

ขั้นตอนการปฏิบัติการ

1. เจ้าหน้าที่ IT Support จะจัดทำแผนการบำรุงรักษาประจำปี นำเสนอผู้จัดการส่วนงาน IT พิจารณาตรวจสอบ
2. เมื่อแผนการบำรุงรักษาประจำปี ผ่านการอนุมัติ
3. ผู้จัดการส่วนงาน IT จัดทำ Checklist การเข้าบำรุงรักษา และตรวจสอบ Software และอุปกรณ์คอมพิวเตอร์ให้กับเจ้าหน้าที่ IT Support เพื่อใช้อ้างอิงการเข้าปฏิบัติงาน
4. เจ้าหน้าที่ IT Support จะทำการวางแผนเข้าตรวจสอบ นัดหมายผู้ใช้งานตามที่กำหนดไว้
5. สิ่งที่เจ้าหน้าที่ IT Support ทำการตรวจสอบ และบำรุงรักษาดังนี้
    5.1. ทำความสะอาดคอมพิวเตอร์
    5.2. ตรวจสอบอุปกรณ์
    5.3. ตรวจสอบความถูกต้องโปรแกรม และ Software
    5.4. ตรวจ VPN Domain
    5.5. ตรวจโปรแกรม Anti-Virus หรือ โปรแกรมป้องกันการโจรกรรม ว่ายังทำงานดีอยู่หรือไม่
6. ทำการบันทึกผลการบำรุงรักษาลงใน Checklist พร้อมลงนามผู้ตรวจสอบ
7. รวบรวมข้อมูลประกอบการจัดทำรายงานการตรวจสอบและบำรุงรักษาอุปกรณ์คอมพิวเตอร์ พร้อมระบุปัญหาที่ตรวจพบ และแนวทางการแก้ไข
8. นำเสนอผู้จัดการส่วนงาน IT พิจารณาลงนามผู้ตรวจสอบ
9. เมื่อบำรุงรักษาอุปกรณ์คอมพิวเตอร์เรียบร้อย เจ้าหน้าที่ IT Support ทำการบันทึกการบำรุงรักษาในแบบฟอร์มเก็บสินทรัพย์ (IT) ของอุปกรณ์คอมพิวเตอร์ ผ่านระบบ Kintone โดยระบุวันที่บำรุงรักษาและรายการที่บำรุงรักษา

ประวัติการการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 กันยายน 2565	วรวุฒิ เทพหัสดิน ณ อยุธยา

ผู้อนุมัติ

ลงชื่อ วรวุฒิ เทพหัสดิน ฯ

(วรวุฒิ เทพหัสดิน ณ อยุธยา)

ผู้รับผิดชอบ

วันที่ 1/09/2565

ลงชื่อ ณิศร ณนางศักเกษม

(ณิศร ณนางศักเกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 1/09/2565

BANGKOK ASSET INTERGROUP	คู่มือกระบวนการปฏิบัติงาน (Procedure Manual)	IT-Procedure-048	
	การแก้ไขระบบ/โปรแกรม	ฉบับที่ : 2.1	แผ่นที่ : 1/2
	System Change Requisition	เริ่มใช้ : 20 มกราคม 2566	

วัตถุประสงค์ เพื่อที่ให้ทำงานเป็นระบบ และควบคุมระบบ หรือ โปรแกรมให้ทำงานได้อย่างมีประสิทธิภาพ

ขั้นตอนการปฏิบัติการ

1. กรณีการแก้ไขข้อมูล
   - 1.1. เมื่อผู้ใช้งาน มีความประสงค์จะแก้ไข ระบบ โปรแกรม และฟอร์ม ให้ดำเนินการขอผ่าน “Change Request” ในระบบ Kintone กรอกรายละเอียดให้เรียบร้อย พร้อมเหตุผลในการแก้ไข
   - 1.2. ระบบจะส่งไปยังผู้จัดการส่วนงานต้นสังกัดเพื่อพิจารณาอนุมัติ
   - 1.3. เมื่อผู้จัดการส่วนงานต้นสังกัดอนุมัติแล้ว ระบบจะแจ้งเตือนไปยังผู้จัดการส่วนงาน IT เพื่อพิจารณาอนุมัติ
   - 1.4. เมื่อผู้จัดการส่วนงาน IT อนุมัติ ระบบจะแจ้งเตือนไปยัง Application Support เพื่อดำเนินการแก้ไขข้อมูลตามที่มีการร้องขอว่าจะดำเนินการอย่างไร
     - 1.4.1. ถ้าหากเป็นระบบที่เป็น Outsource ดูแล จะดำเนินการผ่านกระบวนการจัดซื้อจัดจ้างต่อไป
     - 1.4.2. ถ้าหากเป็นระบบที่สามารถแก้ไขได้จะดำเนินการขั้นต่อไป
   - 1.5. เมื่อใบคำขอได้ดำเนินการแก้ไขเรียบร้อยแล้ว Application Support จะทำการระบุผลกระทบในระบบว่ามีผลกระทบด้านใดบ้าง จากนั้น Application Support ทำการบันทึกข้อมูล และกดApprove ระบบจะส่งไปยังผู้จัดการส่วนงาน IT ทำการตรวจสอบ ระบบงานที่ทาง Application Support แก้ไข
   - 1.6. เมื่อผู้จัดการส่วนงาน IT ตรวจสอบระบบงานที่ทาง Application Support ดำเนินการเรียบร้อยแล้ว ผู้จัดการส่วนงาน IT ทำการระบุ ความคิดเห็น ทำการบันทึกข้อมูล และกดApprove ระบบจะส่งไปยัง ผู้ใช้งานเพื่อทำ UAT
   - 1.7. ระบบจะแจ้งไปยังผู้ใช้งานให้ทราบถึงผลกระทบ จากนั้นผู้ใช้งานทำการทดสอบตามระบบ หรือ Test Script
     - 1.7.1. ถ้าหากผลการทดสอบผ่าน ให้นำใส่ในช่อง Comment
     - 1.7.2. ถ้าหากผลการทดสอบไม่ผ่าน หรือ ไม่ครบถ้วน ผู้ใช้งาน (User) ทำการแจ้งรายละเอียดใส่ในช่อง Comment
       - 1.7.2.1. ระบบจะแจ้งผ่านระบบ Kintone ไปให้ Application Support ดำเนินการแก้ไขเพิ่มเติม
   - 1.8. เมื่อผลการทดสอบผ่าน ผู้ใช้งานยอมรับผลกระทบ ผู้ใช้งานจะทำการกดApprove จากนั้นระบบจะส่งไปยังทาง IT Infrastructure Supervisor เพื่อแจ้งให้ Deploy ระบบ จากนั้นเจ้าหน้าที่ IT จะทำการประกาศวันนำไปใช้
   - 1.9. เมื่อถึงวันใช้ IT Infrastructure Supervisor จะนำไปใช้ในระบบ Production ต่อไป

2. กรณีการเพิ่มข้อมูล
   - 2.1. เมื่อผู้ใช้งาน มีความประสงค์จะเพิ่ม ระบบ โปรแกรม และฟอร์ม ให้ดำเนินการขอผ่าน “ IT Request ”ในระบบ Kintone กรอกรายละเอียดให้เรียบร้อย พร้อมเหตุผลในการเพิ่ม
   - 2.2. ระบบจะส่งไปยังผู้จัดการส่วนงานต้นสังกัดเพื่อพิจารณาอนุมัติ
   - 2.3. เมื่อผู้จัดการส่วนงานต้นสังกัดอนุมัติแล้ว ระบบจะแจ้งเตือนไปยังผู้จัดการส่วนงาน IT เพื่อพิจารณาอนุมัติ
   - 2.4. เมื่อผู้จัดการส่วนงาน IT อนุมัติแล้ว ระบบจะแจ้งเตือนไปยังเจ้าหน้าที่ IT เพื่อดำเนินการเพิ่มข้อมูลตามที่มีการร้องขอว่าจะดำเนินการอย่างไร

2.4.1. ถ้าหากเป็นระบบที่เป็น Outsource ดูแล จะดำเนินการผ่านกระบวนการจัดซื้อจัดจ้างต่อไป

2.4.2. ถ้าหากเป็นระบบที่สามารถเพิ่มได้จะดำเนินการขั้นต่อไป

2.5. เมื่อใบคำขอได้ดำเนินการเพิ่มเรียบร้อยแล้ว ระบบจะส่งไปยังผู้จัดการส่วนงาน IT ทำการตรวจสอบ ระบบงานที่ทางเจ้าหน้าที่ IT แก้ไข

2.6. ระบบจะแจ้งไปยังผู้ใช้งานให้ทราบ แล้วผู้ใช้งานทำการทดสอบตามระบบ หรือ Test Script

2.6.1. ถ้าหากผลการทดสอบผ่าน ให้นำใส่ในช่อง Comment

2.6.2. ถ้าหากผลการทดสอบไม่ผ่าน หรือ ไม่ครบถ้วน ผู้ใช้งาน (User) ทำการแจ้งรายละเอียดใส่ในช่อง Comment

2.7. เมื่อผลการทดสอบผ่าน ผู้ใช้ยอมรับ ทางเจ้าหน้าที่ IT จะทำการประกาศวันนำไปใช้

2.8. เมื่อถึงวันใช้ เจ้าหน้าที่ IT จะนำไปใช้ในระบบ Production ต่อไป

**หมายเหตุ : กรณีฉุกเฉินผู้ขอสามารถมาขอเอกสารแบบฟอร์มการขอเปลี่ยนแปลง / แก้ไขระบบ (Change request) ได้ที่เจ้าหน้าที่ IT

ประวัติการการปรับปรุงเอกสาร				
ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 กันยายน 2565	กร ธรรมมาพาณิชย์
2	1.1	แก้ในส่วนการเพิ่มข้อมูล	7 ตุลาคม 2565	กร ธรรมมาพาณิชย์
3	2.0	แก้ไขกระบวนการ	30 ธันวาคม 2565	กร ธรรมมาพาณิชย์
4	2.1	แก้ไขส่วนของกรณีการเพิ่มข้อมูล เปลี่ยนจากแบบฟอร์ม Get Requirement เป็น แบบฟอร์ม IT Request	20 มกราคม 2566	กร ธรรมมาพาณิชย์

ผู้อนุมัติ

ลงชื่อ กร ธร

(กร ธรรมมาพาณิชย์)

ผู้รับผิดชอบ

วันที่ 20 ม.ค 66

ลงชื่อ [signature]

([signature])

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 20 ม.ค. 66

ขั้นตอนการควบคุมการลง Software

วัตถุประสงค์

1. เพื่อเป็นมาตรฐานในการใช้งานโปรแกรมและระบบในบริษัท
2. เพื่อเป็นควบคุมการใช้งานโปรแกรมและระบบให้ถูกต้องตามกฎหมาย หรือ พรบ.คอมพิวเตอร์

ขั้นตอนการปฏิบัติการ

1. ผู้ใช้งานขอใช้งานโปรแกรม/ระบบ มาทางระบบ Kintone ผ่านแบบฟอร์ม “IT Request”
2. เมื่อได้รับการ Approved จากระบบแล้ว เจ้าหน้าที่ IT Support ตรวจสอบว่าทาง ฝ่ายเทคโนโลยีสารสนเทศได้มีโปรแกรมนั้นอยู่ใน Stock หรือไม่
   2.1. หากไม่อนุมัติให้หัวหน้าสายงานแผนกเทคโนโลยีชี้แจงเหตุผลและกดยกเลิกในระบบ
   2.2. หากมีอยู่แล้วให้ทำการ install ได้เลย
   2.3. หากไม่มีใน stock ให้ทำการแจ้ง หัวหน้าสายงานให้รับทราบ เพื่อทำการสั่งซื้อโปรแกรม
      2.3.1. ทำการขอใบเสนอราคาโปรแกรม หลังจากได้ใบเสนอราคามาแล้ว แจ้งราคาให้หัวหน้าสายงานและผู้ขอใช้งานทราบ
      2.3.2. เมื่อได้รับการอนุมัติแล้วจากหัวหน้าสายงานของผู้ร้องขอ และหัวหน้าสายงานฝ่ายเทคโนโลยีสารสนเทศ ให้ทำการสั่งซื้อโปรแกรมตามที่ผู้ใช้งานร้องขอ
      2.3.3. เมื่อได้รับ License/โปรแกรมมาแล้ว ให้เจ้าหน้าที่เทคโนโลยีสารสนเทศบันทึกใน Software Inventory
      2.3.4. ทำการลงโปรแกรมที่เครื่องของผู้ใช้งานที่ร้องขอ
      2.3.5. ผู้ร้องขอเซ็นรับทราบ
3. ให้เจ้าหน้าที่ IT Support เก็บรายละเอียดเครื่องที่ลงโปรแกรมและวันที่ลงโปรแกรม แล้วบันทึกในระบบ
4. ปิดการขอใน “IT Request” ในระบบ Kintone

ประวัติการการปรับปรุงเอกสาร				
ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 พฤศจิกายน 2565	วีรพล วุฒิเสมานานนท์

ผู้อนุมัติ

ลงชื่อ วีรพล

(วีรพล วุฒิเสมานานนท์)

ผู้รับผิดชอบ

วันที่ 26/10/2565

ลงชื่อ

( )

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 27/10/2565

ขั้นตอนการปฏิบัติงานรองรับสถานการณ์ฉุกเฉิน

1. วัตถุประสงค์

1.1 เพื่อให้บริษัทสามารถดำเนินธุรกิจไปได้อย่างต่อเนื่อง ในสถานการณ์ที่ไม่ปกติหรือสถานการณ์ฉุกเฉิน

1.2 เพื่อที่ลดความเสี่ยงที่จะเกิดขึ้น และรับมือกับความเสี่ยงต่างๆ ที่ทำให้บริษัทหยุดชะงัก ได้อย่างมีประสิทธิภาพ

1.3 เพื่อให้มีแผนที่เป็นระบบเป็นขั้นตอนในการรองรับกับเหตุการณ์ที่จะเกิดขึ้น รวมทั้งทดลอง และปรับปรุงให้ดีขึ้นเหมาะสม

2 ขอบเขต

2.1 โปรแกรม หรือ Application ที่เป็นหลักในการดำเนินธุรกิจของของบริษัท หรือมีผลทำให้บริษัทหยุดชะงักเท่านั้น โดยอาศัยการประเมินจาก Risk Management Method ของบริษัท

2.2 การ Backup และ Recovery ของระบบตามที่ระบบในข้อ 2.1

2.3 การ Backup และ Recovery เป็นไปตามระบบ และข้อกำหนดของโปรแกรม หรือ Application นั้นๆ

2.3.1 ตารางการ Backup

ระบบ	Day	Backup	Location	ผู้รับผิดชอบ
OS	Daily (Sun – Fri) Weekly (Sat) Monthly	Incremental Full Full (Rolling 3 Months)	Cloud	ชาญยุทธ วัฒนาศักดิกุล
DBC	Daily (Mon – Sat) Weekly (Sun)	Differential (Every12-24hrs) Rolling 28 Days	Cloud	ชาญยุทธ วัฒนาศักดิกุล

		Full (Rolling 4 Weeks) Replicated		
Kintone	Everyday	Replicated (Mirroring)	Cloud	ชาญยุทธ วัฒนา ศักดิกุล
Storage (NAS)	Daily (Sun – Sat)	Synchronize to Cloud	Cloud	ชาญยุทธ วัฒนา ศักดิกุล

3 ขั้นตอนการทำงาน

3.1 กระบวนการยอมรับและการประเมินความเสี่ยงของระบบ

3.1.1 การ Backup ระบบโดย Backup เฉพาะระบบ หรือ Application ที่มีความเสี่ยงสูงเท่านั้นจากการประเมณความเสี่ยงของบริษัท

3.1.2 หากมีการเปลี่ยนในกรณีพิเศษหรือฉุกเฉินให้ทำการส่งใบคำขอเปลี่ยนการBackup มาให้ IT เพื่อพิจารณา และดำเนินการ

3.2 กระบวนการ Backup และ Retention เป็นไปตามแผนบริหารความต่อเนื่องทางธุรกิจ (BCP)

3.3 Backup Log จะต้องปฏิบัติมีการตรวจสอบทุกวันตามใบบันทึกการสำรองข้อมูล

3.3.1 หากมีข้อผิดพลาดในการBackup จะต้องมีการบันทึก และ แก้ไข หากมีข้อผิดพลาดหรือสำรองข้อมูลไม่ได้ติดต่อ 3 วันจะต้องรายงานต่อผู้บริหารระดับสูงเพื่อดำเนินการต่อไป

3.4 กระบวนการ Recovery

3.4.1 OS

3.4.1.1 คู่มือการ Backup/Restore OS ดังนี้

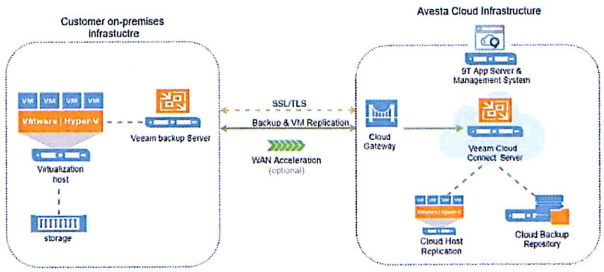
IT-Procedure-007 (Backup Data).docx

3.4.2 DBC

3.4.2.1 คู่มือการ Backup/Restore DBC ดังนี้

IT-Procedure-014
(DBC Backup-Store).

3.4.3 Kintone ระบบ Kintone เป็นระบบที่อยู่บน Cloud Based System ที่มีการทำ Backup แบบ Mirroring Site to Site (100% แบบ Realtime) ที่บริษัท Cybozu แสดงไว้ดังภาพ



(ดังนั้น ระบบ Kintone ไม่ต้องมีกระบวนการ Backup และ Restore)

3.5 กระบวนการทดสอบ (Testing) และการตรวจสอบ (Verification) เป็นไปตามคู่มือ/ขั้นตอนของแต่ละแผนกที่เกี่ยวข้อง มีการตรวจสอบ และปรับปรุงให้ถูกต้องเสมอ

3.6 กระบวนการประเมิน (Evaluation) และปรับปรุง (Improvement) จะมีการประเมินและปรับปรุงหลังจากการทดสอบ เพื่อนำไปประกาศใช้เป็นแผนบริหารความต่อเนื่องทางธุรกิจ (BCP) ฉบับล่าสุดต่อไป

3.7 กระบวนการนำไปใช้ (Execution)

3.7.1 นำไปทบทวนกับแผนบริหารความต่อเนื่องทางธุรกิจ (BCP) อย่างน้อยปีละ 1 ครั้ง เพื่อให้แผนบริหารความต่อเนื่องทางธุรกิจ (BCP) เป็นปัจจุบัน และสอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป เช่น การเปลี่ยนแปลงพนักงานที่มีหน้าที่รับผิดชอบในการดำเนินงานตามแผน

7. สิ่งที่แนบมา

ผลการประเมินจาก Risk Management Method

BAI: Applications Risk and Classification

ลำดับ	ระบบงาน	Version	ผู้พัฒนาระบบ	ที่อยู่ของระบบ	ผู้รับผิดชอบ	ผู้ที่ใช้ระบบ	ระดับความสำคัญ	ความเสี่ยงทางธุรกิจ	วัตถุประสงค์
1	OS	ไม่มี	Programmer : น10 วีรยุทธ คณานันท์	http://www.osintergroup.com	IT	list,sales,DC,Renovate ,Finance-account,MK	สูง	สูง	บันทึกข้อมูลทรัพย์สินและสถานะทรัพย์สิน
2	DBC	19.3.34541.35210	Microsoft	/f36b0000-fc67-467e-834d-9aa70841856b/produ	Finance	Finance, Purchase, Admin	สูง	สูง	ระบบERP ของทางบริษัท
3	Kintone	ไม่มี	Cybozu	http://bai.cybozu.com	IT	Finance, Purchase, Admin, Sales, List, HR	สูง	สูง	แบบฟอร์มและสัญญาแต่งตั้งนายหน้า
4	ขวัญใจ	1.0.94	บริษัท บิลด์ วัน กรุ๊ป จำกัด(สำนักงานใหญ่)	https://kwanjai.bulk.com/login	IT	After service	ปานกลาง	ปานกลาง	สำหรับลูกค้า(ผู้ซื้อ)แจ้งซ่อมบ้านภายหลังใหม่
5	fastinspect.co	2.1.63	บริษัท ฟาสท์ อินสเปก จำกัด	s://api.fastinspect.co/backend/public/login/devel	IT	renovate,After service,sales	ปานกลาง	ปานกลาง	สำหรับตรวจdefect บ้าน
6	ZOHO CRM	3.5.25	Zoho Corporation	http://crm.zoho.com	MK	MK,Sale	ปานกลาง	ปานกลาง	ระบบCRM ของทางบริษัท
7	Timemint	2.8.1	บริษัท เน็กซ์สไปร์ จำกัด	http://timemint.co	HR	All department	ปานกลาง	ปานกลาง	ระบบการบันทึกเวลาพนักงาน
8	Slack	ไม่มี	Slack Technologies	http://bangkokasset.slack.com	IT	All department	ปานกลาง	ปานกลาง	สำหรับใช้สื่อสารกันภายในบริษัท

8. ประวัติ

ประวัติการการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 เมษายน 2565	น.ส.ณัฐธิดา สิงห์คง
2	1.1	แก้ไขตาม Audit Comment บริษัท IVL 1. ชื่อของเอกสาร 2. ผู้อนุมัติ	3 กรกฎาคม 2565	น.ส.ธนิศร ธนวงศ์เกษม
3	2.0	แก้ไขตาม IVL Audit Comment 1.แก้เอกสารจาก SOP เป็น ขั้นตอนการทำงาน 2.เพิ่มรายละเอียดการ Backup	15 พฤศจิกายน 2565	น.ส.ธนิศร ธนวงศ์เกษม
4	2.1	แก้ไขชื่อผู้รับผิดชอบ	15 มกราคม 2567	ชาญยุทธ วัฒนาศักดิกุล

ลงชื่อ_____

(นาย ชาญยุทธ วัฒนาศักดิกุล)

ผู้รับผิดชอบ

วันที่ 15/01/67

ผู้อนุมัติ

ลงชื่อ_____

(นางสาว ธนิศร ธนวงศ์เกษม)

ประธานเจ้าหน้าที่เทคโนโลยีสารสนเทศ

วันที่ 15/01/67

ขั้นตอนการจัดการพนักงานลาออก

วัตถุประสงค์

1. เพื่อเป็นมาตรฐานในการจัดการพนักงานลาออก และรักษาผลประโยชน์สูงสุดให้กับบริษัท
2. เพื่อให้การจัดการระบบทั้ง Hardware/Software/Application ให้ถูกต้องอยู่เสมอ

ขั้นตอนการปฏิบัติการ

1. เจ้าหน้าที่ฝ่ายบุคคล แจ้งชื่อพนักงานที่จะลาออก พร้อมวันที่จะพ้นสภาพจากพนักงานในโปรแกรม Slack
2. เจ้าหน้าที่ IT ตรวจสอบรายการทรัพย์สิน และเตรียมเอกสารให้พนักงานที่ลาออกเซ็นรับคืนทรัพย์สินทั้ง Hardware และSoftware
3. เมื่อพนักงานที่จะลาออกคืนทรัพย์สินกับเจ้าหน้าที่ IT Support จะทำการตรวจสภาพทรัพย์สินทั้งหมด โดยที่
   3.1. กรณีที่ทรัพย์สินทั้งหมดไม่ชำรุด ให้พนักงานที่จะลาออกเซ็นคืนทรัพย์สินกับเจ้าหน้าที่ IT
   3.2. กรณีที่ทรัพย์สินชำรุด ทางเจ้าหน้าที่ IT จะแจ้งอาการกับทางเจ้าหน้าที่ฝ่ายบุคคลเพื่อเรียกเก็บค่าเสียหายตามอาการที่เกิดขึ้น
4. เมื่อเจ้าหน้าที่ IT Support รับคืนทรัพย์สินทั้ง Hardware และSoftware แล้วให้ปรับปรุงข้อมูลผู้ถือครองในแบบฟอร์มเก็บสินทรัพย์ITในระบบ Kintone และโปรแกรมใน Software Inventory ให้ถูกต้อง
5. เจ้าหน้าที่ IT จะแจ้งข้อมูลทรัพย์สินที่ได้ปรับปรุงแล้วให้แผนกบัญชีทราบผ่านโปรแกรม Slack
6. ทางแผนกบัญชีดำเนินการปรับปรุงข้อมูล DBC ให้เป็นปัจจุบันต่อไป

ประวัติการการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 พฤศจิกายน 2565	วีรพล วุฒิเสมานานนท์

ผู้อนุมัติ

ลงชื่อ วีรพล

(วีรพล วุฒิเสมานานนท์)

ผู้รับผิดชอบ

วันที่ 1 ธ.ค 2565

ลงชื่อ ธนวงศ์ทอม

(ธนวงศ์ทอม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 1 ธ.ค. 2565

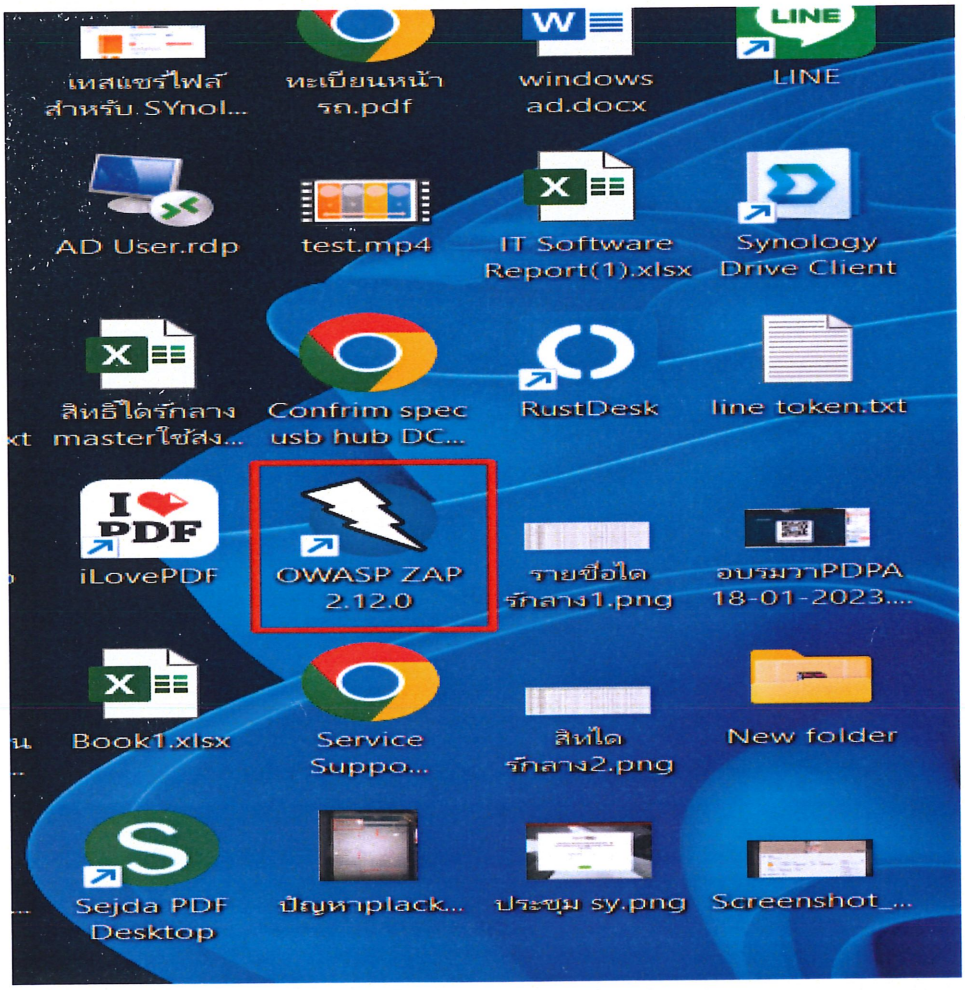
ขั้นตอนการทดสอบเจาะระบบ

วัตถุประสงค์

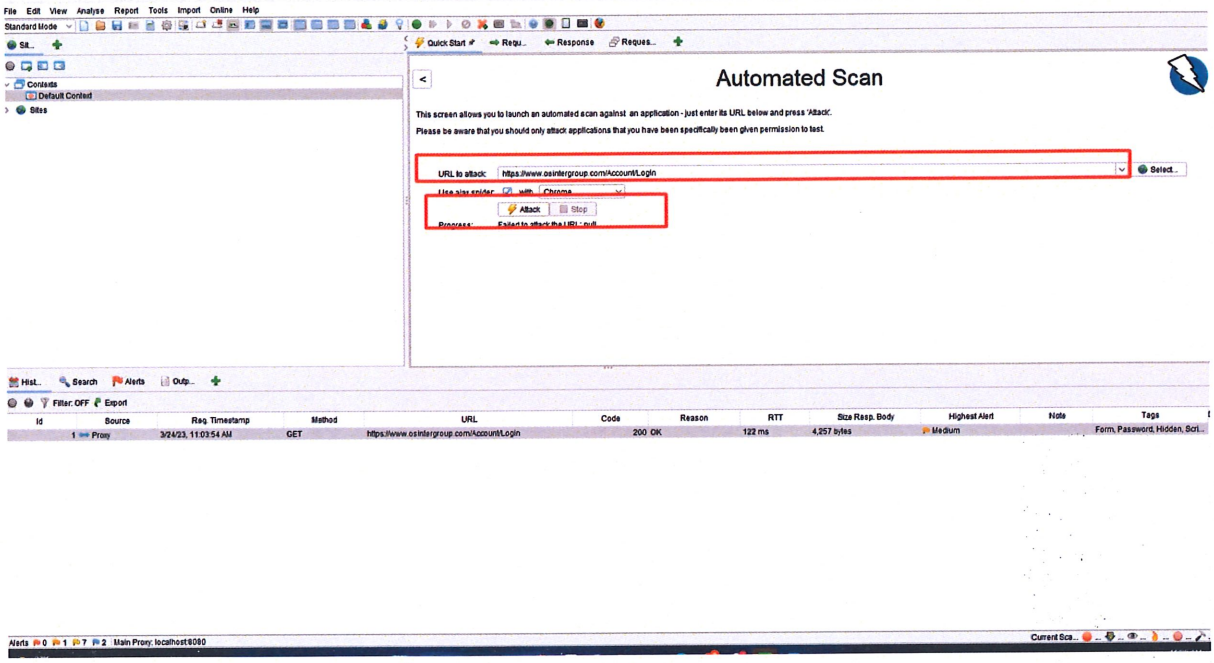
1. เพื่อทดสอบความปลอดภัยของระบบงานให้มีปลอดภัยโดยเราจะทำการทดสอบทุกๆ 3 เดือน
2. เพื่อที่เราจะได้รับรู้และแก้ไขปัญหาได้ก่อนจะเกิดปัญหาขึ้น

ขั้นตอนการปฏิบัติการ

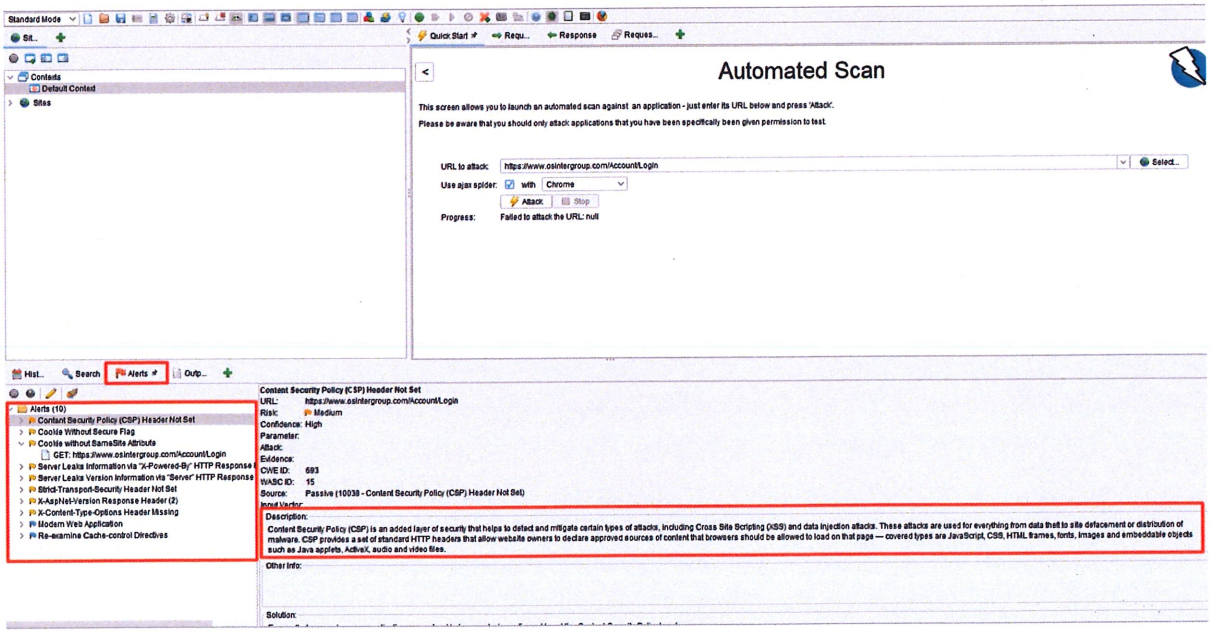
1. เจ้าหน้าที่ ไอทีทำการติดตั้งโปรแกรม Owasp Zap เพื่อทำการค้นหาช่องโหว่ของเว็บไซต์



2. ทำการ กรอก UrlหรือIP ของระบบที่เราต้องการเจาะ เช่น 192.168.1.224:5000 กด Attack



3. ระบบจะทำการรันโปรแกรมและจะขึ้นผลการรันตรงช่อง Alerts และจำนวนการตรวจพบ และบอกคำอธิบายของปัญหาที่ตรวจเจอรวมถึงความเสี่ยงของปัญหานั้นและแนวทางการแก้ปัญหา



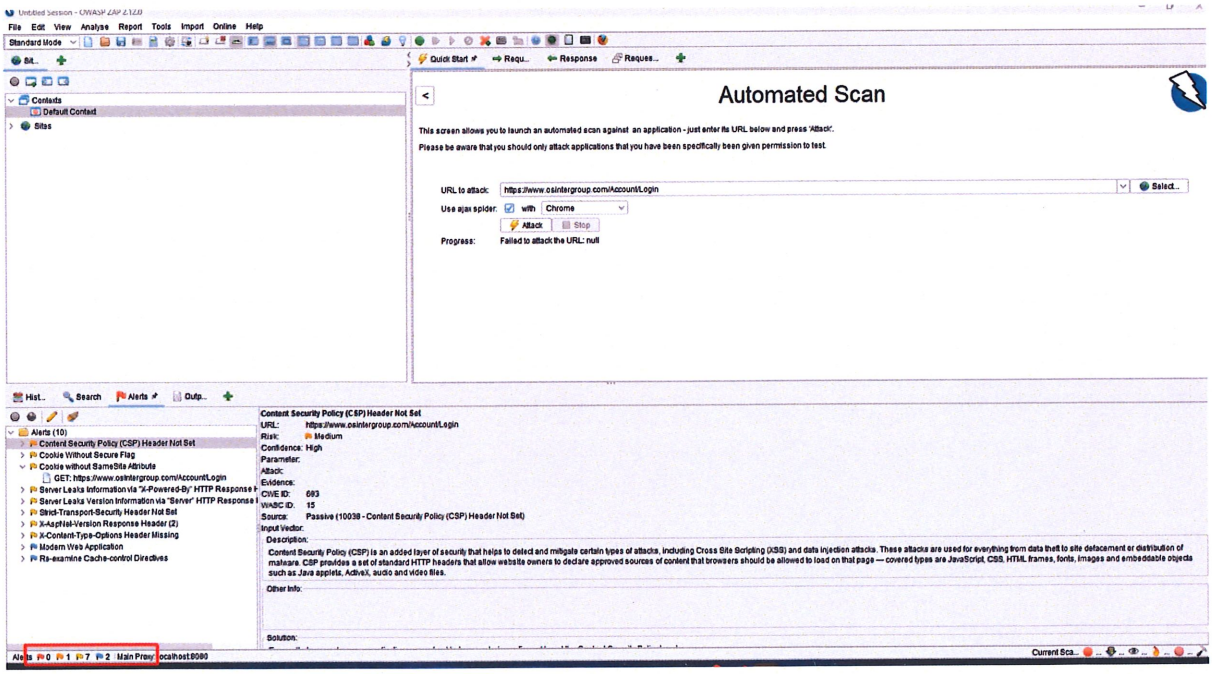
4. เจ้าหน้าที่ ไอทีทำการตรวจสอบ Alert ว่าเป็นประเภทไหน โดยจะแบ่งประเภทตามนี้

4.1. ค่าความเสี่ยงสูงสีแดง เป็นปัญหาที่ถูกตรวจพบและต้องได้รับการแก้ไขโดยทันทีเพราะเป็นปัญหาที่อาจทำให้เราโดนโจมตีหรือทำให้ระบบไม่สามารถใช้งานต่อได้

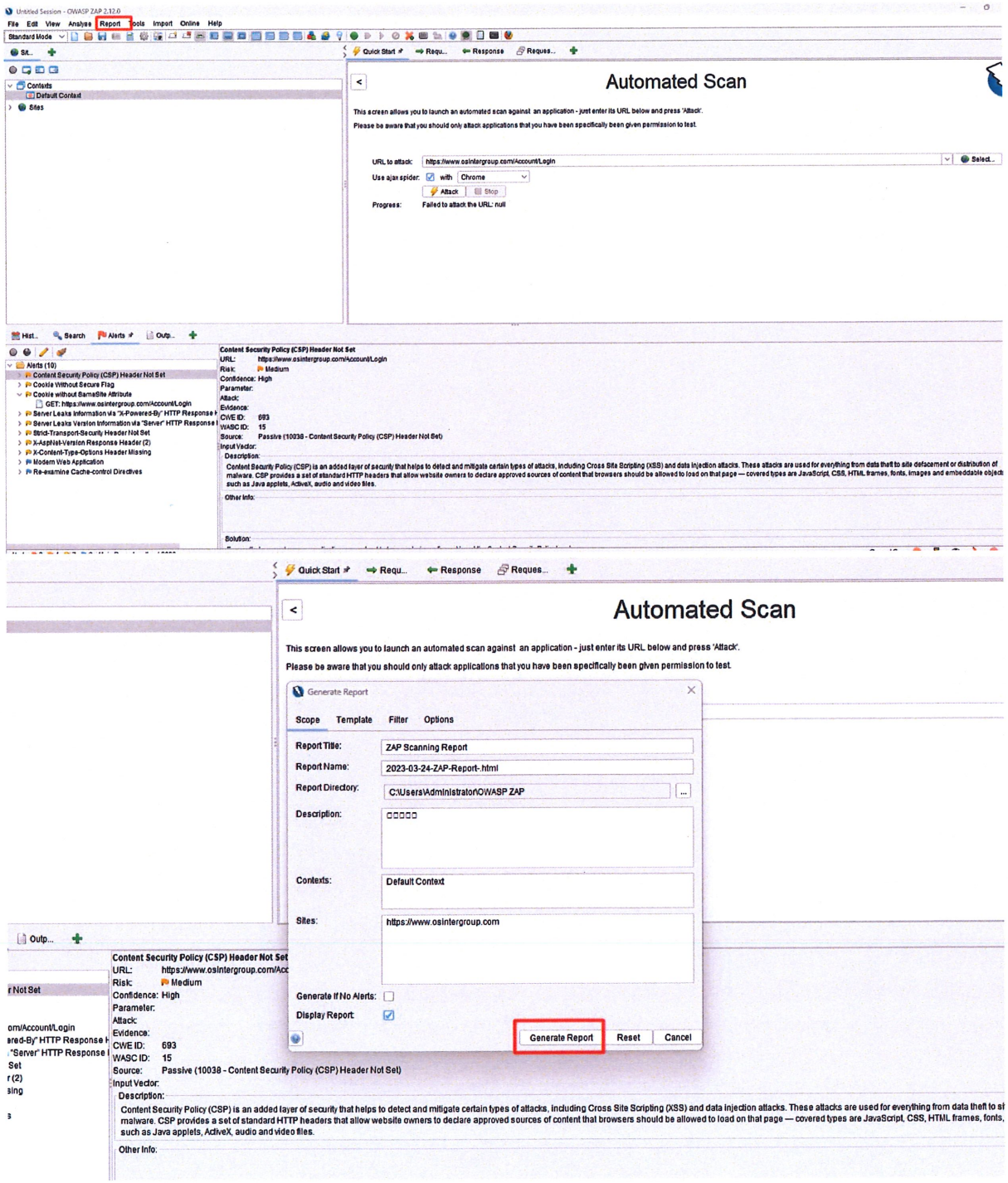
4.2. ค่าความเสี่ยงปานกลางสีส้ม เป็นปัญหาที่ถูกตรวจพบและควรได้รับการแก้ไขแต่หากปัญหานั้นไม่นั้นส่งผลถึงการใช้งานหรือความปลอดภัย ปัญหานั้นไม่นั้นไม่จำเป็นที่ต้องได้รับการแก้ไขในทันที

4.3. ค่าความต่ำสีเหลือง เป็นปัญหาที่ถูกตรวจพบ แต่ไม่ส่งผลต่อระบบความปลอดภัยหรือส่งผลต่อการใช้งาน

4.4. ความเสี่ยงต่ำสีฟ้า อาจเป็นปัญหาหรือข้อมูลที่เราควรทราบว่าตรวจพบแต่ไม่ส่งผลแก่ระบบนั้น



5. เมื่อทำการแสกนเสร็จแล้วให้ทำการกดไปที่ปุ่ม Report เพื่อ Report ปัญหาที่ตรวจพบทั้งหมดออกมา



Site http://197.163.21.1 (0) (3) (5) (7)

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Application Error Disclosure	Medium	1 (14.3%)
Content Security Policy (CSP) Header Not Set	Medium	4 (57.1%)
Missing Anti-clickjacking Header	Medium	4 (57.1%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	8 (114.3%)
Timestamp Disclosure - Unix	Low	74 (1,057.1%)
Information Disclosure - Suspicious Comments	Informational	3 (42.9%)
Modern Web Application	Informational	2 (28.6%)
Total		7

Alerts

ประวัติการการปรับปรุงเอกสาร				
ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 มีนาคม 2566	วีรพล วุฒิเสมานานนท์

ผู้อนุมัติ

ลงชื่อ วีรพล

(วีรพล วุฒิเสมานานนท์)

ลงชื่อ ธนิศร ธนวงศ์เกษม

(ธนิศร ธนวงศ์เกษม)

ผู้รับผิดชอบ

วันที่ 1 มีนาคม 2566

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 1 มีนาคม 2566

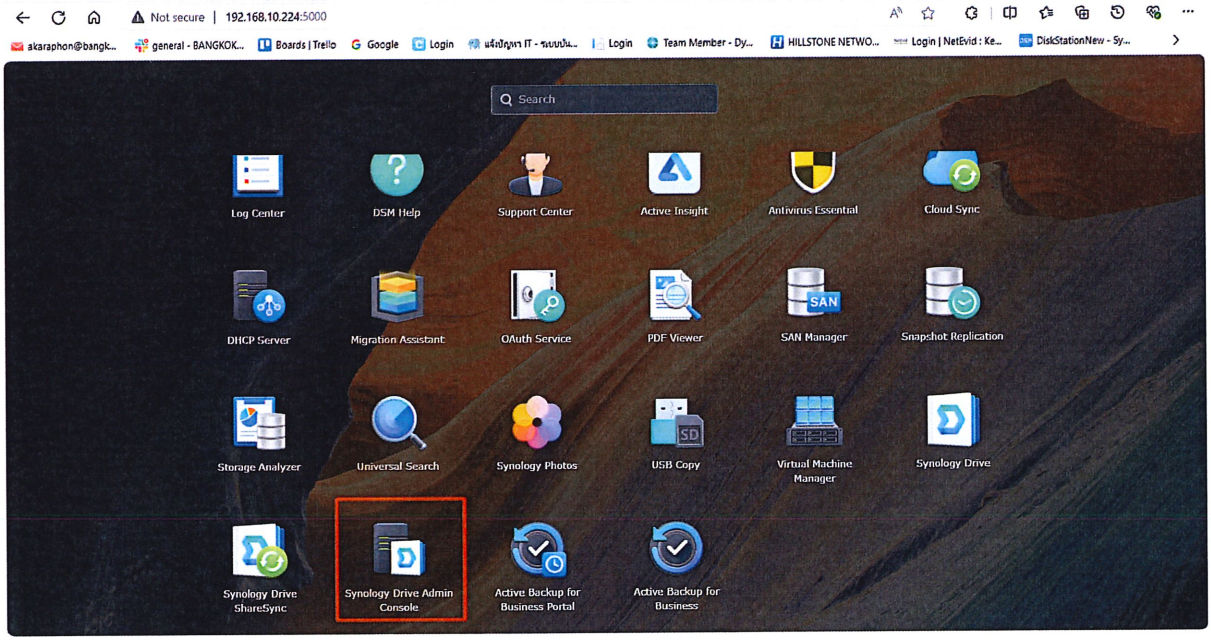
ขั้นตอนการกู้ข้อมูลจากไฟล์ที่อยู่ใน Server

วัตถุประสงค์

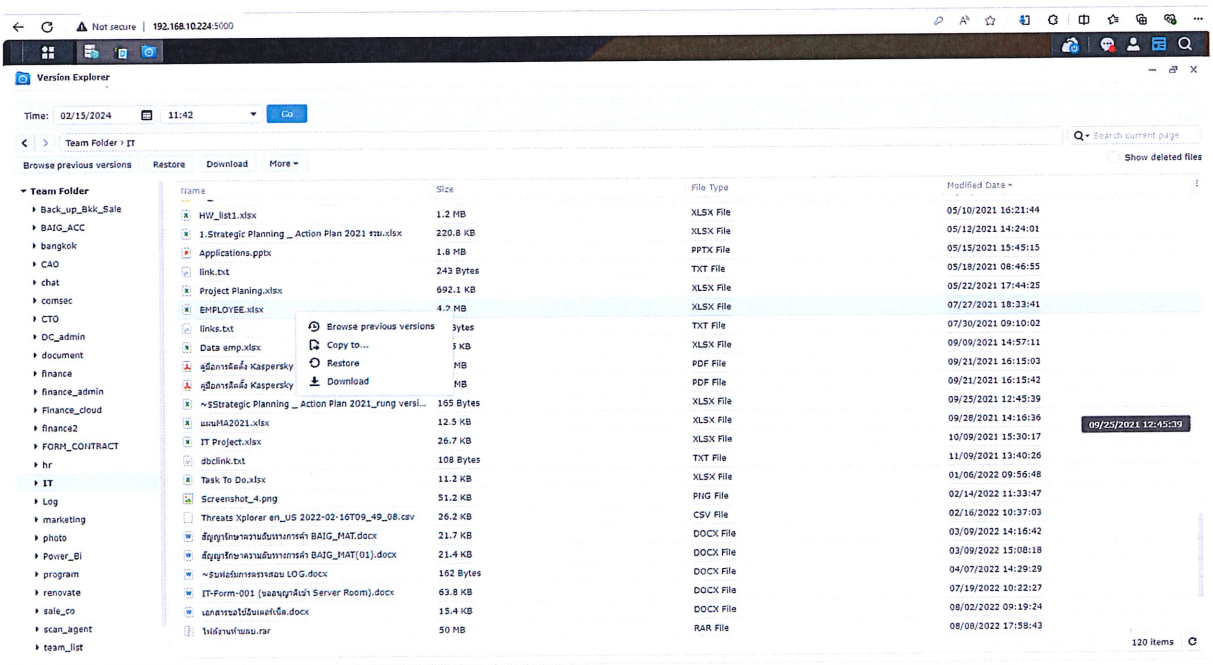
1. เพื่อทำการเรียกข้อมูลเดิมที่ได้มีการลบออกไปจาก Server ให้สามารถนำกลับมาใช้งานได้อีกครั้ง
2. เพื่อป้องกันข้อมูลจากการถูกคุกคามทาง Cyber เช่น Malware , Ransomware ,ไฟล์ถูกเข้ารหัส (Encrypt)

ขั้นตอนการปฏิบัติการ

1. Log in เข้าใช้งาน server 192.168.10.224 โดยใช้สิทธิ์ admin
2. **กรณีต้องการกู้คืนเป็น ไฟล์** คลิกเลือกสัญลักษณ์  มุมบนซ้ายของหน้าจอและเลือกหัวข้อ Synology Drive Admin Console ตามภาพด้านล่าง



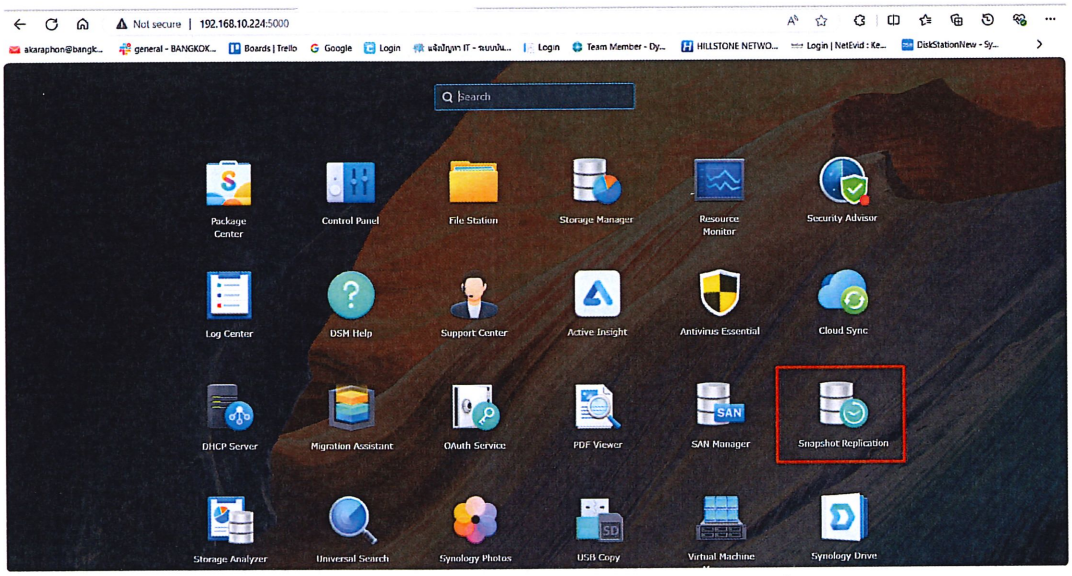
3. เลือกไฟล์ที่ต้องการโดยคลิกที่ Team Folder>Version Explorer>เลือก วัน/เวลาที่ทำการลบไฟล์ไป>เลือกไฟล์ ที่ต้องการ>คลิกขวาไฟล์ที่ต้องการกู้คืน ตามรูป



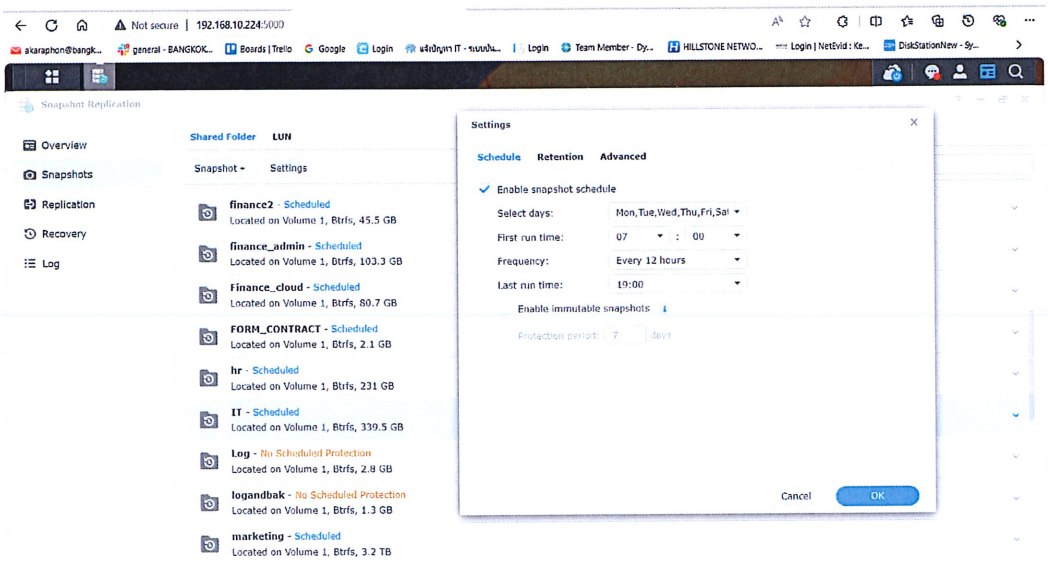
3.1. กรณีเลือก Restore ไฟล์ที่เลือกจะกลับไปปรากฏที่เดิม ที่ได้ทำการลบไป

3.2. กรณีเลือก Download ไฟล์ที่เลือก จะถูก Download มาอยู่ในเครื่อง

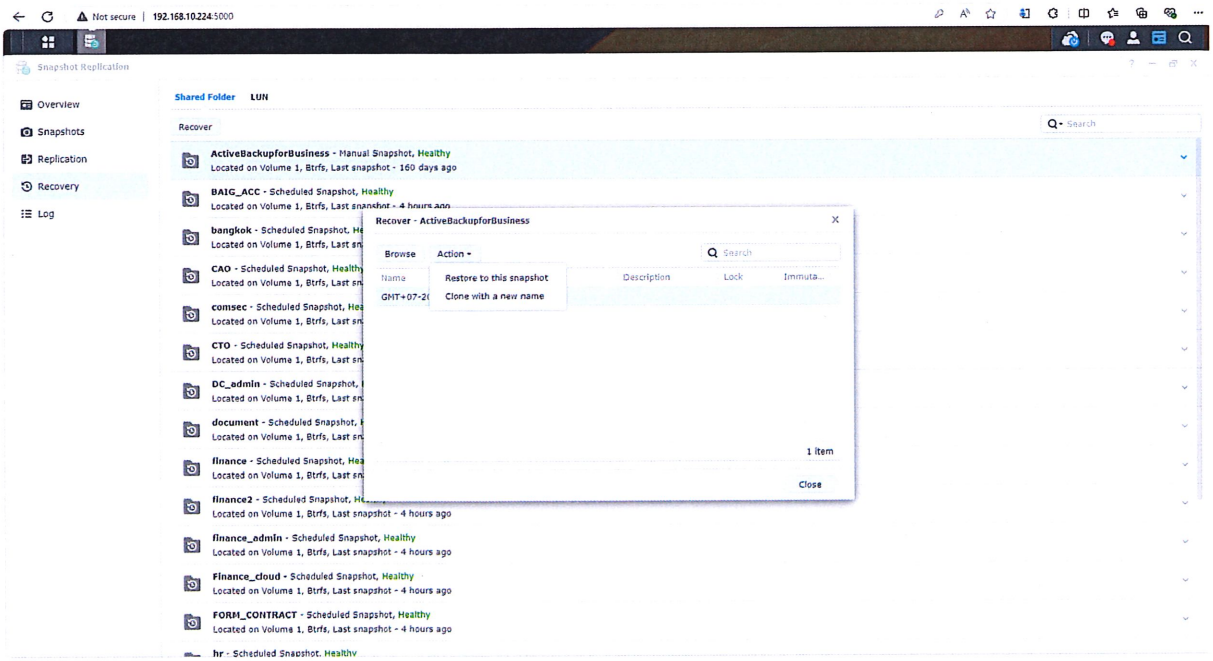
4. **กรณีต้องการกู้คืนเป็น โฟลเดอร์** คลิกเลือกสัญลักษณ์  มุมบนซ้ายของหน้าจอและเลือกหัวข้อ Snapshot Replication ตามภาพด้านล่าง



5. วิธีการตั้ง วัน/เวลา ในการ Back up ข้อมูล โดยการเลือก Snapshots > Folderที่ต้องการ Back up > Settings > Select Days (เลือกวัน ที่ต้องการ) > Starting at (เลือกเวลาที่ต้องการ) > OK



6. จากนั้นเลือก Recovery >เลือกโฟลเดอร์ที่ต้องการกู้ข้อมูลคืน >เลือก Recover >เลือก วันและเวลาที่ต้องการกู้ข้อมูลคืน >เลือก Action



5.1 หากเลือก Restore to this snapshot โฟลเดอร์ที่ถูกกู้คืนจะเข้าไปแทนที่ โฟลเดอร์ ปัจจุบัน

5.2 หากเลือก Clone with a new name โฟลเดอร์ที่ถูกกู้คืนจะ ถูกสร้างขึ้นมาใหม่

หลังจากทำการ Recover เสร็จเรียบร้อยแล้ว จากนั้นก็สามารถใช้งานข้อมูลในโฟลเดอร์ได้ตามปกติ

ประวัติการการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	8 พฤษภาคม 2566	จเร เณรแตง
2	1.1	แก้ไขIP	1 กุมภาพันธ์ 2567	ชาญยุทธ วัฒนาศักดิกุล

ลงชื่อ_____

(นาย ชาญยุทธ วัฒนาศักดิกุล)

ผู้รับผิดชอบ

วันที่ 01/02/67

ผู้อนุมัติ

ลงชื่อ_____

(นางสาว ธนิศร ธนวงศ์เกษม)

ประธานเจ้าหน้าที่เทคโนโลยีสารสนเทศ

วันที่ 01/02/67

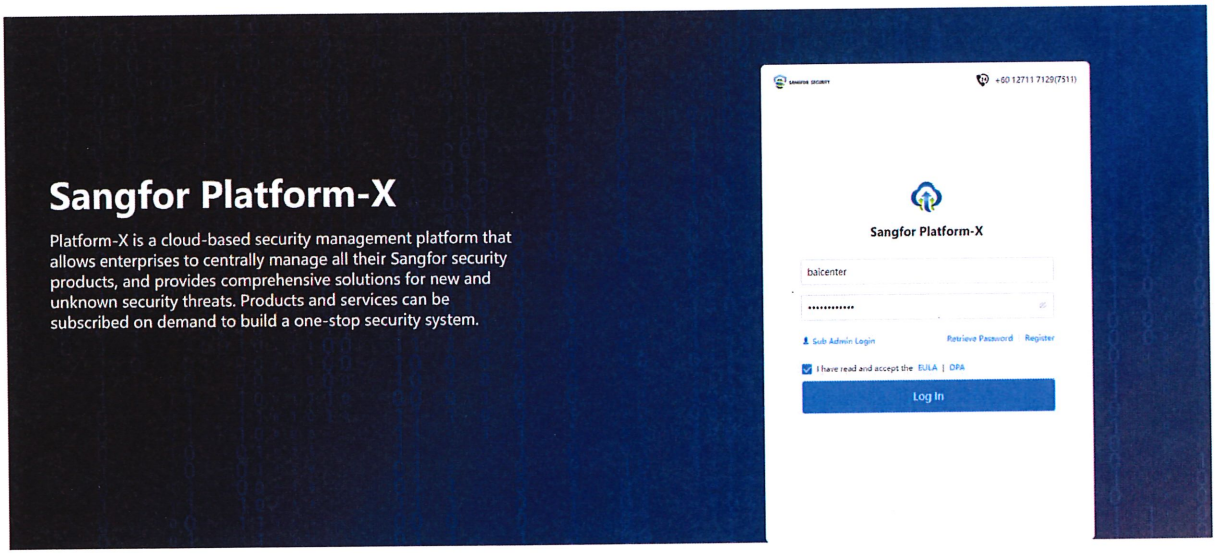
ขั้นตอนการเก็บ Log Anti-Virus

วัตถุประสงค์

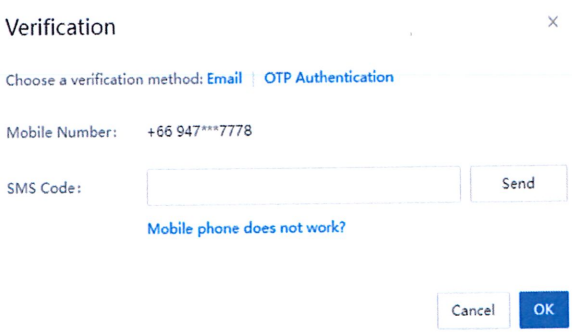
1. เพื่อเก็บข้อมูลของไวรัสและตรวจสอบความปลอดภัยของโปรแกรม Anti-Virus อย่างสม่ำเสมอ

ขั้นตอนการปฏิบัติการ

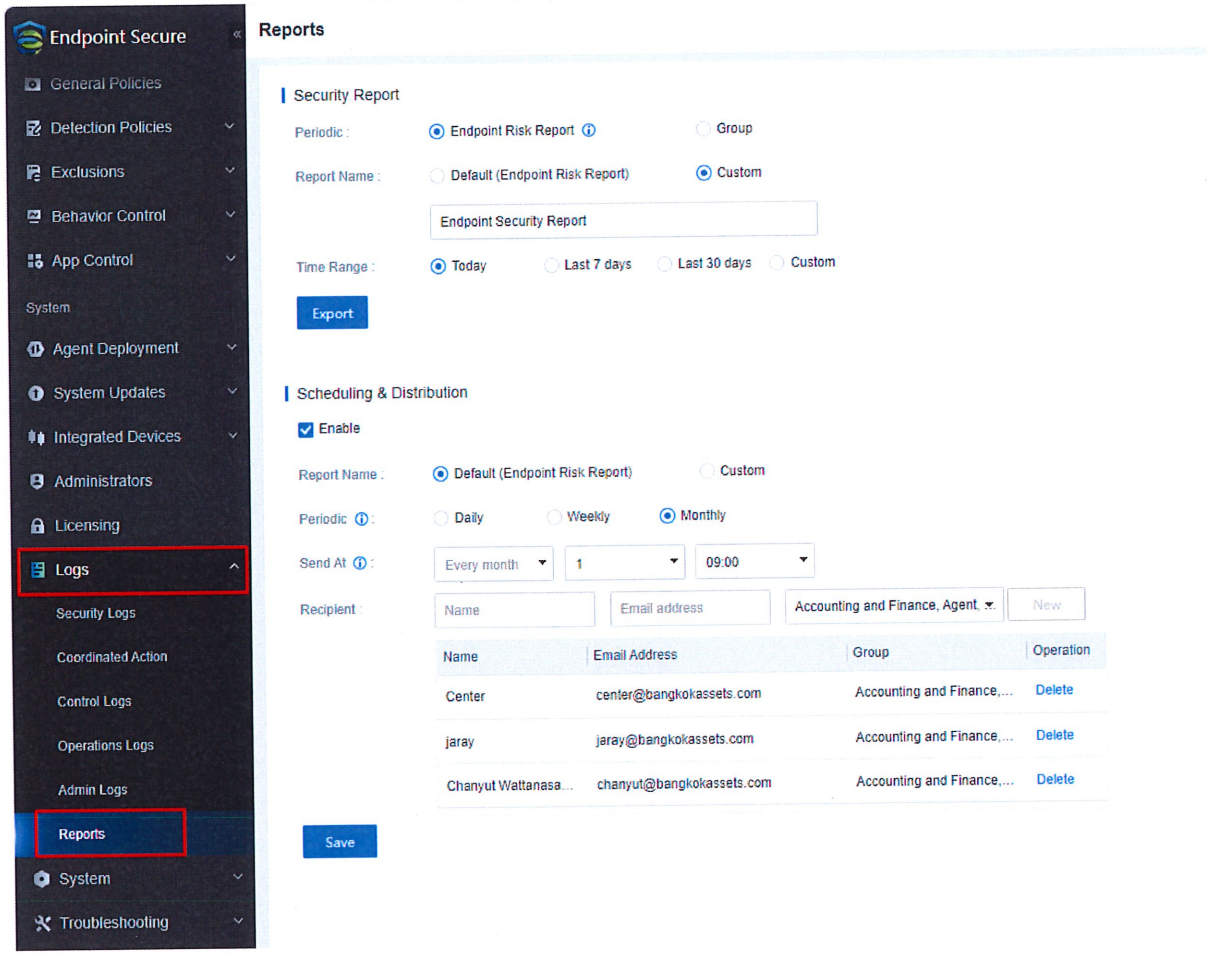
1. เปิดเว็บไซต์ https://edrsaas.sangfor.com/ กรอกอีเมล เพื่อทำการ log in



2. เปิดโทรศัพท์ IT เพื่อกรอกรหัส 2FA



3. คลิกที่ปุ่ม Logs >> Report

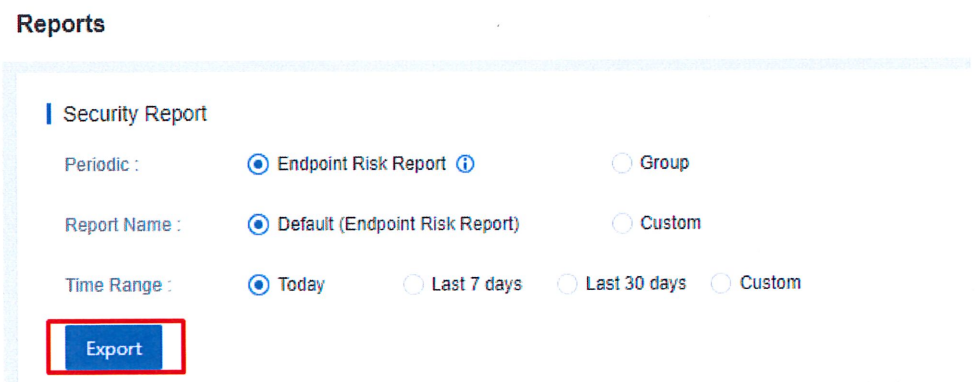


4. Reriodic : Endpoint Risk Report

   Report Name : Default (Endpoint Risk Report)

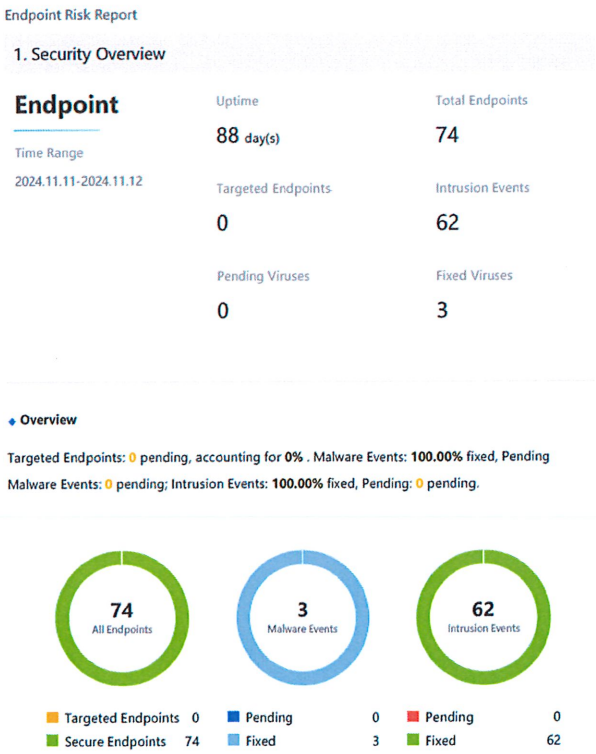
   Time Rang : Last 30 Day

5. เลือก Export เป็น PDF

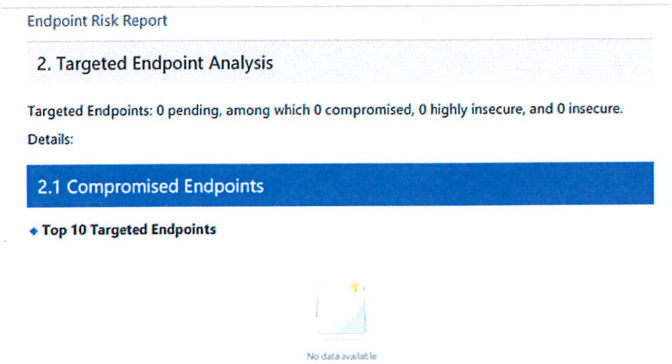


6. ตัวอย่าง Report

6.1 Security Overview แสดง Event ต่างๆที่เกิดขึ้นและรอการแก้ไขหรือได้รับการแก้ไข



6.2 Targeted Endpoint Analysis แสดงจำนวนเครื่องที่ถูก Compromised


Endpoint Risk Report

2. Targeted Endpoint Analysis

Targeted Endpoints: 0 pending, among which 0 compromised, 0 highly insecure, and 0 insecure.

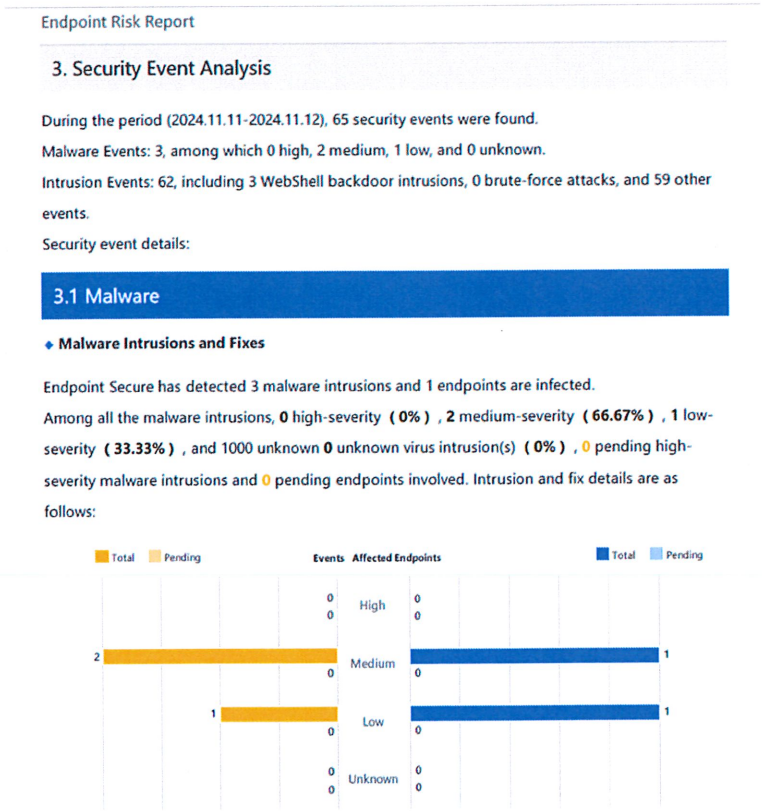
Details:

2.1 Compromised Endpoints

◆ Top 10 Targeted Endpoints

No data available

6.3 Security Event Analysis แสดงจำนวนการโจมตีที่ถูกตรวจจับได้


Endpoint Risk Report

3. Security Event Analysis

During the period (2024.11.11-2024.11.12), 65 security events were found.

Malware Events: 3, among which 0 high, 2 medium, 1 low, and 0 unknown.

Intrusion Events: 62, including 3 WebShell backdoor intrusions, 0 brute-force attacks, and 59 other events.

Security event details:

3.1 Malware

◆ Malware Intrusions and Fixes

Endpoint Secure has detected 3 malware intrusions and 1 endpoints are infected.

Among all the malware intrusions, **0** high-severity **(0%)** , **2** medium-severity **(66.67%)** , **1** low-severity **(33.33%)** , and 1000 unknown **0** unknown virus intrusion(s) **(0%)** , 0 pending high-severity malware intrusions and 0 pending endpoints involved. Intrusion and fix details are as follows:

ประวัติการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 กรกฎาคม 2566	วีรพล วุฒิเสมานานนท์
2	2.0	แก้ไขวิธีเก็บ Log	11 พฤศจิกายน 2567	ชาญยุทธ วัฒนาศักดิกุล

ลงชื่อ_____

(นาย ชาญยุทธ วัฒนาศักดิกุล)

ผู้รับผิดชอบ

วันที่ 11/11/67

ผู้อนุมัติ

ลงชื่อ_____

(นางสาว ธนิศร ธนวงศ์เกษม)

ประธานเจ้าหน้าที่เทคโนโลยีสารสนเทศ

วันที่ 11/11/67

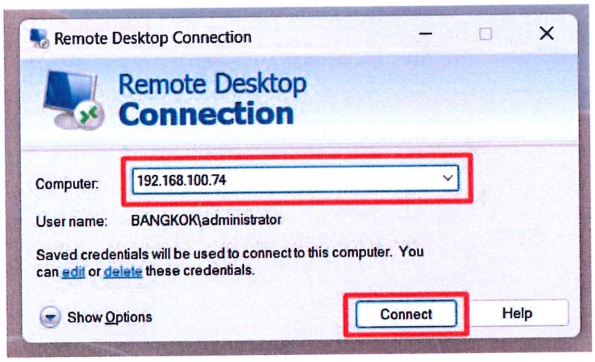
ขั้นตอนการ backup ข้อมูลของ SERVER บัญชี และการ Revert ไฟล์ 192.168.100.74

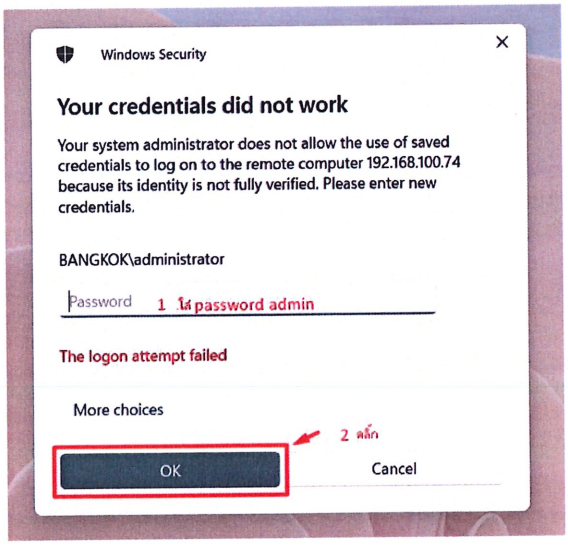
วัตถุประสงค์

เพื่อเป็นการ Back up ข้อมูลจาก Server ของบัญชี สามารถ Recovery กลับมาใช้งานได้ ในกรณีไฟล์ สูญหาย

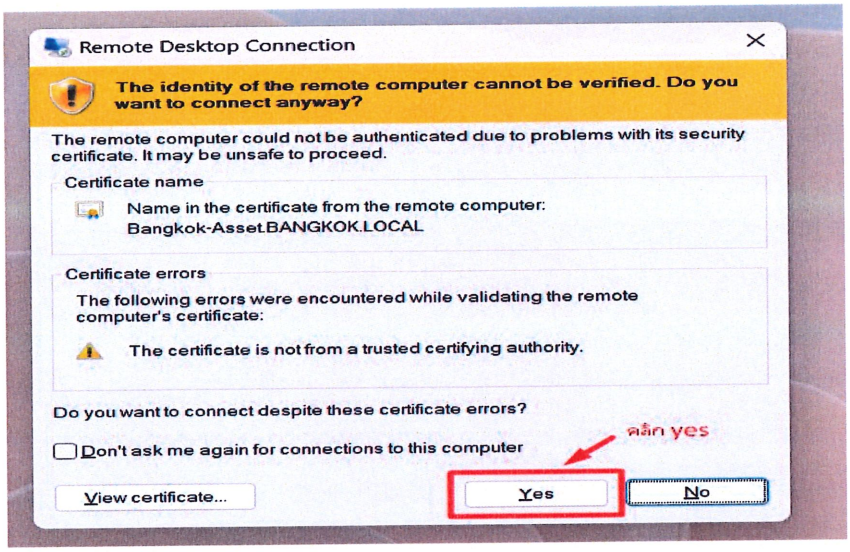
ขั้นตอนการปฏิบัติการ

1. Log in เข้า Server \\192.168.100.74 โดยใช้สิทธิ์ รหัสผ่าน Admin

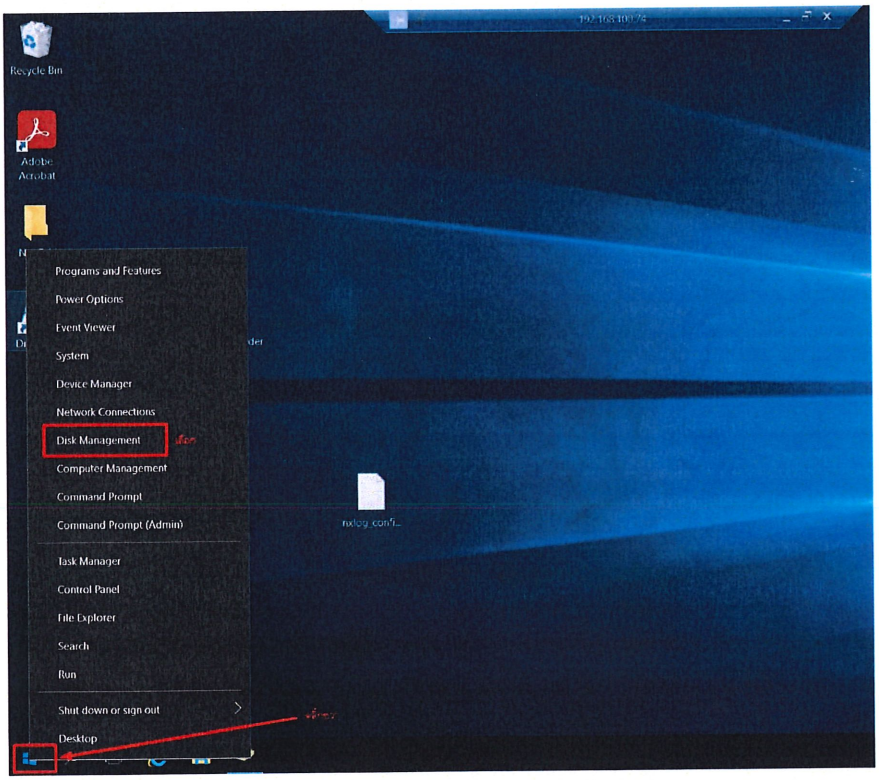




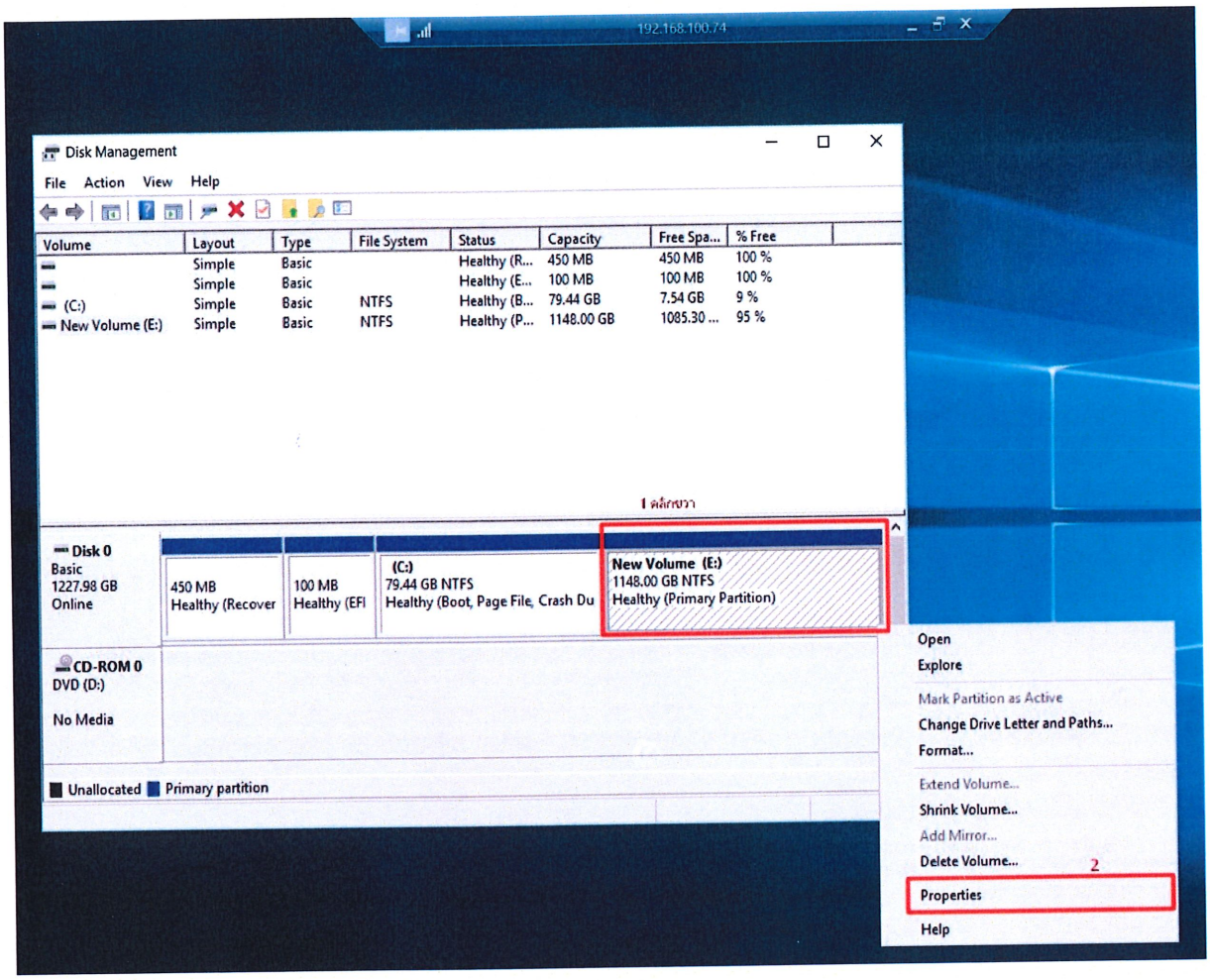
2. คลิก “yes”



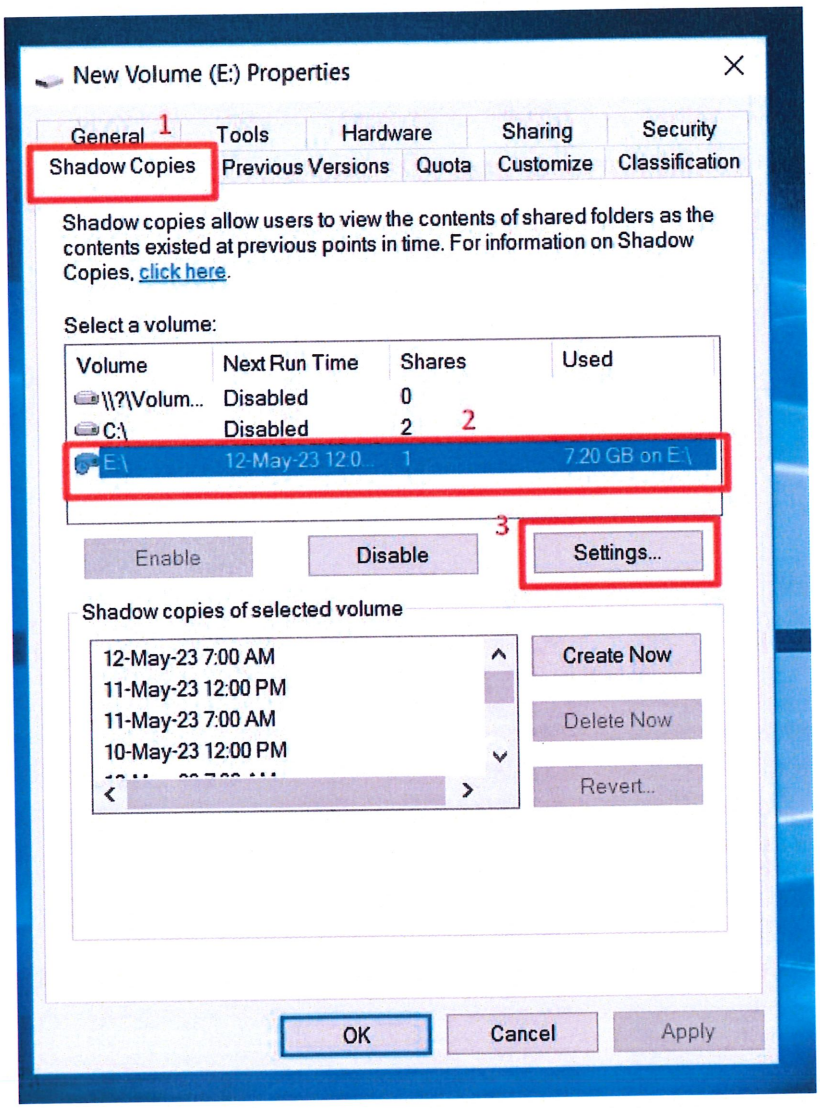
3. คลิกขวาที่ start >เลือก Disk Management



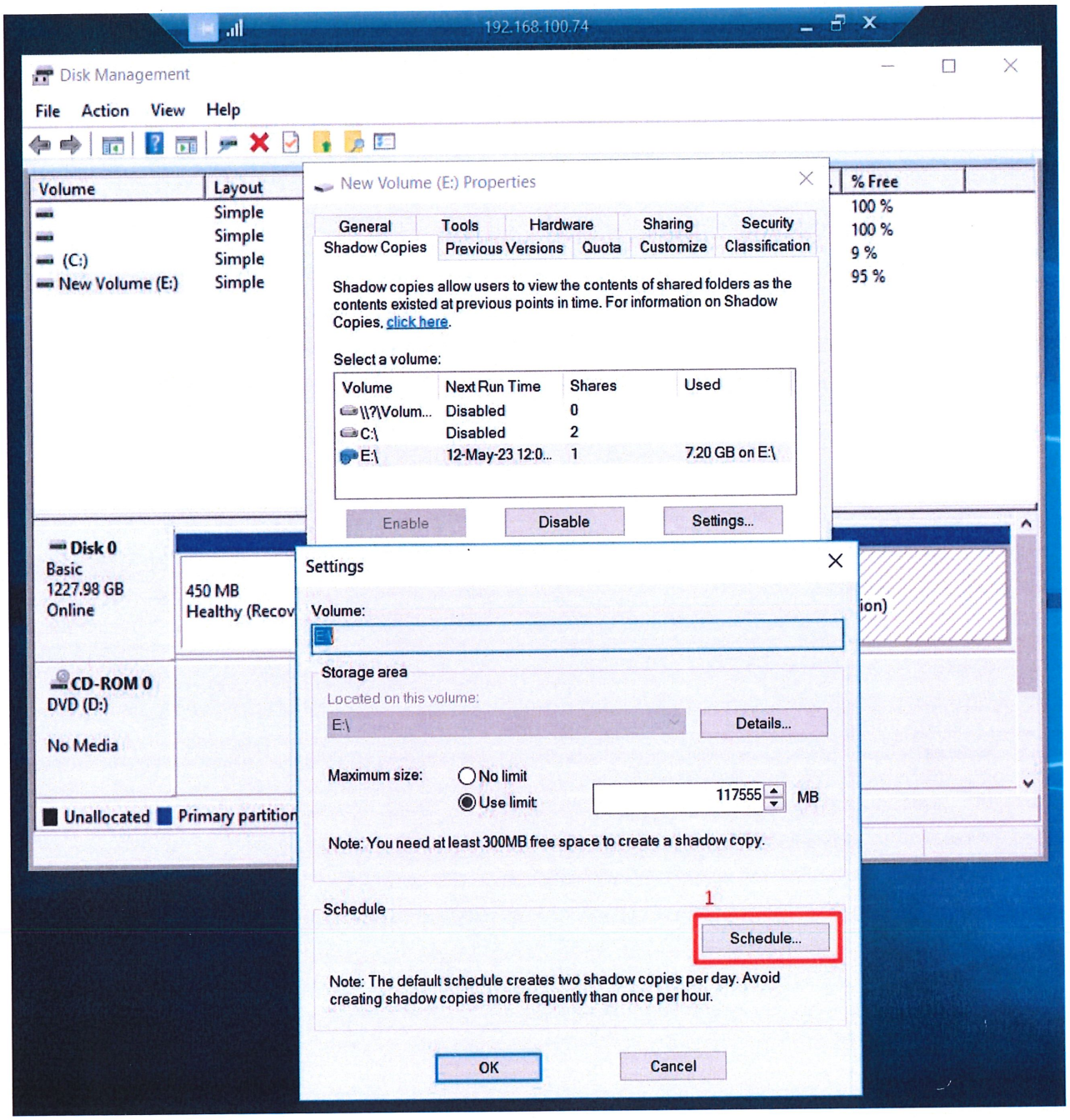
4. คลิกขวาที่ ตำแหน่งในการจัดเก็บไฟล์ New Volume (E) และเลือก Properties ตามรูป



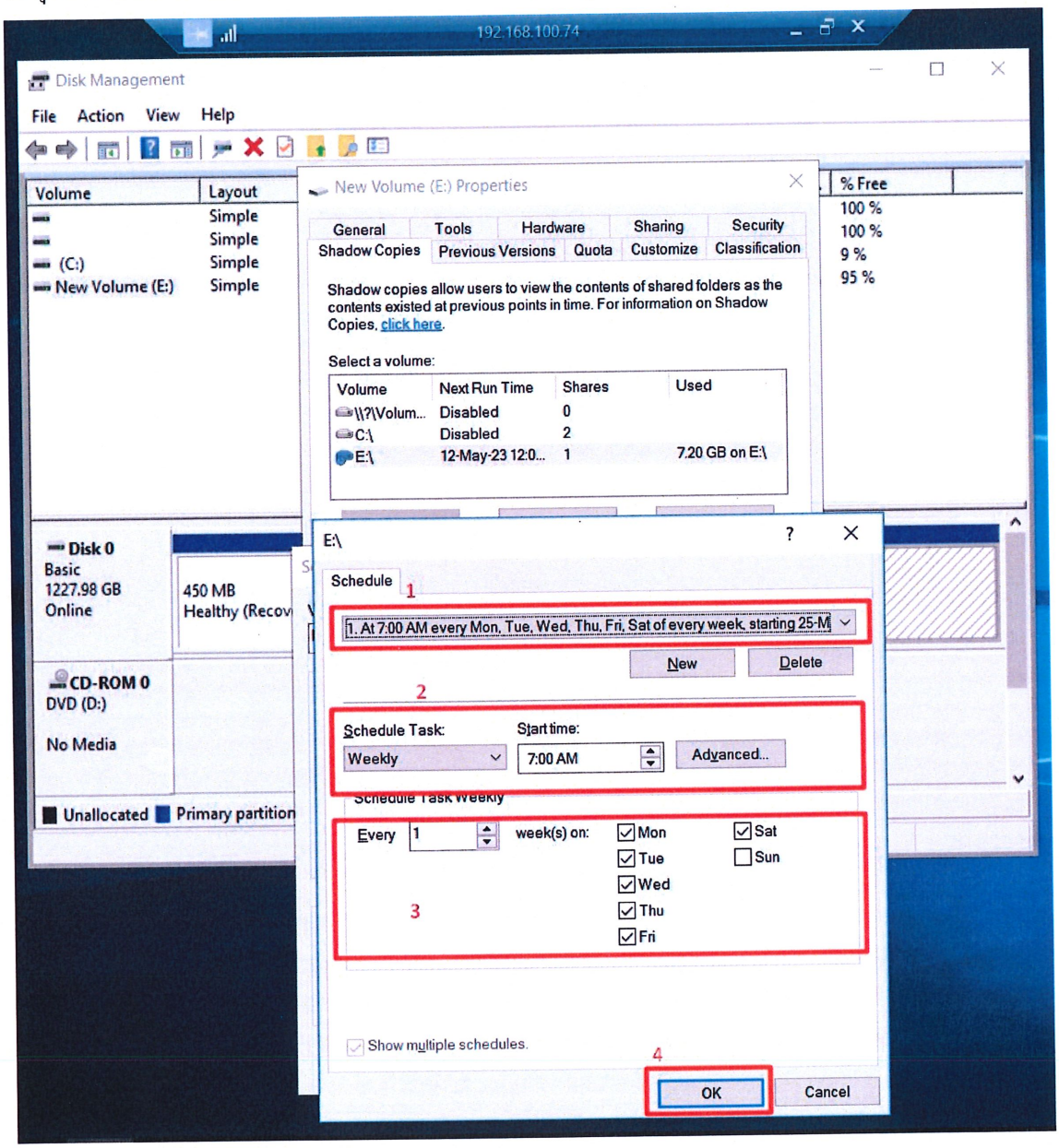
5. เลือก Shadow Copies >E:\>Setting>OK ตามภาพด้านล่าง



6. เลือก Schedule



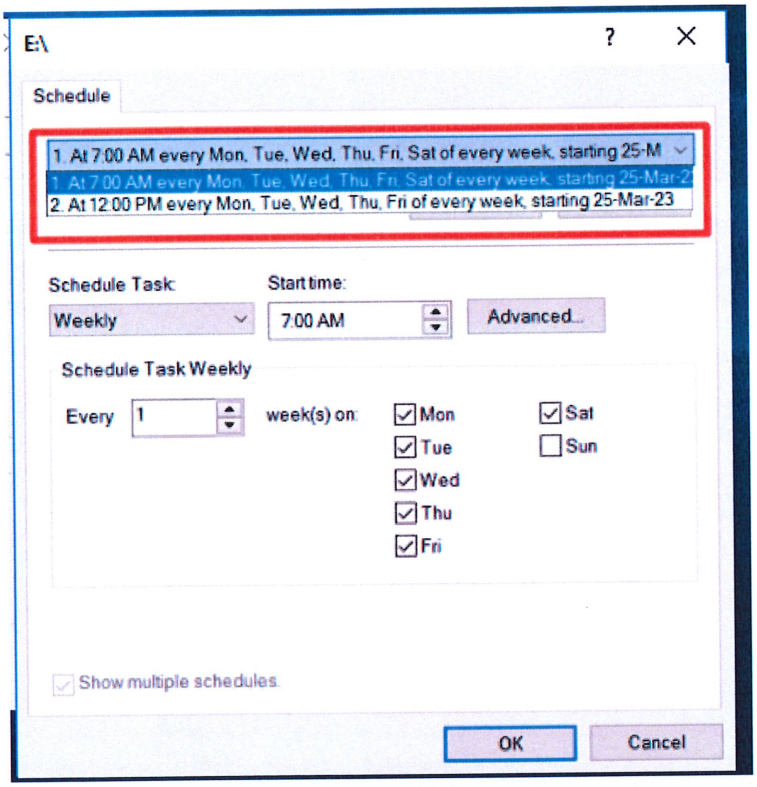
7. ระบุรายละเอียด วันและเวลา ที่ต้องการในการ Backup ข้อมูล



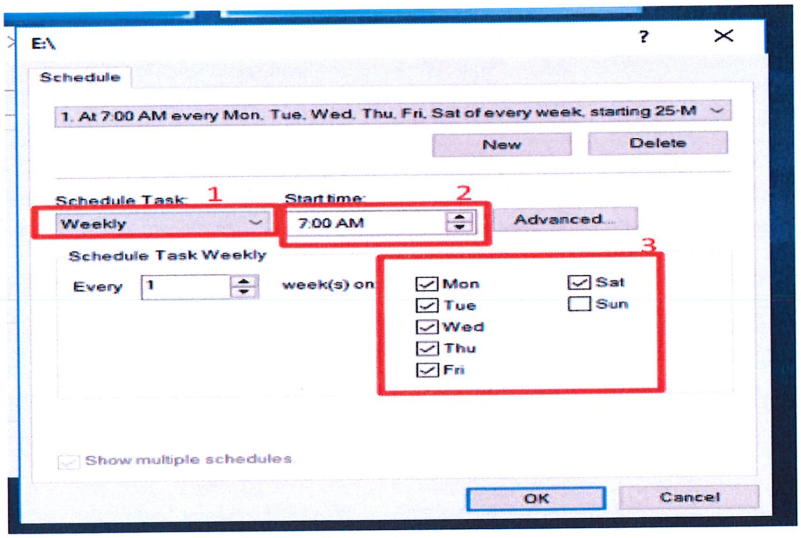
7.1 Schedule คือระบุ ช่วงเวลาที่ต้องการ Backup

ข้อ1. เริ่ม Backup เวลา 7.00 น. ของทุกวัน

ข้อ2. เริ่ม Backup เวลา 12.00 น. ของทุกวัน



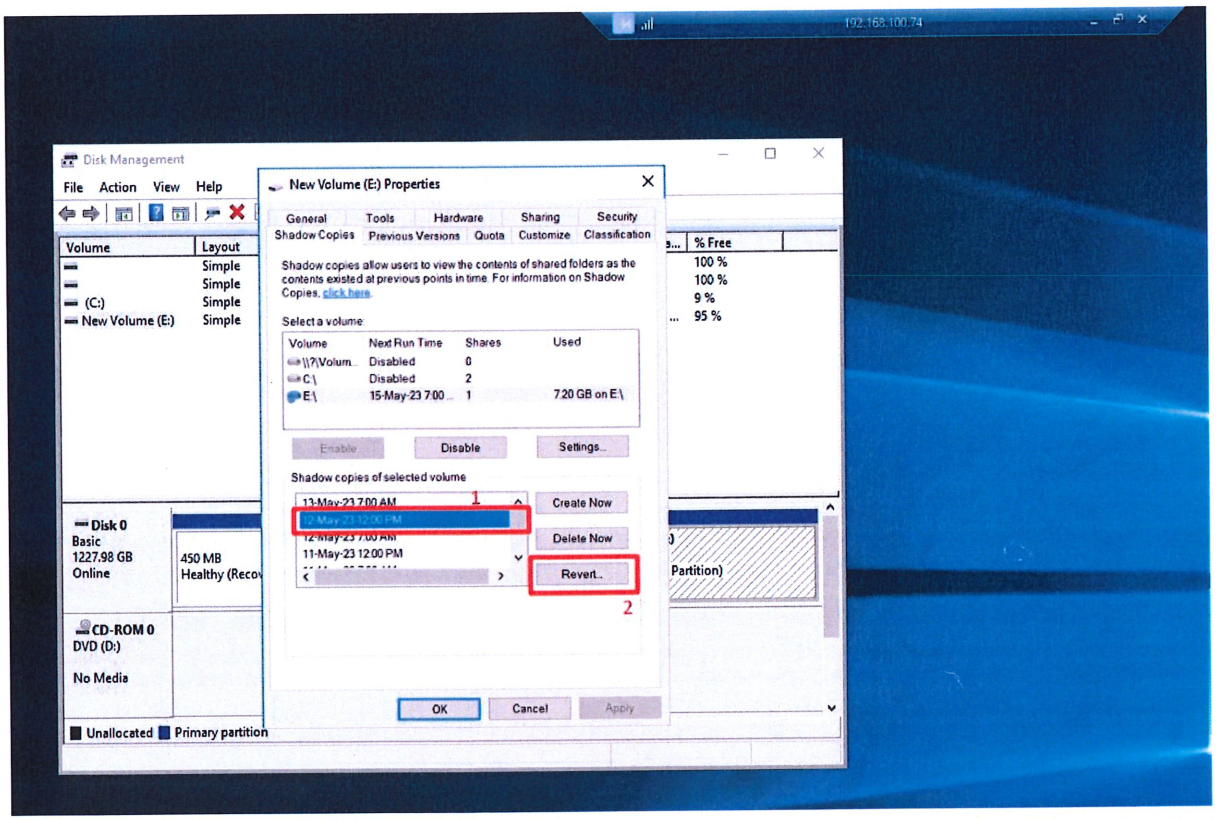
7.2 เลือกSchedule Task เป็น Weekly เลือก Start Time เป็น 7.00น.คลิก จันทร์-เสาร์



กด OK เป็นอันเสร็จสิ้น การตั้งค่า Backup

8. หากต้องการดึงข้อมูลที่ได้ทำการ Backupไว้ กลับมาใช้งานอีกครั้ง ใช้ขั้นตอนการเข้าจาก ข้อ4. จากนั้นเลือกวันและเวลาล่าสุดที่ได้ทำการ Backup ไว้ และเลือก Revert

(วิธีนี้ แนะนำให้ใช้เฉพาะในกรณีที่ไฟล์ทุกไฟล์หายหมด หรือเสียหายไม่สามารถใช้งานได้อีก ระบบจะทำการกู้ข้อมูลทุกไฟล์ ทุกFolder กลับมา)

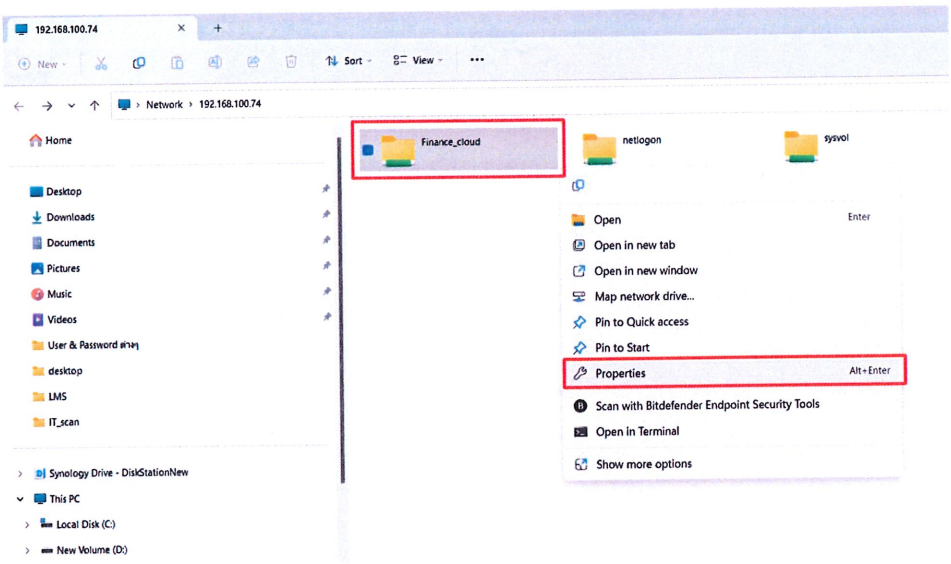


ขั้นตอนดังกล่าว ระบบจะทำการนำข้อมูลที่มา และบันทึก ทับข้อมูลปัจจุบันทันที

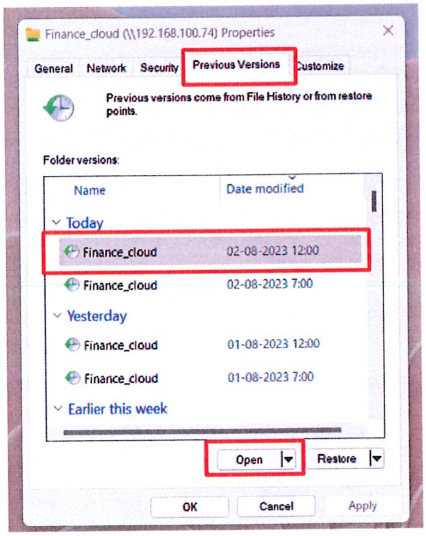
(ควรใช้เฉพาะในกรณีที่ไม่สามารถนำ ข้อมูลปัจจุบันกลับมาใช้ได้อีกแล้ว)

9. วิธีการ Revert file จากเครื่อง user โดย คลิกขวาของ folder ที่ต้องการ file > Properties

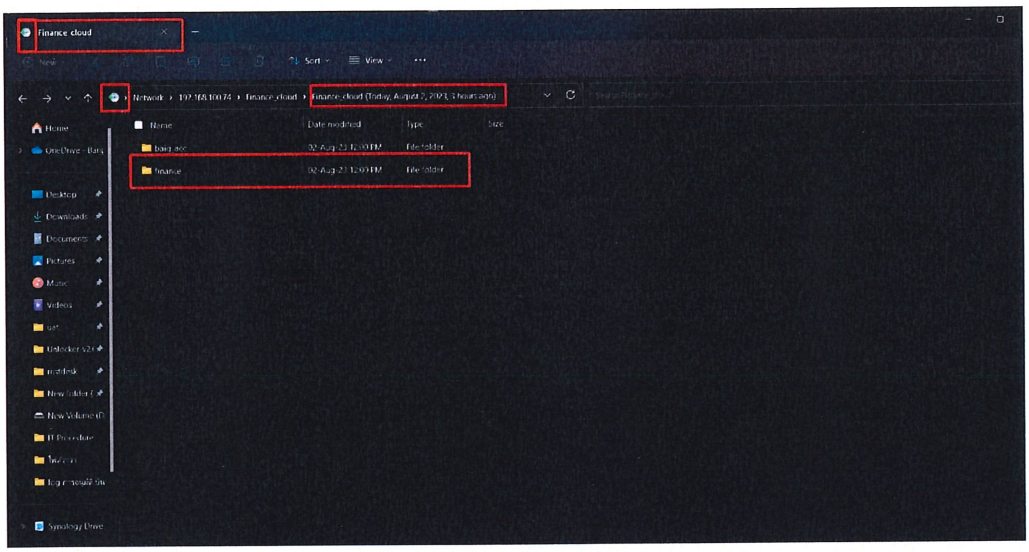
(แนะนำให้ใช้วิธีนี้เพราะ คือการเลือกแบบจำเพาะเจาะจง ของไฟล์ที่ต้องการนำกลับมาใช้งานได้)



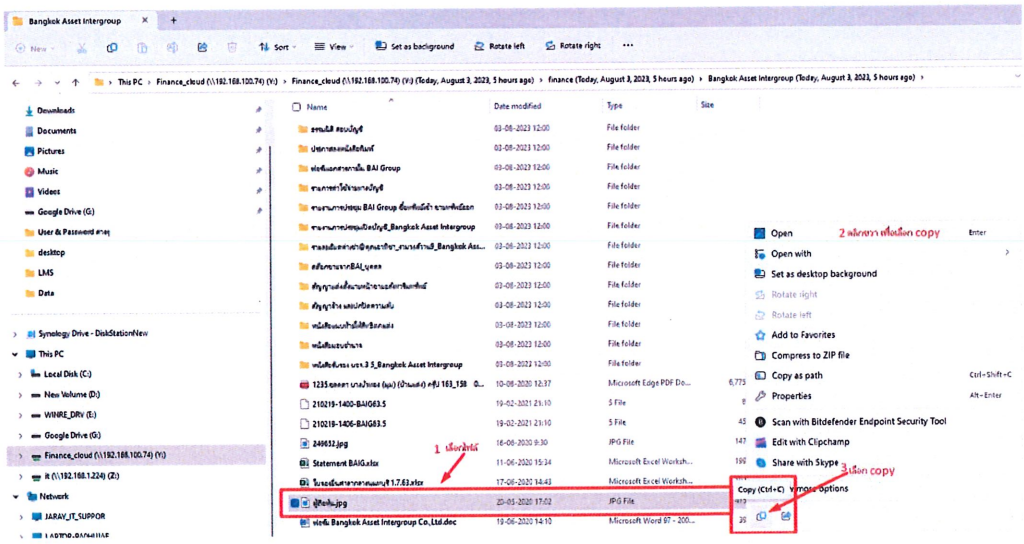
10. เลือก previous version >เลือก Open (ในกรณีนี้เครื่อง User จะต้องมีสิทธิ์เข้าถึง 192.168.100.74 เท่านั้น)



11. หลังจากเข้ามาแล้ว จะมีสัญลักษณ์  ที่แสดงถึง อยู่ระหว่างการ Revert File และสถานะของ Folder จะแสดง วันที่ ที่เราต้องการที่จะ Revert File >ต้องเลือกใช้หัวข้อ Copy เท่านั้นที่ใช้ในการดึงไฟล์ หรือ Folder นั้นๆที่ต้องการ เพื่อนำกลับไปใช้งานได้ตามปกติ

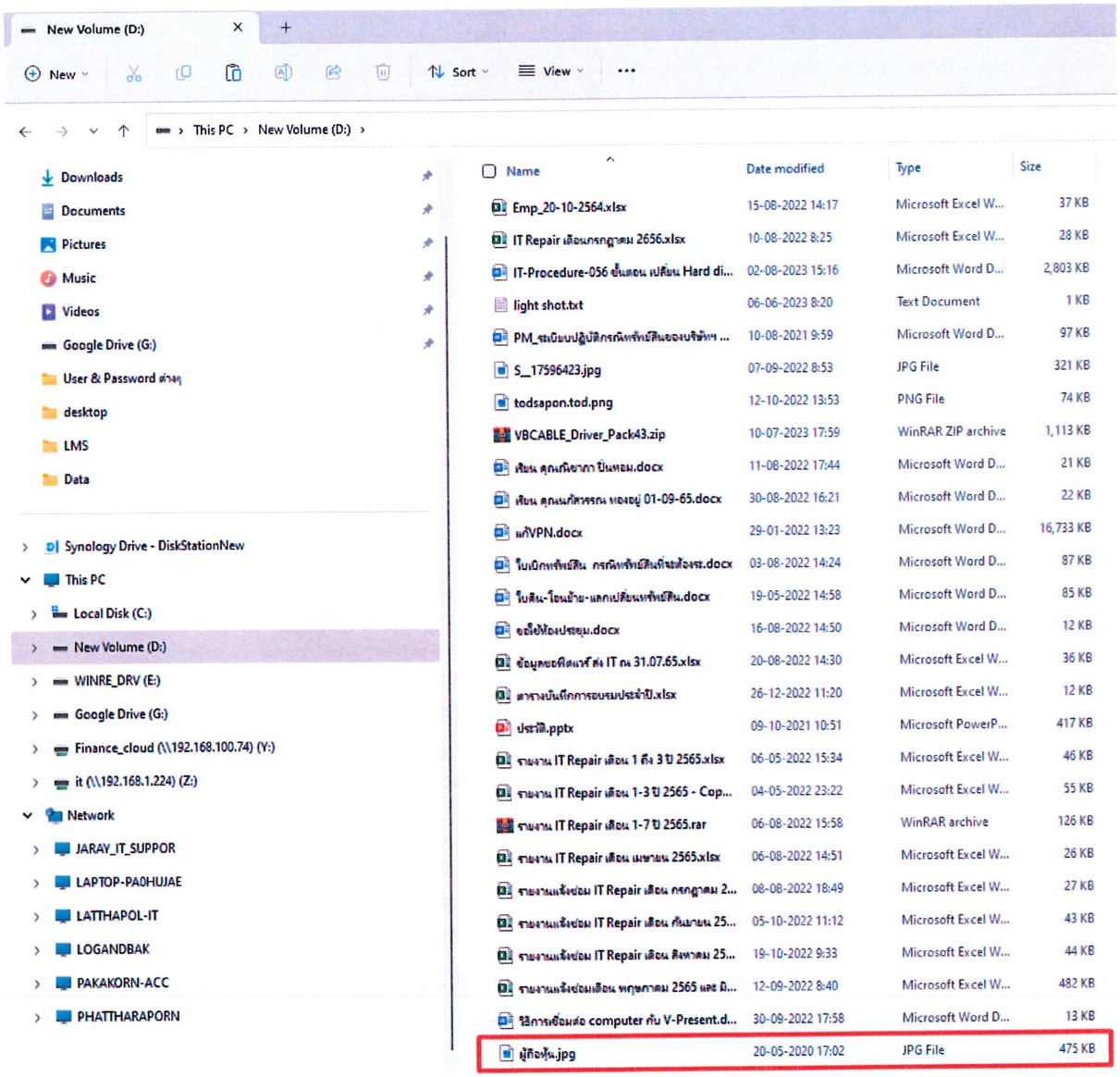


12. Copy โดยการ คลิกขวาที่ ไฟล์ต้องการนำกลับมาใช้งาน จากนั้นเลือกหัวข้อ Copy แล้วนำไปวางใน Folder ที่ต้องการได้เลย



13. ตัวอย่างไฟล์ที่ได้มาจากการ Copy แล้วนำมาวางไว้ใน ไดร์ฟ D: ของเครื่อง USER

(เพื่อให้มั่นใจว่าไฟล์ที่ได้มานั้นถูกต้อง ครับถ้วน จึงควรให้ User ดำเนินการด้วยตัวเอง)



ประวัติการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 กรกฎาคม 2566	วรวุฒิ เทพหัสดิน ณ อยุธยา

ผู้อนุมัติ

ลงชื่อ วรวุฒิ

(วรวุฒิ เทพหัสดิน ณ อยุธยา)

ผู้รับผิดชอบ

วันที่ 1/07/66.

ลงชื่อ ธนพร

(ธนพร ธนวงศ์ เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 1/07/66

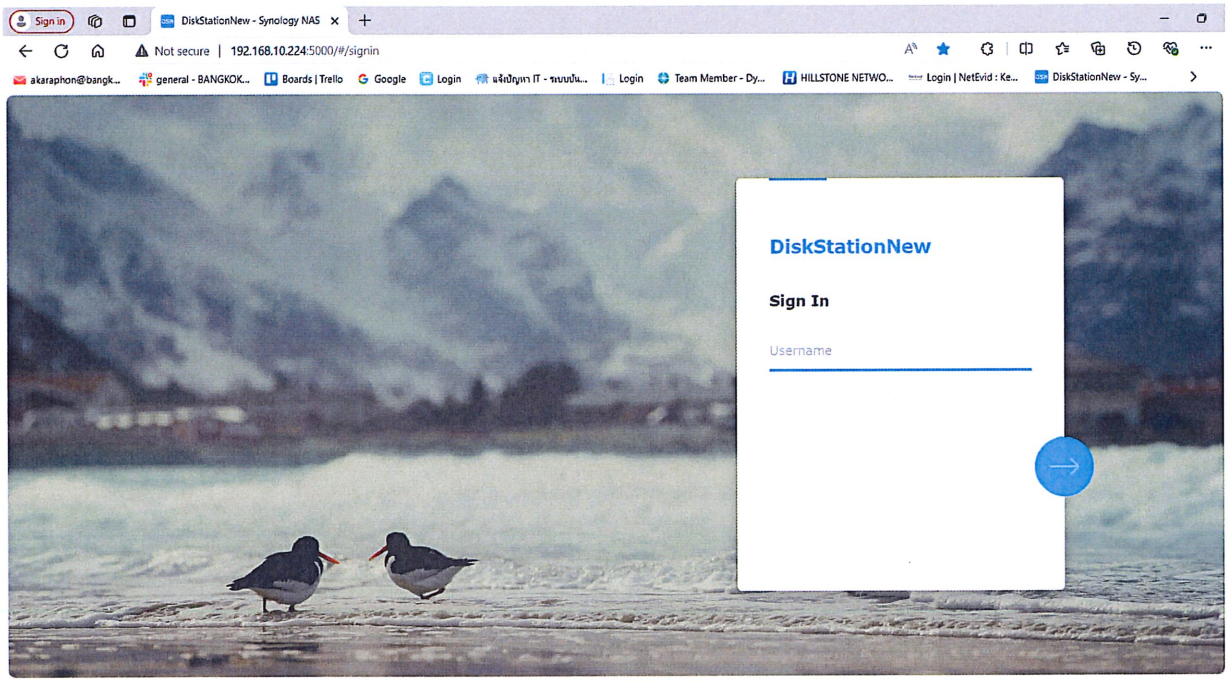
ขั้นตอนการเปลี่ยน Hard Disk Server 192.168.10.224

วัตถุประสงค์

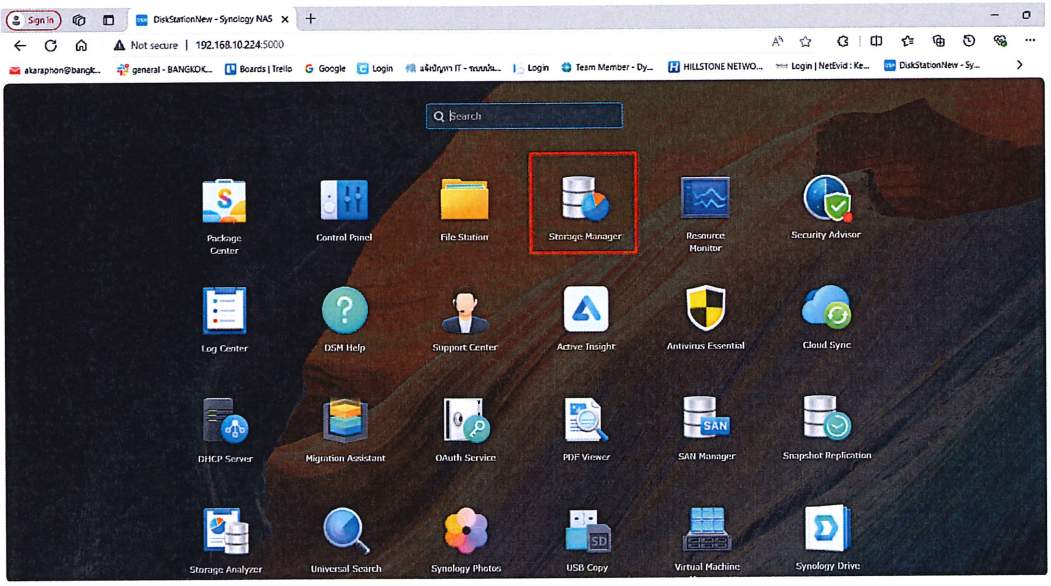
1. เพื่อเป็นการ อธิบายขั้นตอนวิธีการ เปลี่ยน Hard Disk ไดร์กลาง ในกรณี Hard Disk เดิมเสียหาย ให้สามารถกลับมาใช้งานได้อีก
2. เพื่อใช้ทดแทน Hard Disk เดิม เพื่อเพิ่มพื้นที่จัดเก็บที่เพิ่มมากขึ้น

ขั้นตอนการปฏิบัติการ

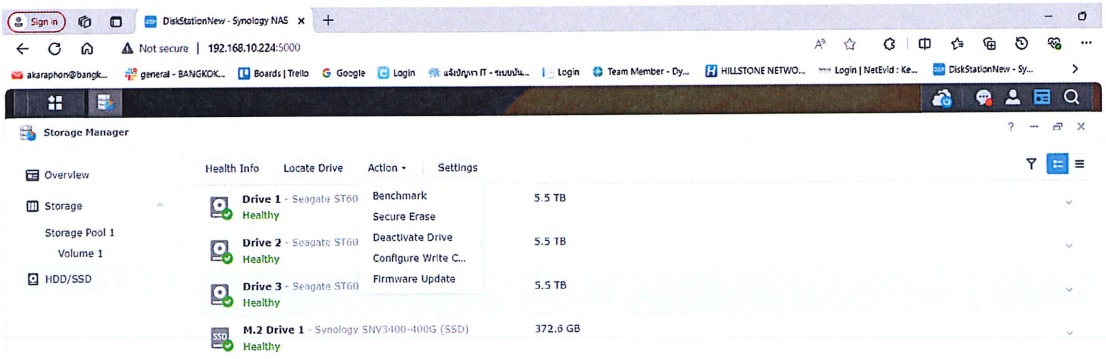
1. Log in เข้าใช้งาน server \\192.168.10.224 โดยใช้สิทธิ์ รหัสผ่าน admin



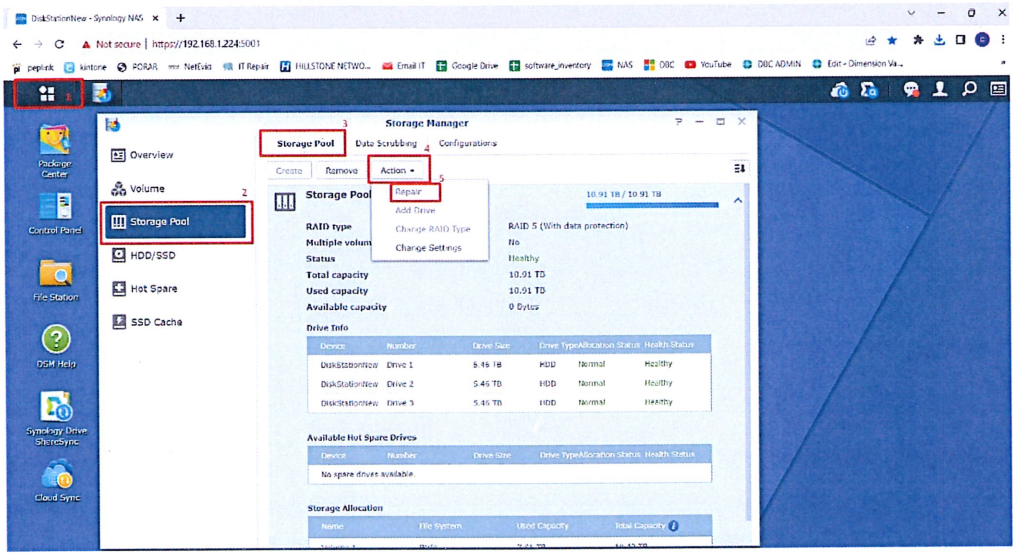
2. เลือก  Main Menu >Storage Manager



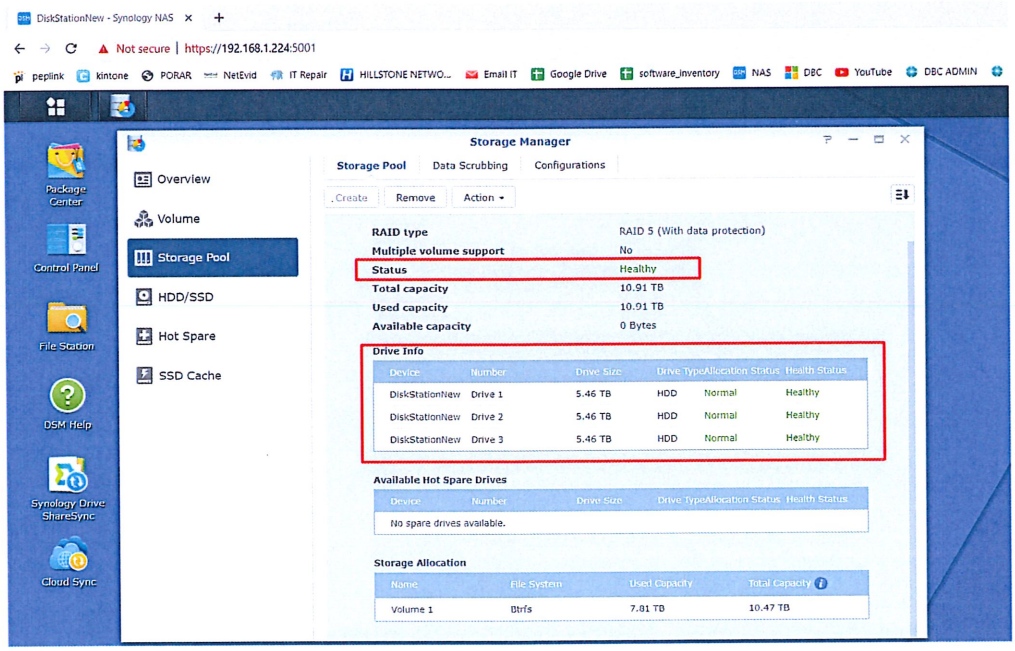
3. เลือกหัวข้อ HDD/SSD >Deactivate >เลือก Drive ที่ต้องการนำออก ให้ขึ้นแถบสีฟ้า >เลือก Action > เลือก Deactivate



4. ถอด Hard Disk Server ตัวเดิมออก แล้วทำการใส่ตัวใหม่เข้าไปแทนที่ได้เลย โดยที่ไม่ต้องปิดเครื่อง
5. หลังจาก ใส่ Hard Disk Server ตัวใหม่เสร็จเรียบร้อยแล้ว ให้ทำการคลิ้กที่รูป  >เลือก Strorage Pool >เลือก Storage Pool >เลือก Action >เลือก Repair



6. Status จะเปลี่ยนเป็น Healthy เป็นอันเสร็จสิ้นกระบวนการเปลี่ยน Hard Disk Server



ประวัติการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 กรกฎาคม 2566	วรวุฒิ เทพหัสดิน ณ อยุธยา
2	1.1	แก้ไขIP	1 กุมภาพันธ์ 2567	ชาญยุทธ วัฒนาศักดิกุล

ลงชื่อ _____

(นาย ชาญยุทธ วัฒนาศักดิกุล)

ผู้รับผิดชอบ

วันที่ 01/02/67

ผู้อนุมัติ

ลงชื่อ _____

(นางสาว ธนิศร ธนวงศ์เกษม)

ประธานเจ้าหน้าที่เทคโนโลยีสารสนเทศ

วันที่ 01/02/67

ขั้นตอนการบริหารจัดการ Email

วัตถุประสงค์

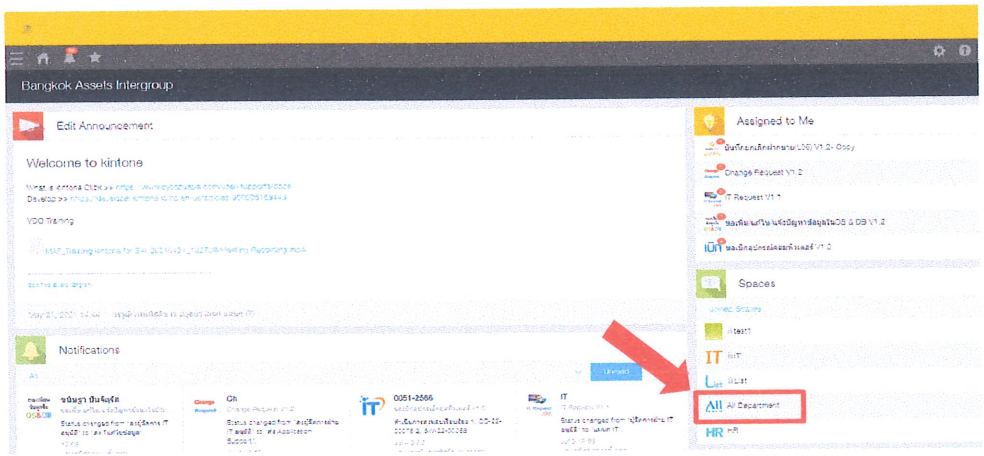
1. เพื่อเป็นการมาตรฐานการบริหารจัดการอีเมล ให้มั่นคงปลอดภัย
2. เพื่อเป็นการควบคุมการใช้งานอีเมล ให้เป็นไปตามนโยบายบริษัท และภายใต้กฎหมาย

แนวทางการปฏิบัติ

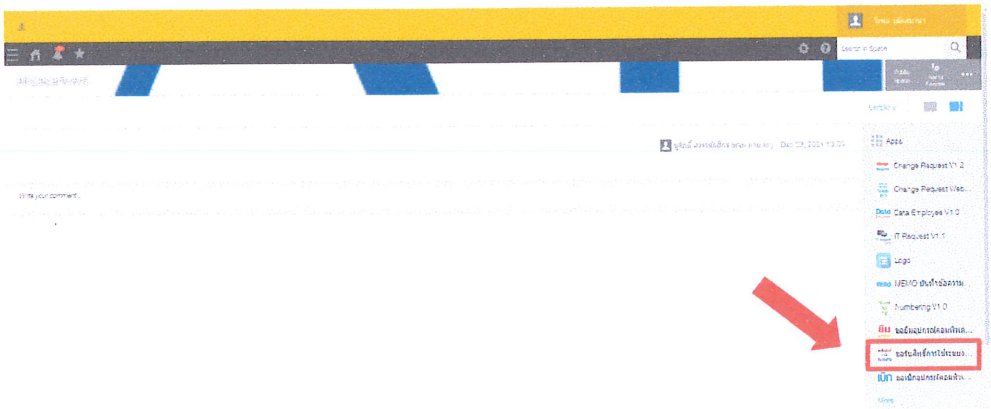
1. **ขั้นตอนการขอใช้ อีเมล**

1.1. ผู้ใช้ส่งคำร้องขอใช้งาน อีเมล ในระบบ Kintone หัวข้อ “ขอรับสิทธิ์การใช้ระบบงาน”

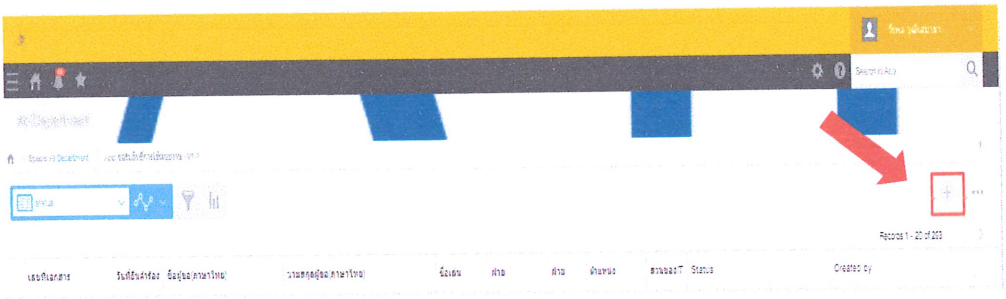
1.2. เลือก All Department



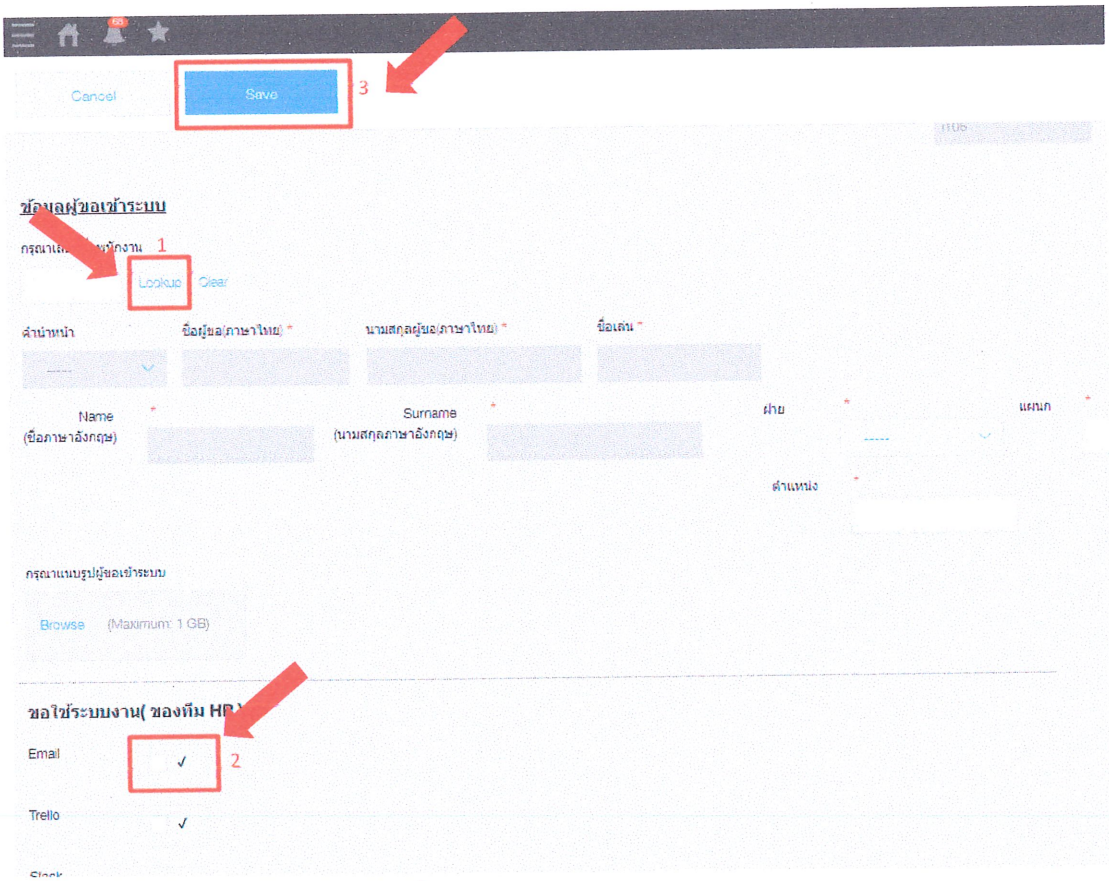
1.3. เลือก “ขอรับสิทธิ์การใช้ระบบงาน”



1.4. กดปุ่ม +



1.5. คลิกที่ Lookup เพื่อเลือกชื่อผู้ที่ต้องการขอใช้งานอีเมล (Email) คลิก ✓ แล้วกด Save



1.6. เอกสารจะถูกส่งไปยังแผนกไอที เพื่อทำการสร้าง User

2. ขั้นตอนการสร้าง อีเมล

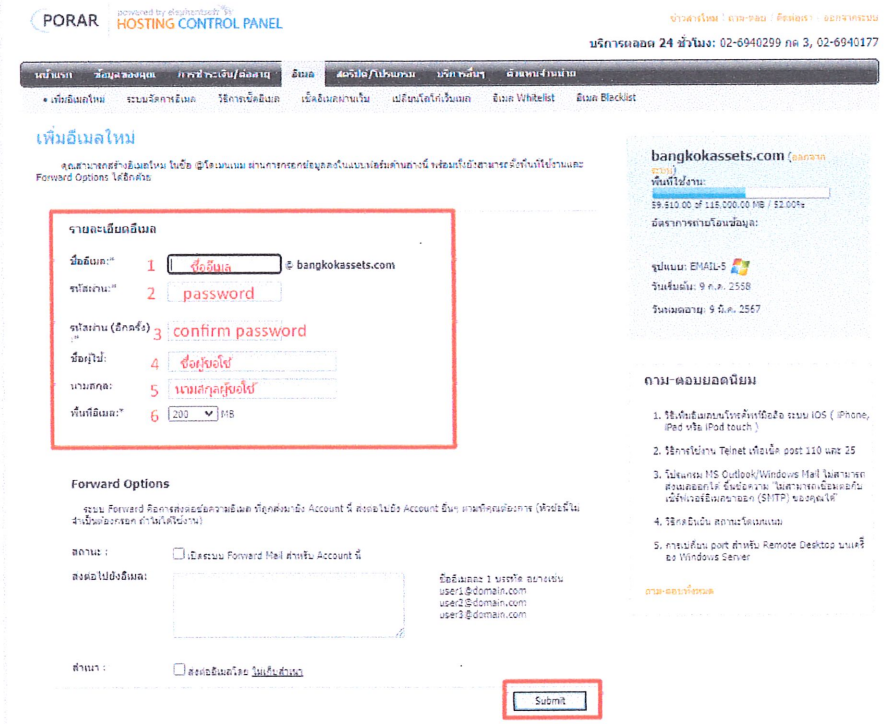
2.1. ให้เข้าไปที่ https://control.porar.com/ โดยใช้ user & password ของ admin



2.2. เลือก “อีเมล” แล้วเลือก “เพิ่มอีเมล์ใหม่”



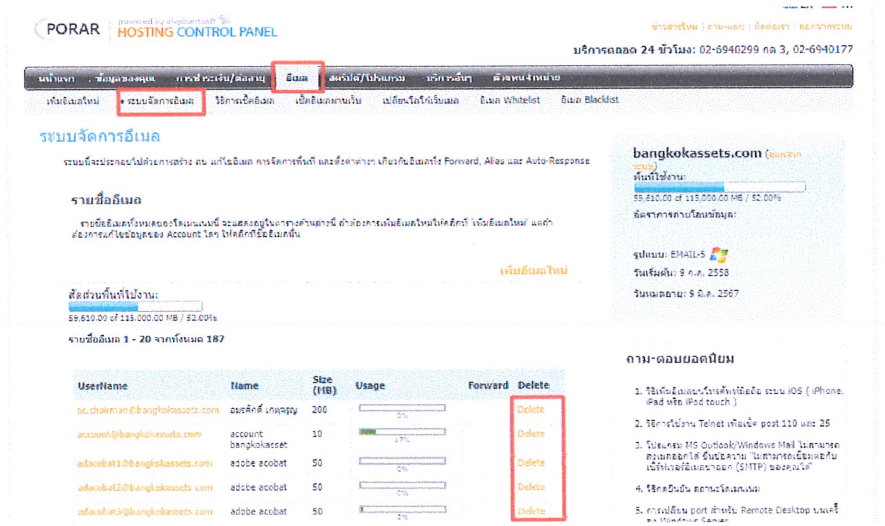
2.3. กรอกข้อมูลตามข้อ 1-5 ตามรูปด้านล่างแล้วกด Submit



3. ขั้นตอนการลบ อีเมล

3.1. ให้เข้าไปที่ https://control.porar.com/ โดยใช้ user & password ของ admin

3.2. เลือก “อีเมล” แล้วเลือก “ระบบจัดการอีเมล” ให้เลือก “Delete” ผู้ใช้งานที่ต้องการ



ประวัติการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	5 กรกฎาคม 2566	วรวุฒิ เทพหัสดิน ณ อยุธยา

ผู้อนุมัติ

ลงชื่อ วรวุฒิ

(วรวุฒิ เทพหัสดิน ณ อยุธยา)

ผู้รับผิดชอบ

วันที่ 5 กรกฎาคม 2566

ลงชื่อ [illegible]

([illegible])

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 5 กรกฎาคม 2566

ขั้นตอนการบริหารจัดการ WiFi

วัตถุประสงค์

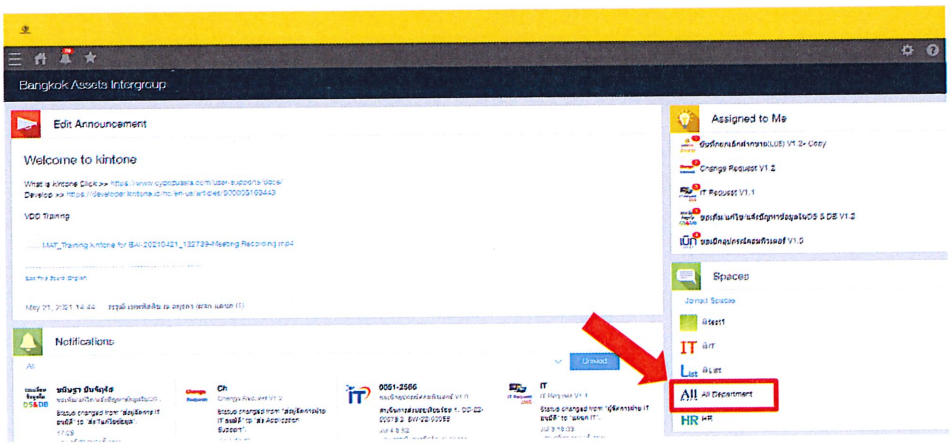
1. เพื่อเป็นมาตรฐานในการใช้งาน WiFi ของบริษัท ให้มีความมั่นคงและปลอดภัย
2. เพื่อเป็นการควบคุมการใช้งาน WiFi ให้เป็นไปตามนโยบายบริษัท และภายใต้กฎหมาย

แนวทางการปฏิบัติ

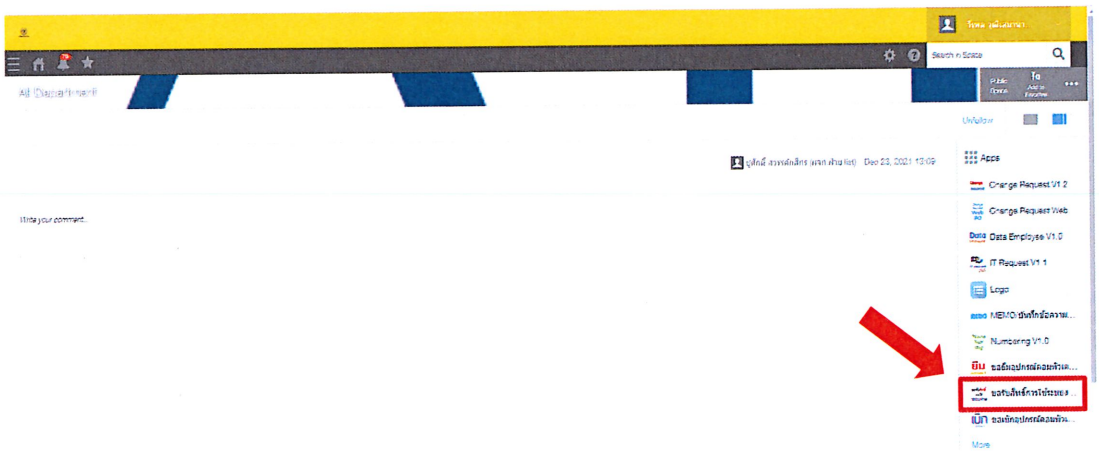
1. ขั้นตอนการขอใช้ WiFi

1.1. ผู้ใช้ส่งคำร้องขอใช้งาน WiFi ในระบบ Kintone หัวข้อ “ขอรับสิทธิการใช้ระบบงาน”

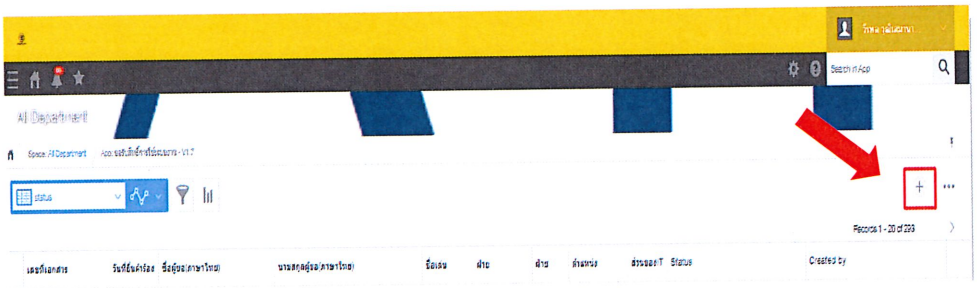
1.2. เลือก All Department



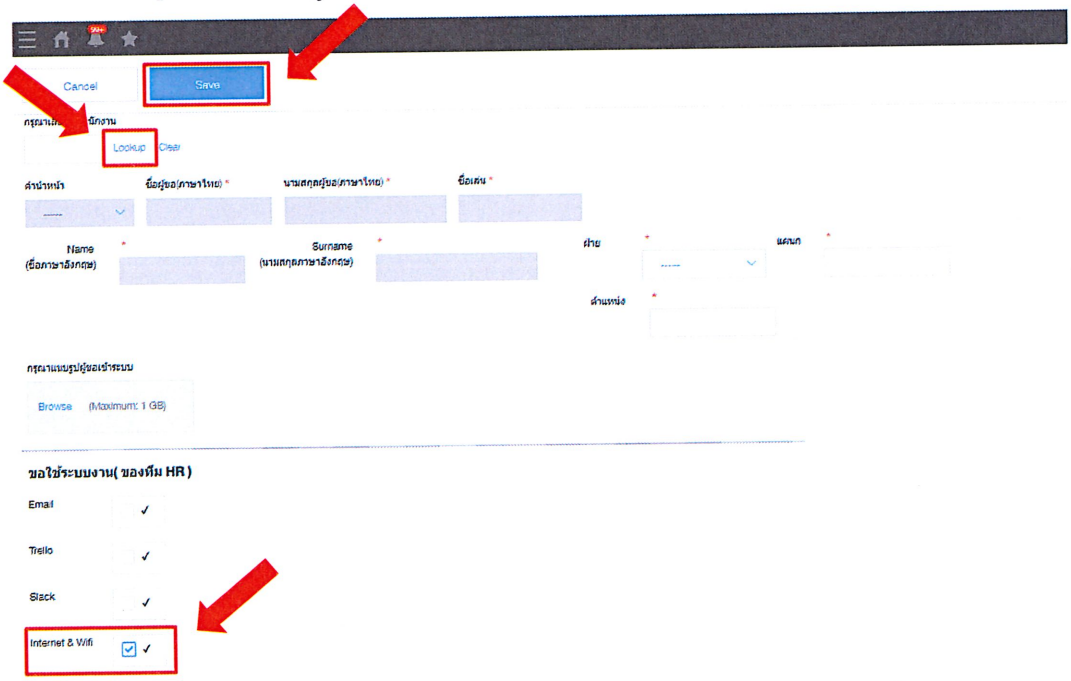
1.3. เลือก “ขอรับสิทธิ์การใช้ระบบงาน”



1.4. กดปุ่ม + มุมบนทางขวามือ



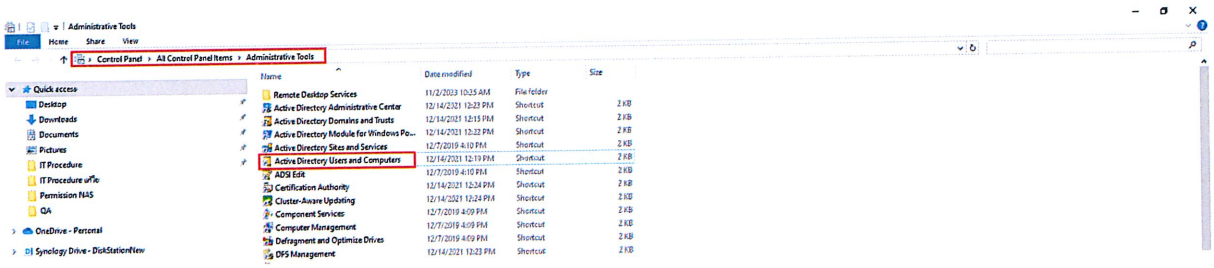
1.5. คลิกที่ Lookup เพื่อเลือกชื่อผู้ที่ต้องการขอใช้งาน WiFi คลิก ✓ ที่ (Internet&WiFi) แล้วกด Save



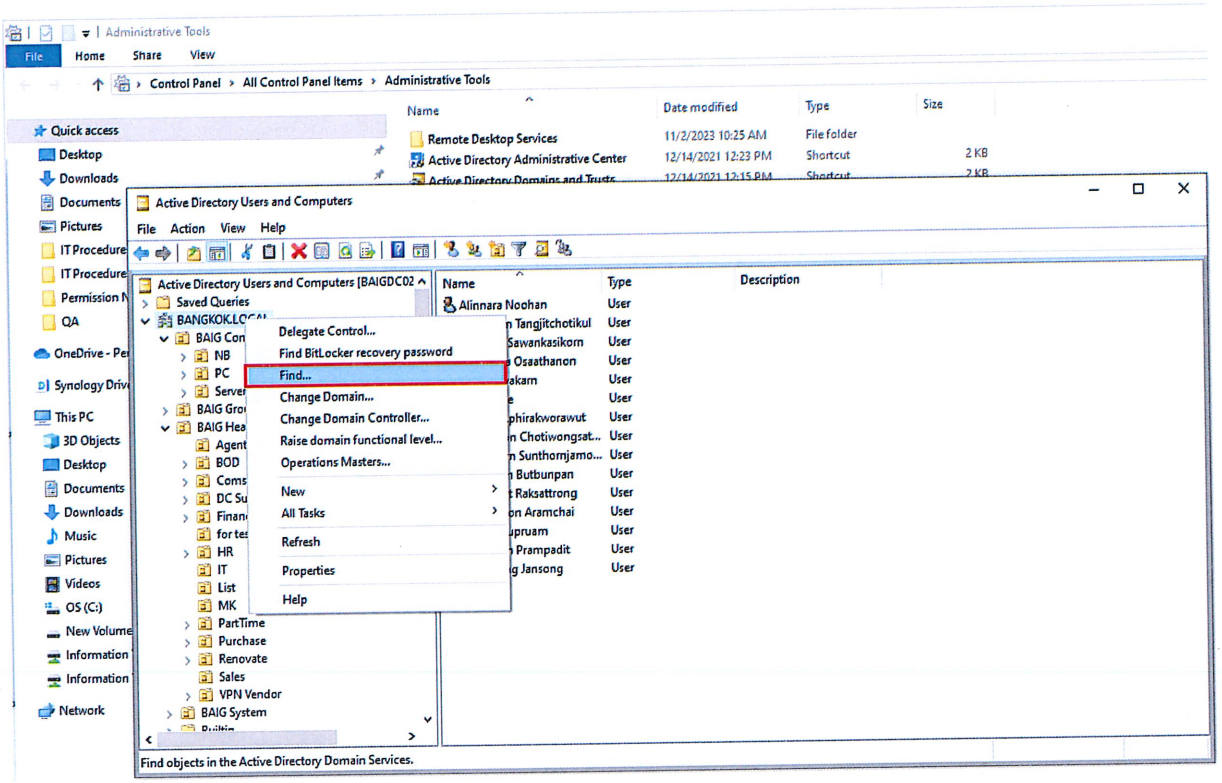
1.6. เอกสารจะถูกส่งไปยังแผนกไอที เพื่อทำการสร้าง User & Password ให้สำหรับผู้ที่ต้องการเข้าใช้งาน WiFi

2. ขั้นตอนการเพิ่มสิทธิ์ใช้งาน WiFi

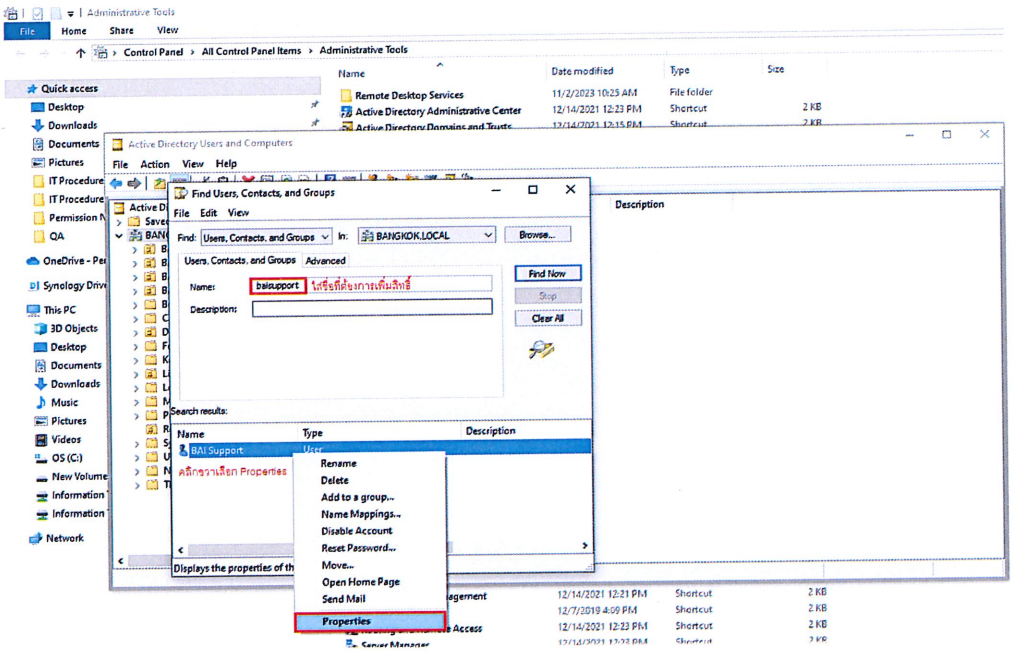
2.1. เปิด Active Directory User and Computer



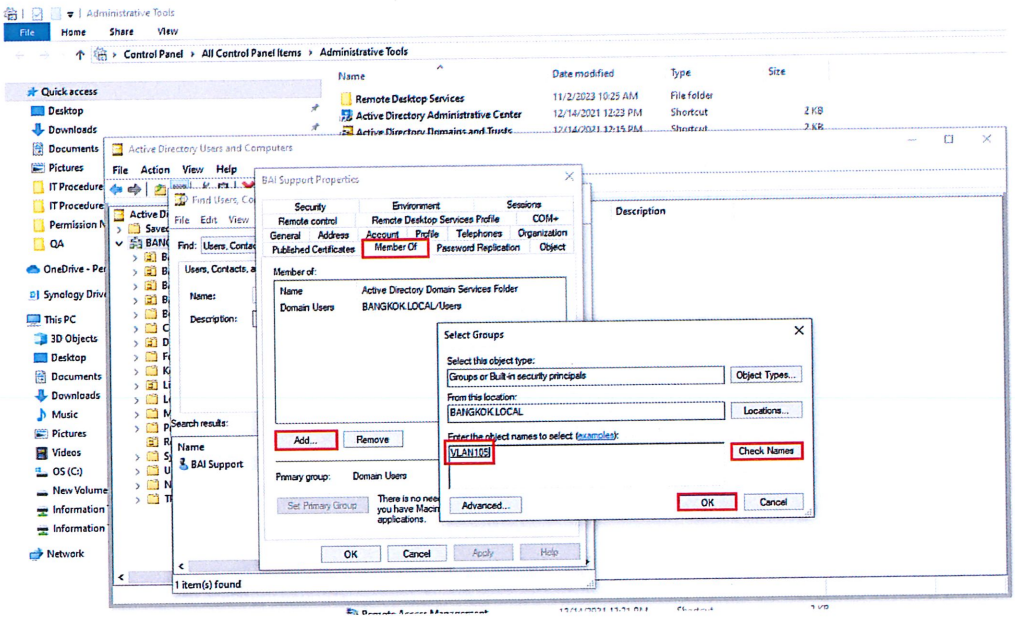
2.2. ค้นหา Account ที่ต้องการ



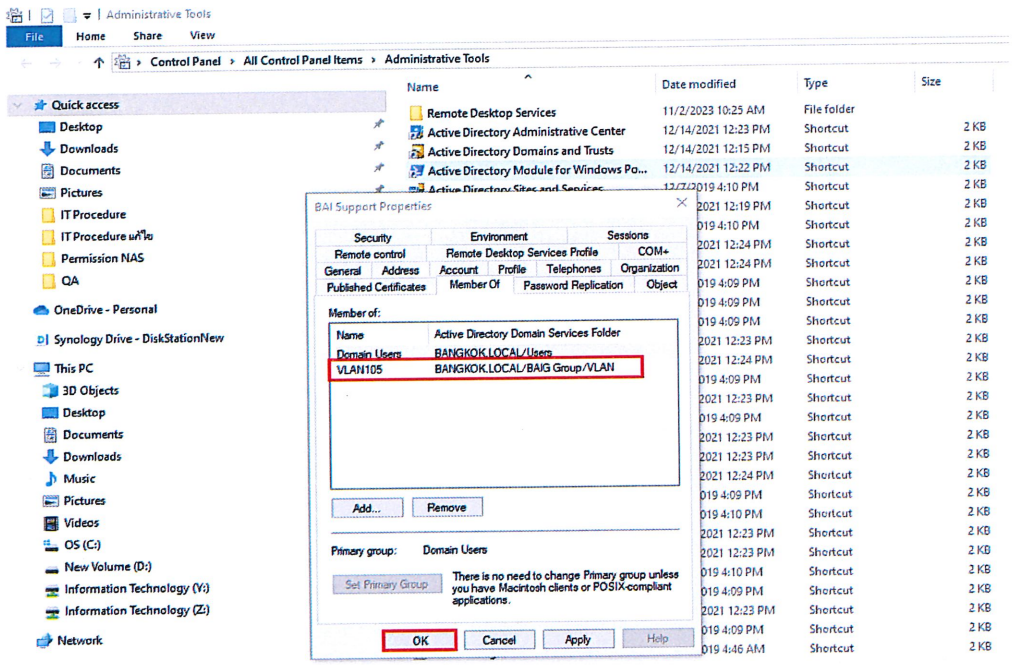
2.3. ใส่ชื่อที่ต้องการค้นหา



2.4. เลือก Member Of >> Add >> ระบุ VLAN ตามแผนก >> Check Name >> OK

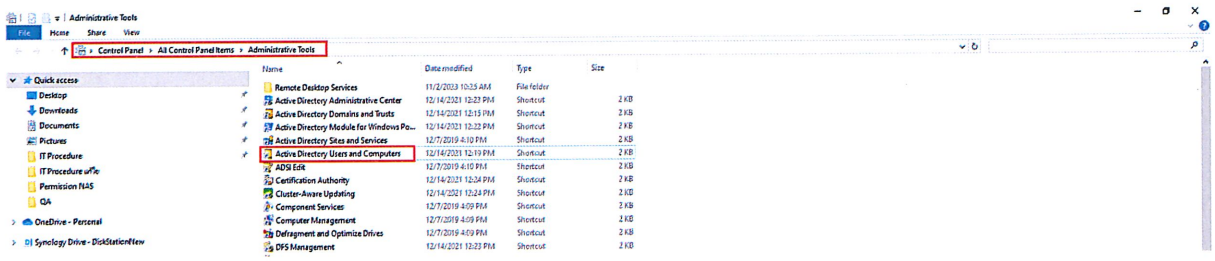


2.5. VLAN ที่เพิ่มจะอยู่ในนช่อง Member Of และ กด OK เพื่อยืนยัน

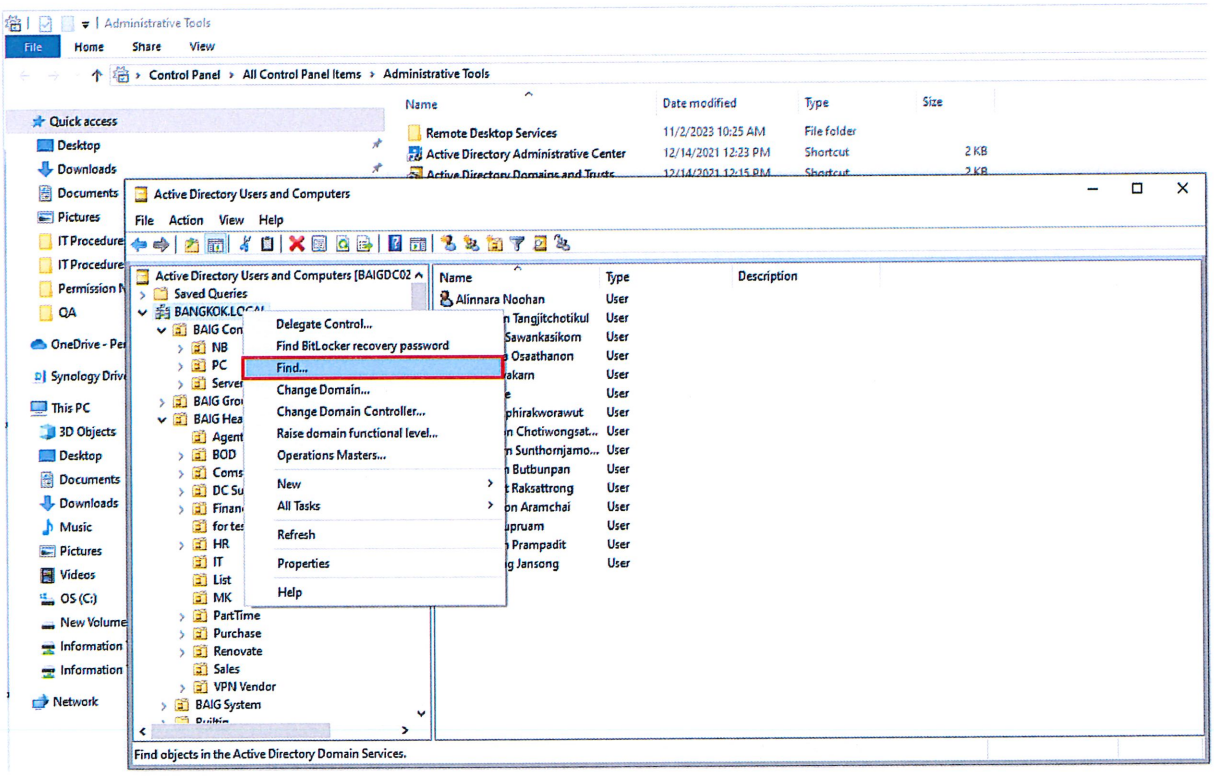


3. ขั้นตอนการลบสิทธิ์เข้าใช้งาน WiFi

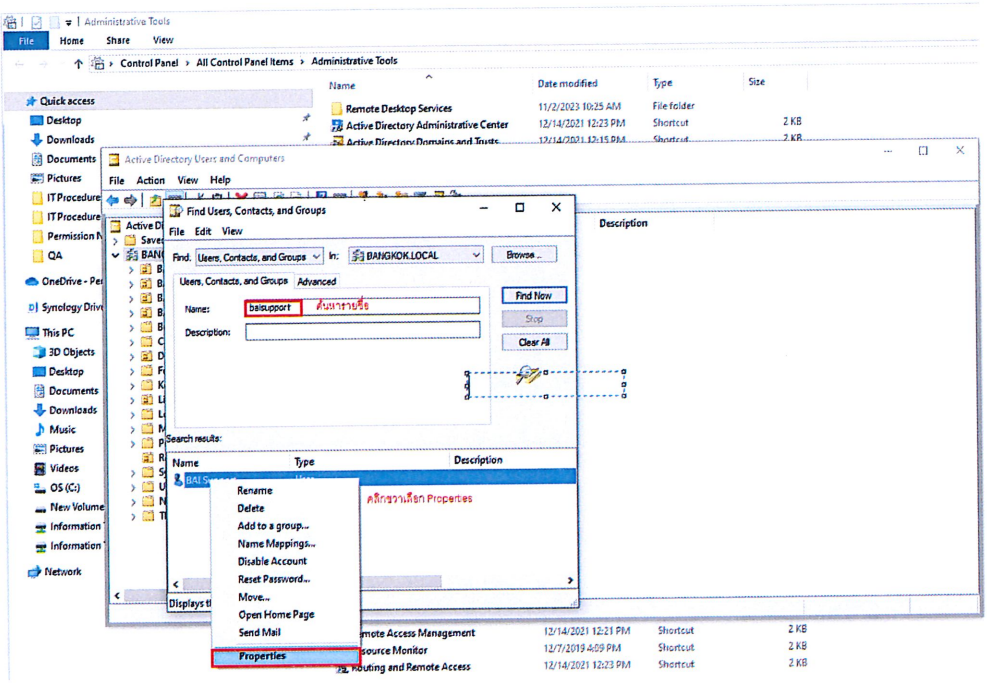
3.1. เปิด Active Directory User and Computer



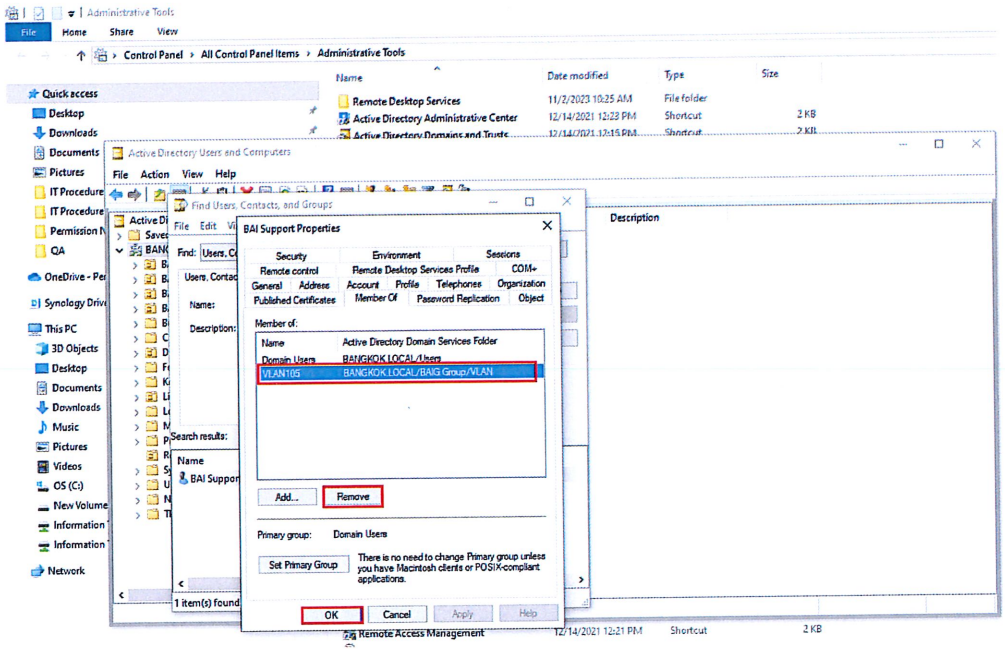
3.2. ค้นหา Account ที่ต้องการ



3.3. ใส่ชื่อที่ต้องการค้นหา



3.4. เลือก VLAN >> Remove >> OK เพื่อยืนยัน



ประวัติการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 สิงหาคม 2566	วรวุฒิ เทพหัสดิน ณ อยุธยา
2	2.0	ปรับเปลี่ยนวิธีเพิ่มสิทธิ์การใช้งาน	1 กุมภาพันธ์ 2567	ชาญยุทธ วัฒนาศักดิกุล

ลงชื่อ 

(นาย ชาญยุทธ วัฒนาศักดิกุล)

ผู้รับผิดชอบ

วันที่ 01/02/67

ผู้อนุมัติ

ลงชื่อ 

(นางสาว ธนิศร ธนวงศ์เกษม)

ประธานเจ้าหน้าที่เทคโนโลยีสารสนเทศ

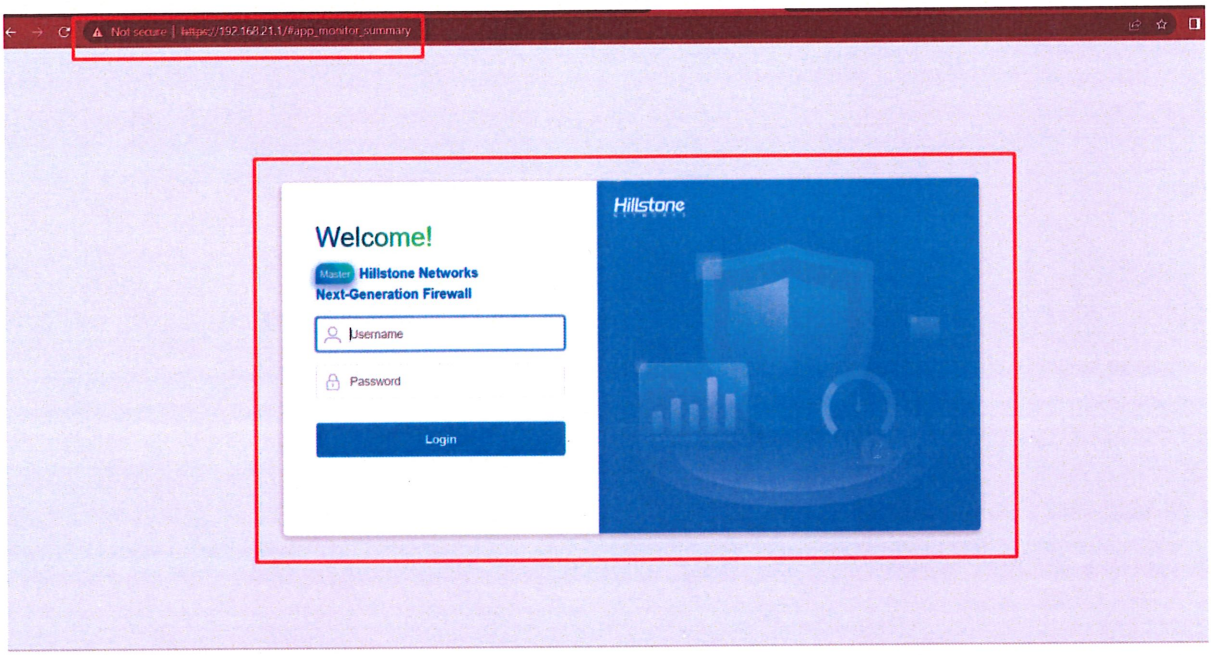
วันที่ 01/02/67

ขั้นตอน

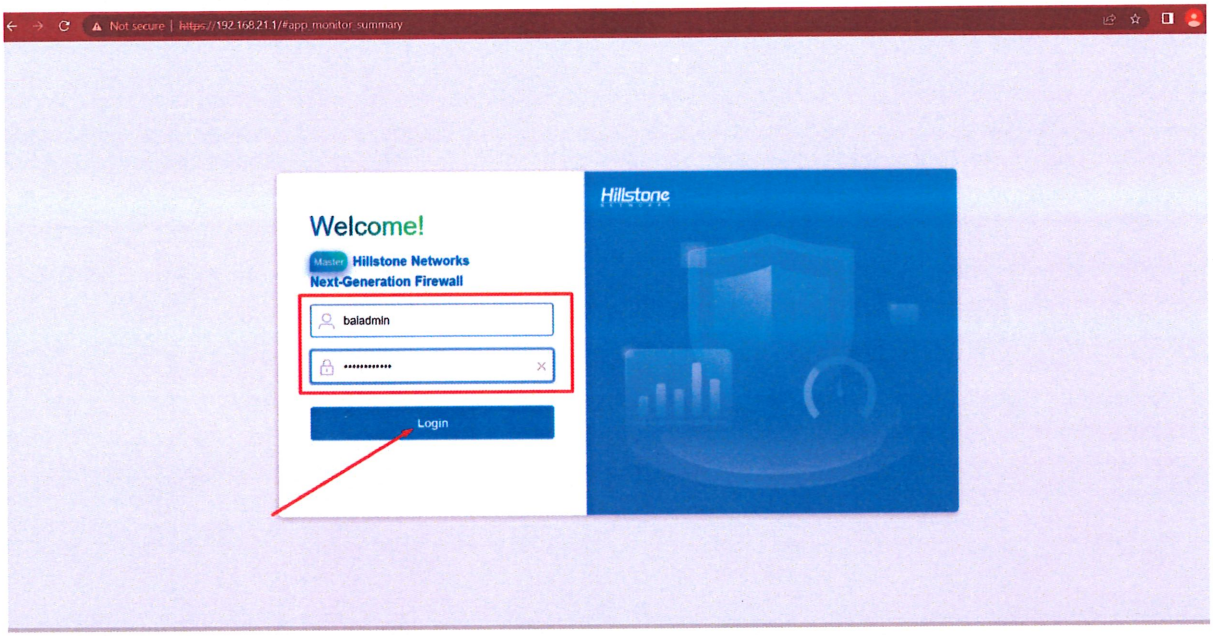
วัตถุประสงค์

1. เพื่อเป็นทดสอบสถานะทำงานของอุปกรณ์ให้พร้อมใช้งานเสมอ
2. เพื่อเป็นการตรวจสอบสถานะของ เน็ตเวิร์ค ให้พร้อมใช้งานเสมอ

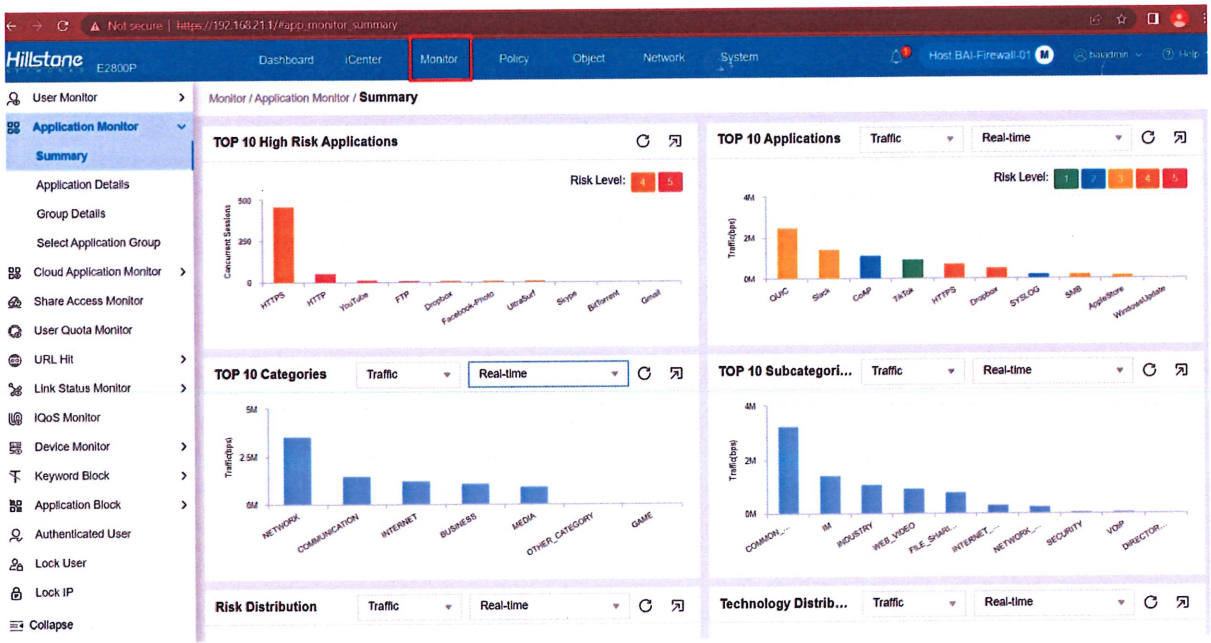
1.เข้าหน้าเว็บไซต์ https://192.168.21.1



2. ทำการ Log in เข้าระบบ



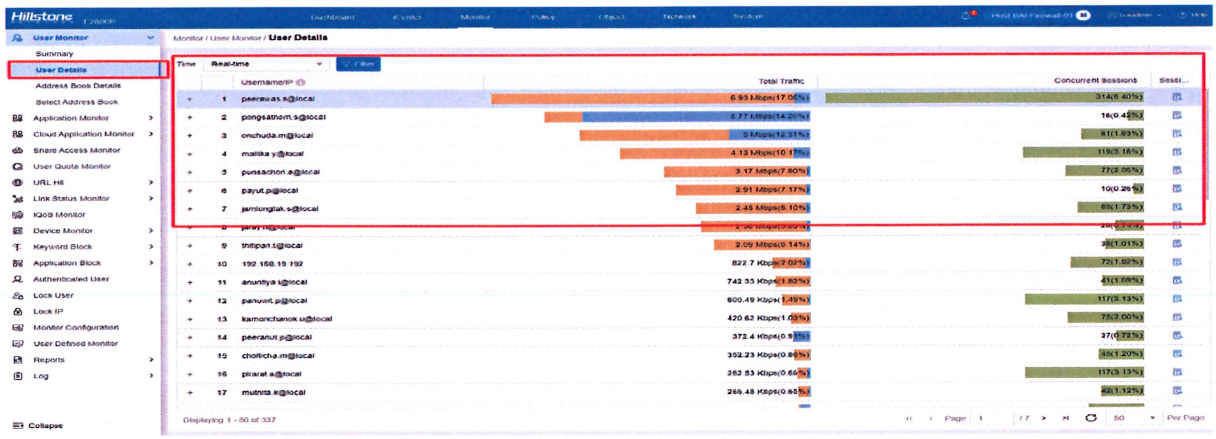
3.หลังจากเข้าระบบแล้วไปที่หน้า Monitor



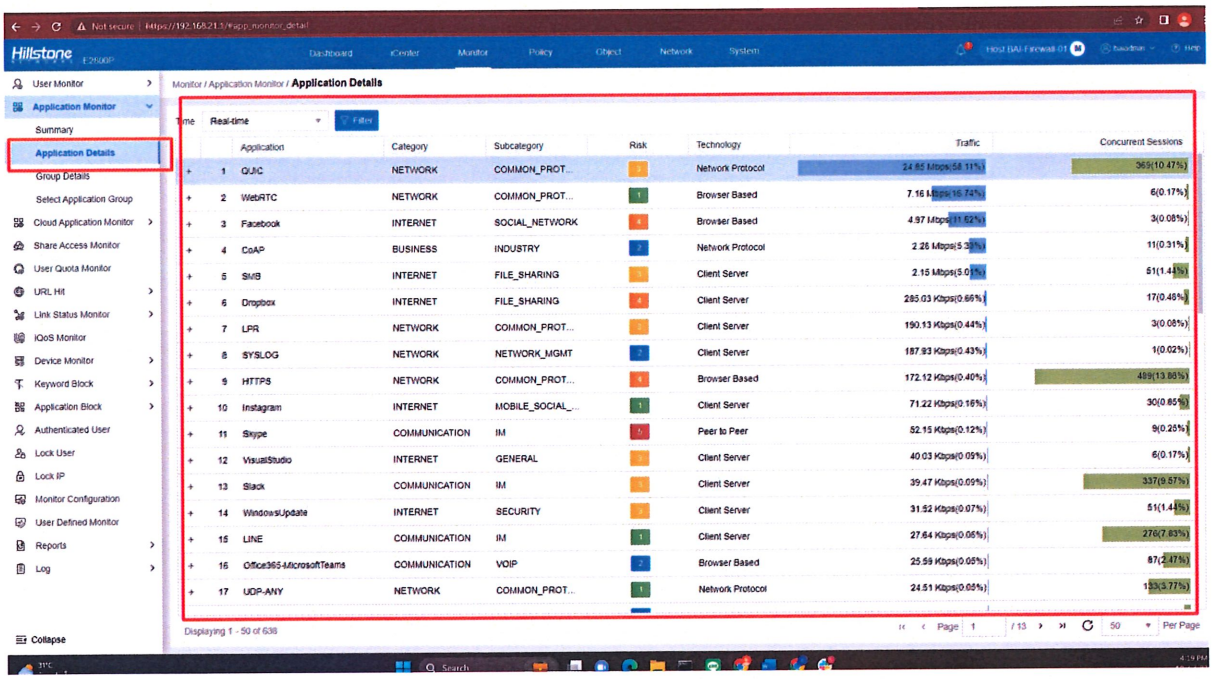
4.เลือกหัวข้อ Application Monitor เลือก Summary โดยหน้านี้จะแสดงผลของผู้ใช้ที่ใช้ Traffic เยอะสุดและ User ที่มีการเชื่อมต่อเยอะสุด



5.เลือกหัวข้อ User Details เพื่อดูข้อมูลว่า User ไหนใช้ข้อมูล Traffic เยอะสุด โดยหน้านี้จะมีข้อมูล Concurrent Sessions แสดงอยู่ด้วย



6.ในหัวข้อ Application Monitor เลือก Application Details หน้านี้จะแสดงข้อมูลเกี่ยวกับการใช้งาน Traffic ของ Application ต่างๆ



ประวัติการปรับปรุงเอกสาร				
ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	1 สิงหาคม 2566	วรวุฒิ เทพหัสดิน ณ อยุธยา

ผู้อนุมัติ

ลงชื่อ วรวุฒิ

(วรวุฒิ เทพหัสดิน ณ อยุธยา)

ผู้รับผิดชอบ

วันที่ 01/08/66

ลงชื่อ ธนิศร

(ธนิศร ธนวงศ์เกษม)

ผู้บริหารฝ่ายคอมพิวเตอร์

วันที่ 01/08/66

ขั้นตอนการจัดทำแผนกลยุทธ์เทคโนโลยีสารสนเทศ

วัตถุประสงค์

1. เพื่อเป็นการกำหนดกรอบในการทำงานฝ่ายเทคโนโลยีสารสนเทศให้สอดคล้องกับนโยบายบริษัท
2. เพื่อเป็นแนวปฏิบัติการบริหารการจัดการฝ่ายเทคโนโลยีสารสนเทศที่สำคัญภายใต้งบประมาณที่จัดสรร

ขอบเขต

ภายในบริษัท บางกอก แอสเซท อินเตอร์กรุ๊ป จำกัด (มหาชน)

ผู้รับผิดชอบ

ประธานบริหารฝ่ายเทคโนโลยีสารสนเทศ

แนวทางการปฏิบัติ

1. เขียนบททั่วไป ประกอบไปด้วย
   1.1. บทนำ
   1.2. ปรัชญา และปณิธาน
   1.3. วิสัยทัศน์
   1.4. พันธกิจ
   1.5. เป้าหมาย

   เป็นการประชุมในฝ่ายเพื่อ กำหนดปรัชญา, ปณิธาน, วิสัยทัศน์, พันธกิจ และเป้าหมาย

2. การวิเคราะห์สถานภาพด้านเทคโนโลยีสารสนเทศ
   2.1. เป็นการนำบริบทของบริษัท ความต้องการของทุกหน่วยงาน มาวิเคราะห์ด้วย SWOT Analysis โดยการหาจุดแข็ง (Strength) จุดอ่อน (Weakness) โอกาส (Opportunity) และ อุปสรรค (Threat)
   2.2. นำจุดอ่อน และโอกาส มาศึกษาวิเคราะห์ความเป็นไปได้ นำเทคโนโลยีสารสนเทศ มาพัฒนาเข้าไปช่วยแก้ปัญหาจุดอ่อนต่างๆ และอาศัยโอกาสทำแผนพัฒนาเชิงรุก
3. ยุทธศาสตร์ เป้าหมาย มาตรการ และแนวทาง

3.1. คัดเลือกจุดอ่อนหรือโอกาสที่สำคัญมาไม่เกิน 5 ข้อ มาสร้างแผนกลยุทธ์ พร้อมทั้งกำหนดเป้าหมาย มาตรการ และแนวทาง

4. แผนพัฒนาระบบสารสนเทศ

เป็นการนำกลยุทธ์หรือยุทธศาสตร์มาทำแผนระยะสั้น และระยะยาว พร้อมงบประมาณที่คาดว่าจะใช้

4.1. แผนพัฒนาสารสนเทศระยะสั้น เป็นการวางแผนในระยะเวลา 1 ปี ซึ่งมีการจัดทำแผนปฏิบัติงานสารสนเทศประจำปี ไว้รองรับ

4.2. แผนพัฒนาสารสนเทศระยะยาว เป็นการวางแผนในระยะเวลา 5 ปี

4.3. แผนงบประมาณรายจ่าย เป็นการการกำหนดงบประมาณคาดว่าจะใช้ตามแผนกลยุทธ์ที่วางไว้

5. การวางแผนกลยุทธ์เทคโนโลยีสารสนเทศกำหนดไว้ 5 ปีจะดำเนินการเปลี่ยนแผนทั้งหมด แต่มีการทบทวนแผนทุกปี หากไม่มีการเปลี่ยนแปลงที่เป็นสาระสำคัญ จะไม่มีการเปลี่ยนแปลงยุทธศาสตร์

6. แผนกลยุทธ์ที่สมบูรณ์จะต้องได้รับการเห็นชอบจากคณะกรรมการบริษัท ลงนามโดยประธานคณะกรรมการบริษัท

ประวัติการปรับปรุงเอกสาร				
ครั้งที่	เวอร์ชัน	รายละเอียด	วันที่	ผู้ดำเนินการ
1	1.0	เอกสารฉบับแรก	25 มกราคม 2567	ชาญยุทธ วัฒนาศักดิกุล

ลงชื่อ _____

(ชาญยุทธ วัฒนาศักดิกุล)

ผู้รับผิดชอบ

วันที่ 20 ม.ค. 2567

ผู้อนุมัติ

ลงชื่อ _____

(ธนินทร ธนวงศ์เกษม)

ประธานบริหารฝ่ายคอมพิวเตอร์

วันที่ 20 ม.ค. 2567