BANGKOK ASSET
INTERGROUP

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 **ระบบ LAN และระบบ Intranet** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อ สื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในบริษัทฯ **ระบบ Internet** 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

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

วัตถุประสงค์

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

แนวทางปฏิบัติ

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 การคุกคามทางไซเบอร์ จากการใช้ 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 ให้ถูกต้องเป็นไปตามกฎระเบียบของบริษัทฯ 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 เขียนโปรแกรมเพิ่มเติมจะต้องส่งคำขอเพื่อเปลี่ยนแปลง 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. เพื่อสร้างความเข้าใจให้พนักงานหรือบุคคลที่ใช้อุปกรณ์เชื่อมต่อระบบเครือข่ายของบริษัท ฯ 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 หรือบริษัท ฯ 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** เป็นการกำหนดบทบาทหน้าที่ 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 ระบบเครือข่ายและระบบให้บริการ 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

หมวดที่ 8 นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

วัตถุประสงค์

1. เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยของการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเครือข่ายและคอมพิวเตอร์

แนวทางปฏิบัติ

1. บริษัทฯ ต้องมีการควบคุมการเข้าออกห้อง Server อย่างเพียงพอจะเป็นการป้องกันบุคคลที่ไม่ได้รับอนุญาตเข้าสู่ห้อง Server และความเสียหายอันจะเกิดจากอุปกรณ์หรือระบบต่างๆ เช่น ระบบไฟฟ้า ระบบอุณหภูมิและความชื้น ซึ่งย่อมมีความเสี่ยงต่องอุปกรณ์และข้อมูลของบริษัทฯ 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 รวมถึงการพิจารณาการเลิกจ้าง

เพื่อให้ทราบโดยทั่วกันและยึดถือปฏิบัติให้เป็นไปในแนวทางเดียวกัน จึงประกาศใช้นโยบายกำกับดูแลและรักษาความปลอดภัยเทคโนโลยีสารสนเทศ

นโยบายนี้มีผลบังคับใช้ตั้งแต่วันที่ 14 ธันวาคม 2567

ลงชื่อ_____

(นายศิริพล ยอดเมืองเจริญ)

ประธานคณะกรรมการบริษัท

บริษัท บางกอก แอสเซท อินเตอร์กรุ๊ป จำกัด (มหาชน)