

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (IT Security Policy) (ฉบับทบทวนปี 2568)

สารบัญ

หน้า

ส่วนที่ 1	บทนำและเรื่องที่ต้องปฏิบัติ	
1.1	วัตถุประสงค์	4
1.2	คำจำกัดความ	4
1.3	ขอบเขตและผลบังคับใช้ของนโยบาย	7
1.4	การตรวจสอบให้เป็นไปตามนโยบาย	8
1.5	การทบทวนนโยบาย	8
ส่วนที่ 2	การปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	
2.1	นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	9
2.2	โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ	10
2.3	ความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศด้านบุคลากร	13
2.4	การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)	14
2.5	การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)	16
2.6	การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (Access Control)	16
2.7	การควบคุมการเข้ารหัสข้อมูล (Cryptographic Control)	20
2.8	การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental)	20
2.9	การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ	22
2.10	การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศ ผ่านระบบเครือข่ายคอมพิวเตอร์ (Communications Security)	27
2.11	การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ	29
2.12	การใช้บริการระบบสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing)	31
2.13	การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ	32
2.14	การบริหารความต่อเนื่องทางธุรกิจในการมั่นคงปลอดภัยของระบบสารสนเทศ	34

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (IT Security Policy) (ฉบับปรับปรุงปี 2568)

บริษัทตระหนักถึงความสำคัญเรื่อง ระบบเทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญในการขับเคลื่อนธุรกิจ รวมทั้ง ตระหนักถึงบทบาทและความสำคัญของเทคโนโลยีสารสนเทศในการประกอบธุรกิจหลักทรัพย์จัดการกองทุน จึงได้พิจารณาให้มีการบริหารความเสี่ยงและการรักษาความปลอดภัยในเรื่องดังกล่าวอย่างมีประสิทธิภาพเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในการดำเนินงาน ทั้งนี้ เพื่อให้สอดคล้องกับแนวทางของหน่วยงานกำกับภายนอก คณะผู้บริหารของบริษัทจึงได้กำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขึ้น เพื่อเป็นกฎระเบียบและข้อปฏิบัติในการควบคุมความปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องในการดำเนินธุรกิจของบริษัท

ทั้งนี้ เพื่อให้บริษัท สามารถกำกับดูแล ป้องกัน ควบคุม ติดตามการดำเนินงานของบริษัทอย่างมีประสิทธิภาพ สอดคล้องและเป็นไปในทิศทางเดียวกัน บริษัทจึงจัดทำนโยบายดังกล่าว เพื่อให้พนักงานและผู้บริหารทุกระดับได้รับทราบ และนำไปปฏิบัติอย่างเคร่งครัด โดยที่ประชุมคณะกรรมการบริษัทครั้งที่ 5/2568 วันที่ 16 ธันวาคม 2568 ได้มีมติอนุมัตินโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (IT Security Policy) ดังมีรายละเอียดตามเอกสารแนบท้ายนี้

ผู้บังคับบัญชามีหน้าที่ต้องติดตามและแนะนำผู้ใต้บังคับบัญชาตามลำดับชั้น ในการปฏิบัติงานให้สอดคล้องกับนโยบาย ขั้นตอน และวิธีการปฏิบัติที่กำหนดไว้ในนโยบายฉบับนี้ โดยสม่ำเสมอ

คณะกรรมการบริษัท

ส่วนที่ 1 บทนำและเรื่องที่ต้องปฏิบัติ

1.1 วัตถุประสงค์

บริษัท หลักทรัพย์จัดการกองทุน ไอรา จำกัด (บริษัท) ตระหนักถึงความสำคัญเป็นอย่างยิ่งในบทบาทของเทคโนโลยีสารสนเทศในการประกอบธุรกิจหลักทรัพย์ จึงได้พิจารณาให้มีการบริหารความเสี่ยงและการรักษาความปลอดภัยในเรื่องดังกล่าวอย่างมีประสิทธิภาพเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในการดำเนินงาน ทั้งนี้ เพื่อให้สอดคล้องกับแนวทางของหน่วยงานกำกับภายนอก คณะผู้บริหารของบริษัท จึงได้กำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขึ้น เพื่อเป็นกรอบระเบียบและข้อปฏิบัติในการควบคุมความปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องในการดำเนินธุรกิจของบริษัท โดยมีวัตถุประสงค์ดังต่อไปนี้

- 1) เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ
- 2) เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้รับทราบเกี่ยวกับหน้าที่และความรับผิดชอบและแนวทางในการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศต่าง ๆ ดังนี้
 - ความเสี่ยงจากการเข้าถึงข้อมูลและระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง
 - ความเสี่ยงจากการที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลในระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ
 - ความเสี่ยงจากความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์
 - ความเสี่ยงจากการที่ไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ
 - ความเสี่ยงจากการที่ไม่ได้จัดให้มีการบริหารจัดการระบบคอมพิวเตอร์ และบุคลากรด้านคอมพิวเตอร์ให้เหมาะสมและเพียงพอแก่การสนับสนุนการประกอบธุรกิจ

1.2 คำจำกัดความ

“สินทรัพย์คอมพิวเตอร์”	หมายถึง สินทรัพย์ทุกอย่างที่เกี่ยวข้องกับการใช้ระบบคอมพิวเตอร์ เช่น ฮาร์ดแวร์, ซอฟต์แวร์ และข้อมูล เป็นต้น
“ระบบเครือข่าย”	หมายถึง ระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯ
“คอมพิวเตอร์แม่ข่าย”	หมายถึง เครื่องคอมพิวเตอร์ในระบบเครือข่ายที่ทำหน้าที่เป็น ศูนย์กลางของการทำงาน อาทิ จัดเก็บข้อมูลหรือซอฟต์แวร์สำหรับให้บริการแก่เครื่องคอมพิวเตอร์อื่น ๆ หรือควบคุมการทำงานในระบบเครือข่าย
“การเข้าถึงเครือข่ายจากระยะไกล”	หมายถึง การที่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายเชื่อมต่อเข้ากับเครื่องคอมพิวเตอร์หรือเครือข่ายอื่นผ่านอุปกรณ์สื่อสารหรือสื่อสัญญาณอื่น ๆ อาทิ โมเด็ม, เครือข่ายส่วนตัวเสมือน (VPN)
“การควบคุมการเข้าถึง”	หมายถึง การควบคุมการเข้าถึงหรือใช้งานสินทรัพย์คอมพิวเตอร์ให้เป็นไปตามสิทธิ์ที่กำหนดไว้เท่านั้น
“เครื่องคอมพิวเตอร์”	หมายถึง อุปกรณ์ที่ใช้ในการประมวลผลข้อมูลที่ทำงาน ด้วยระบบอิเล็กทรอนิกส์ โดยทำงานตามคำสั่งผ่านทางซอฟต์แวร์ให้ได้ผลตามที่ต้องการ อาทิ คอมพิวเตอร์

	แม่ข่าย (Server), คอมพิวเตอร์ส่วนบุคคล (Personal computer) และคอมพิวเตอร์แบบพกพาได้ (Notebook Computer)
“อุปกรณ์คอมพิวเตอร์”	หมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่ใช้งานร่วมกับเครื่องคอมพิวเตอร์เพื่อสนับสนุนให้เครื่องคอมพิวเตอร์ปฏิบัติงานได้ตามต้องการ และให้รวมถึง เครื่องคอมพิวเตอร์
“สื่อสัญญาณ”	หมายถึง สื่อกลางใด ๆ ที่ใช้เชื่อมต่อระหว่างอุปกรณ์คอมพิวเตอร์ อาทิ สายทองแดง, สายใยแก้วนำแสง, เครือข่ายไร้สาย
“ฮาร์ดแวร์”	หมายถึง อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย รวมถึงอุปกรณ์อื่น ๆ ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของบริษัท
“ซอฟต์แวร์”	หมายถึง ระบบหรือโปรแกรมคอมพิวเตอร์ดังนี้ 1. ซอฟต์แวร์ระบบ (system software) เช่น ระบบปฏิบัติการ หรือโปรแกรมตรวจจับไวรัส เป็นต้น 2. ซอฟต์แวร์ประยุกต์ (application software) เช่น โปรแกรมประมวลผลคำ (word processor) หรือโปรแกรมสำหรับการประชุมออนไลน์ เป็นต้น
“ระบบเทคโนโลยีสารสนเทศ”	หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ อาทิ อุปกรณ์คอมพิวเตอร์, ระบบเครือข่าย, โปรแกรมระบบงานและสารสนเทศ
“ระบบเทคโนโลยีสารสนเทศมีนัยสำคัญ” (Critical system)	หมายถึง ระบบคอมพิวเตอร์หรือระบบเครือข่ายที่หากมีการหยุดชะงักจะส่งผลกระทบ อย่างมีนัยสำคัญต่อการดำเนินงานหรือความต่อเนื่องในการดำเนินงาน ชื่อเสียง หรือฐานะของบริษัท หรือการใช้บริการของลูกค้า เช่น ระบบซื้อขาย ระบบสนับสนุนการปฏิบัติการ (back office system) ระบบจัดเก็บและบริหารจัดการ ข้อมูลลูกค้า ระบบจัดการลงทุน หรือระบบจัดเก็บทรัพย์สิน เป็นต้น
“สารสนเทศ” (Information)	หมายถึง ข้อมูลที่ผ่านการประมวลผลแล้วจัดระเบียบของข้อมูลให้อยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก โดยอยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และเรื่องอื่น ๆ ได้
“ระบบงาน”	หมายถึง การนำระบบเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการทำงานเพื่อให้งานสำเร็จตามวัตถุประสงค์ที่ตั้งไว้ อาทิ ระบบการจัดเก็บเอกสาร, ระบบการจอยานพาหนะ
“ระบบปฏิบัติการ” (Operating System)	หมายถึง โปรแกรมควบคุมการทำงานของเครื่องคอมพิวเตอร์ และจัดสรรการใช้ทรัพยากรของระบบ ซึ่งได้แก่ การจัดการหน่วยความจำ การควบคุม การทำงานของอุปกรณ์ป้อนข้อมูล (แป้นพิมพ์ / เมาส์) และอุปกรณ์แสดงผล (จอภาพ / เครื่องพิมพ์)

“ระบบป้องกันการบุกรุก” (Firewall)	หมายถึง ระบบรักษาความปลอดภัยที่ประกอบด้วยกลุ่มอุปกรณ์คอมพิวเตอร์และโปรแกรม ซึ่งทำหน้าที่ป้องกันผู้ไม่ได้รับอนุญาตจากเครือข่ายภายนอกเข้าใช้ระบบ และจำกัดการใช้งานของผู้ใช้งานภายในให้เป็นไปตามนโยบายที่บริษัท กำหนด
“ข้อมูล” (Data)	หมายถึง ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลได้ด้วยวิธีการทางอิเล็กทรอนิกส์บนอุปกรณ์คอมพิวเตอร์ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์
“ไฟล์” (File)	หมายถึง ข้อมูลที่ถูกรวบรวมลงสื่อบันทึกและระบุเป็นหนึ่งหน่วยโดยมี ชื่อเฉพาะ เช่น โปรแกรมใช้งาน และไฟล์เอกสารต่าง ๆ ที่สร้างขึ้นและใส่ชื่อให้แก่ไฟล์นั้นแล้วเก็บบันทึกลง สื่อบันทึก เป็นต้น
“บริษัท” (Company)	หมายถึง บริษัทหลักทรัพย์จัดการกองทุน ไอรา จำกัด
“ผู้ใช้งาน” (User)	หมายถึง พนักงานของบริษัท และบุคลากรภายนอกที่มีการปฏิบัติงานโดยมีการเข้าถึงข้อมูลลับหรือระบบงานสำคัญภายในองค์กรโดยไม่รวมถึงลูกค้า
“ความเสี่ยง” (Risk)	หมายถึง โอกาสของสินทรัพย์คอมพิวเตอร์ในการถูกละเมิดการรักษาความปลอดภัย
“เหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ” (IT Incident)	หมายถึง เหตุการณ์ด้านเทคโนโลยีสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) เช่น (1) ระบบเทคโนโลยีสารสนเทศของบริษัทถูกบุกรุกหรือโจมตี (2) ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศถูกคุกคาม (3) ระบบเทคโนโลยีสารสนเทศหยุดชะงัก ไม่สามารถให้บริการได้ เป็นต้น
“ส่วนงาน”	หมายถึง ฝ่าย/ส่วนงาน ที่เป็นไปตามโครงสร้างองค์กรของบริษัท
“ส่วนงานเจ้าของข้อมูล”	หมายถึง เจ้าหน้าที่ในส่วนงานตั้งแต่ 1 คนขึ้นไปที่ได้รับมอบหมายจากส่วนงานให้เป็นผู้รับผิดชอบข้อมูล
“โปรแกรมประสงค์ร้าย”	หมายถึง อุปกรณ์คอมพิวเตอร์หรือโปรแกรมที่มีการตั้งใจใส่เข้าไปในระบบโดยไม่ได้รับอนุญาต เพื่อให้ทำงานตามความประสงค์ของผู้ประสงค์ร้าย ซึ่งมีผลให้คอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศ หรือชุดคำสั่งอื่น ๆ ได้รับความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
“บุคคลภายนอก” (Third party)	หมายถึง บุคคลภายนอกที่มีความเกี่ยวข้องกับบริษัท ทั้งนี้ ไม่รวมถึงลูกค้า ที่ใช้บริการหรือผลิตภัณฑ์ของบริษัท (1) ผู้ให้บริการงานด้านเทคโนโลยีสารสนเทศ (2) ผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของบริษัท (3) ผู้ที่สามารถเข้าถึงข้อมูลสำคัญของบริษัทหรือข้อมูลของลูกค้า ที่อยู่ในรูปแบบอิเล็กทรอนิกส์และอยู่ภายใต้การควบคุมดูแลของบริษัท

“เอกสารโครงแบบ” (Configuration Document)	หมายถึง เอกสารที่แสดงรายละเอียดการกำหนดค่าต่าง ๆ ในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศใช้งานได้ตามความต้องการ
“ผู้บริหารเครือข่าย” (Network Administrator)	หมายถึง บุคคลซึ่งทำหน้าที่รับผิดชอบในการดูแลและบำรุงรักษาเครือข่าย
“ผู้บริหระคอมพิวเตอร์แม่ข่าย” (Host/Server Administrator)	หมายถึง บุคคลซึ่งทำหน้าที่รับผิดชอบในการดูแลและบำรุงรักษาคอมพิวเตอร์แม่ข่าย
“ผู้บริหระระบบป้องกันการบุกรุก” (Firewall administrator)	หมายถึง บุคคลซึ่งทำหน้าที่รับผิดชอบในการดูแลและบำรุงรักษาระบบป้องกันการบุกรุก
“บัญชีผู้บริหระคอมพิวเตอร์แม่ข่าย” (Administrator Account)	หมายถึง บัญชีที่ผู้บริหระคอมพิวเตอร์แม่ข่ายใช้เพื่อการบริหารระบบคอมพิวเตอร์แม่ข่าย
“บัญชีผู้ใช้งาน” (User account)	หมายถึง บัญชีที่ผู้ใช้งานใช้ในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นไปตามข้อตกลงระหว่างผู้ใช้งานกับผู้ให้บริการระบบเทคโนโลยีสารสนเทศ
“การใช้งานอุปกรณ์เคลื่อนที่” (Mobile device)	หมายถึง การปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่เพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศที่มีนัยสำคัญ โดยผ่านการเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในของบริษัทโดยตรง
“การใช้งานอุปกรณ์ส่วนตัว” (Bring Your Own Device : BYOD)	หมายถึง การใช้งานอุปกรณ์ส่วนตัวของพนักงานเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศรวมถึงการเข้าถึงระบบอีเมล และตารางการประชุมของบริษัท ไม่ว่าจะเป็นกระทำผ่าน แอปพลิเคชัน เว็บเบราว์เซอร์ หรือช่องทางใด ๆ
“การบริหารจัดการ โครงการด้านเทคโนโลยีสารสนเทศ” (IT project management)	หมายถึง การจัดหา พัฒนา หรือแก้ไขเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศที่มีผลกระทบอย่างมีนัยสำคัญ ต่อการให้บริการ การดำเนินธุรกิจ หรือโครงสร้างพื้นฐาน (infrastructure) ด้านเทคโนโลยีสารสนเทศ
“การปฏิบัติงานจากเครือข่ายภายนอก” (teleworking)	หมายถึง การปฏิบัติงานที่มีการเข้าถึงระบบเทคโนโลยีสารสนเทศที่มีนัยสำคัญ โดยไม่ผ่านการเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในของบริษัทโดยตรง
“MFA”	หมายถึง การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication)
“Privileged user”	หมายถึง ผู้ใช้งานที่ได้รับสิทธิในการใช้งานในระดับสูง

1.3 ขอบเขตและผลบังคับใช้ของนโยบาย

1.3.1 นโยบายการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศมีขอบเขตครอบคลุมถึงเรื่องต่อไปนี้

- การแบ่งแยกอำนาจหน้าที่ (Segregation Of Duties)
- การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)
- การรักษาความปลอดภัยข้อมูลระบบคอมพิวเตอร์และระบบเครือข่าย (Information and Network Security)

- การควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)
- การสำรองข้อมูลและระบบคอมพิวเตอร์และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)
- การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)
- การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

1.3.2 ผลบังคับใช้

แนวทางปฏิบัติฉบับนี้ใช้เป็นแนวทางในการกำหนดหลักเกณฑ์อันว่าด้วยการปฏิบัติตามนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศหรือข้อกำหนดของทางกรอื่นใดที่เกี่ยวข้อง

ผู้ที่ต้องปฏิบัติตามแนวทางปฏิบัติฉบับนี้ ผู้บริหารทุกระดับ พนักงานทุกคน รวมถึงตัวแทน และผู้ที่ได้รับมอบหมายจากบริษัท ต้องปฏิบัติตามแนวทางปฏิบัติฉบับนี้โดยเคร่งครัด

1.4 การตรวจสอบให้เป็นไปตามนโยบาย

- ผู้บริหารสูงสุดของแต่ละสายงานฯ ต้องดูแลผู้บังคับบัญชาของตนให้ปฏิบัติตามนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างถูกต้อง
- หน่วยงานตรวจสอบหรือคณะกรรมการบริษัทพิจารณามอบหมายบุคคลที่เหมาะสมเพื่อตรวจสอบการปฏิบัติตามนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง
- ต้องจัดให้มีการตรวจสอบด้านเทคนิคสำหรับอุปกรณ์คอมพิวเตอร์และโปรแกรม เพื่อให้มั่นใจว่าได้มีการปฏิบัติตามการควบคุมที่กำหนดไว้
- ต้องประกาศใช้และสื่อสารนโยบายให้แก่บุคคลที่เกี่ยวข้องอย่างทั่วถึง เพื่อให้สามารถปฏิบัติตามได้ เช่น จัดการฝึกอบรม เป็นต้น
- ต้องมีการติดตามการปฏิบัติงานของเจ้าหน้าที่ให้เป็นไปตามนโยบายอย่างเคร่งครัด
- ต้องมีขั้นตอนหรือวิธีปฏิบัติเพื่อให้มีการปฏิบัติตามนโยบายที่ได้กำหนดไว้อย่างครบถ้วน
- บริษัทกำหนดให้ ต้องแจ้งสำนักงาน ก.ล.ต. ทันที เมื่อมีกรณีที่เกิดผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

1.5 การทบทวนนโยบาย

บริษัทกำหนดให้มีการทบทวนนโยบายอย่างน้อยปีละ 1 ครั้งหรือเมื่อมีประกาศของทางกรที่เกี่ยวข้องมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

ส่วนที่ 2 การปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

2.1 นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

บริษัท ได้จัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อใช้เป็นแนวทางในการปฏิบัติควบคุมการปฏิบัติงานและการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพตลอดจนอยู่ในมาตรฐานที่ยอมรับได้จากคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และกลุ่มบริษัท

ทั้งนี้ บริษัทจึงกำหนดหลักการ แนวทางปฏิบัติ การควบคุมและการปฏิบัติงาน การรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ โดยมีสาระสำคัญของวัตถุประสงค์และแนวทางปฏิบัติสอดคล้องกับประกาศของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ.38/2565 และสธ.33/2567 รวมทั้ง นป.6/2567 ประกอบด้วย 13 หัวข้อ ประกอบด้วยรายละเอียดดังต่อไปนี้

- หัวข้อที่ 1 นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (Information Security Policy)
- หัวข้อที่ 2 โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Organization of Information Technology Security)
- หัวข้อที่ 3 ความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศด้านบุคลากร (Human Resources Security)
- หัวข้อที่ 4 การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)
- หัวข้อที่ 5 การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)
- หัวข้อที่ 6 การควบคุมการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ (Access Control)
- หัวข้อที่ 7 การควบคุมการเข้ารหัสข้อมูล (Cryptographic Controls)
- หัวข้อที่ 8 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)
- หัวข้อที่ 9 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ (Operations Security)
- หัวข้อที่ 10 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (Communications Security)
- หัวข้อที่ 11 การจัดหา พัฒนา และดูแลรักษาระบบเทคโนโลยีสารสนเทศ (System Acquisition, Development and Maintenance)
- หัวข้อที่ 12 การใช้บริการระบบเทคโนโลยีสารสนเทศจากผู้รับดำเนินการ (IT Outsourcing)
- หัวข้อที่ 13 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (Information Security Incident Management)
- หัวข้อที่ 14 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (Information Security Aspects of Business Continuity Management)

2.2 โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Organization of Information Technology Security)

2.2.1 โครงสร้างภายในองค์กร (Internal Organization)

วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ของบริษัทฯ สำหรับส่วนต่าง ๆ ภายในองค์กรให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

แนวทางการปฏิบัติ

1. บริษัทฯ กำหนดให้ผู้บริหารระดับสูง เป็นผู้รับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และแนวทางในการปฏิบัติหน้าที่ให้กับบุคลากรของบริษัทฯ และกำหนดให้มีผู้บริหารระดับสูง เป็นผู้รับผิดชอบในการสอบทานการปฏิบัติงานเพื่อป้องกันความเสี่ยงในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศที่อาจเกิดขึ้น ในการปฏิบัติหน้าที่ในการสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ของบริษัทฯ อย่างเป็นลายลักษณ์อักษร
2. กำหนดให้มีการแบ่งแยกหน้าที่ในการปฏิบัติงานด้านต่าง ๆ ที่เกี่ยวกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอย่างชัดเจน เพื่อให้มีการสอบทานการปฏิบัติงานระหว่างกันเพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้น ในกรณีที่ไม่สามารถแบ่งแยกหน้าที่ความรับผิดชอบเนื่องจากข้อจำกัดทางด้านขนาดของการประกอบธุรกิจ บริษัทฯ ได้จัดให้มีกระบวนการติดตาม และตรวจสอบการปฏิบัติงานของบุคลากรที่เกี่ยวข้องอย่างใกล้ชิดและสม่ำเสมอ เพื่อลดความเสี่ยงที่อาจเกิดขึ้น
3. มีการจัดทำทะเบียนรายชื่อและช่องทางสำหรับการติดต่อ (Contact Person) กับหน่วยงานอื่น เพื่อให้สามารถติดต่อประสานงานหรือขอความช่วยเหลือในกรณีเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ เช่น สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ตลาดหลักทรัพย์แห่งประเทศไทย หรือผู้ให้บริการอื่น ๆ ที่สนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของบริษัทฯ เป็นต้น พร้อมทั้งมีการปรับปรุงทะเบียนรายชื่อและช่องทางสำหรับการติดต่อดังกล่าวให้เป็นปัจจุบัน

2.2.2 การปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่ (Mobile device) เพื่อเข้าถึงระบบสารสนเทศภายในองค์กร และการปฏิบัติงานจากเครือข่ายภายนอกบริษัท (Teleworking)

วัตถุประสงค์

เพื่อกำหนดมาตรการรักษาความมั่นคงปลอดภัยสำหรับการปฏิบัติงานจากเครือข่ายภายนอกบริษัท รวมทั้งการใช้งานอุปกรณ์เคลื่อนที่เพื่อเข้าถึงระบบงานภายในองค์กร

แนวทางการปฏิบัติ

1. ในกรณีการใช้อุปกรณ์เคลื่อนที่สำหรับการปฏิบัติงานที่มีการเชื่อมต่อกับระบบงานภายในองค์กร ทั้งนี้ ไม่รวมถึงระบบ Mail Service ฝ่ายเทคโนโลยีสารสนเทศต้องมีมาตรการป้องกันข้อมูลสารสนเทศที่สำคัญ โดยพิจารณาถึงแนวทางดังต่อไปนี้
 - (1) กำหนดให้มีการลงทะเบียน อุปกรณ์เคลื่อนที่ เช่น ยี่ห้อ รุ่น ระบบปฏิบัติการ รหัสประจำเครื่อง (Serial number) และหมายเลขอ้างอิงอุปกรณ์เครือข่าย (MAC address) เป็นต้น อย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนอุปกรณ์ เพื่อให้มั่นใจได้ว่าการใช้งานอุปกรณ์ดังกล่าว มีความสอดคล้องเป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

- (2) มีมาตรการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญ (Sensitive Data) กรณีที่อุปกรณ์เคลื่อนที่สูญหาย เช่น การกำหนดให้ใส่รหัสผ่านก่อนใช้งานอุปกรณ์ (Lock Screen) หรือการลบข้อมูลจากระยะไกล (Remote Wipe-out) เป็นต้น
- (3) ห้ามใช้อุปกรณ์เคลื่อนที่ (Tablet, Smartphone) ที่ถูกปรับแต่ง (Rooted หรือ Jailbroken) เข้าถึงระบบเทคโนโลยีสารสนเทศ หรือเครื่องคอมพิวเตอร์แบบพกพาที่มีการติดตั้งโปรแกรมสำหรับวิเคราะห์ระบบเครือข่าย
- (4) กำหนดประเภทบริการการใช้งาน (Application Service) ที่อนุญาตให้ใช้งานผ่านอุปกรณ์เคลื่อนที่และกำหนดมาตรการควบคุมการเข้าถึงบริการการใช้งานดังกล่าว โดยคำนึงถึงความปลอดภัยของการเชื่อมต่อกับเครือข่าย เช่น จำกัดให้เข้าถึงบริการการใช้งานบางประเภท หากเป็นการเชื่อมต่อกับเครือข่ายภายนอก เป็นต้น
- (5) จัดให้มีการเข้ารหัสข้อมูลสารสนเทศที่สำคัญบนอุปกรณ์เคลื่อนที่และที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์
- (6) จัดให้มีการอบรมผู้ใช้งานเพื่อตระหนักและทราบถึงความเสี่ยงจากการใช้งาน และแนวทางการควบคุมความเสี่ยงดังกล่าว
- (7) ควบคุมให้มีการติดตั้งเฉพาะโปรแกรมที่ถูกต้องตามลิขสิทธิ์ และโปรแกรมเพื่อปิดช่องโหว่ (Patches) ที่เหมาะสมกับการใช้งาน
- (8) กำหนดมาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Malware)
- (9) จัดให้มีการดำเนินการเพื่อลดผลกระทบเมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลสารสนเทศ เช่น ตัดการเชื่อมต่อโดยทันทีที่ทราบเหตุ เป็นต้น

ทั้งนี้ หากอุปกรณ์เคลื่อนที่เป็นทรัพย์สินของพนักงาน ฝ่ายเทคโนโลยีสารสนเทศต้องพิจารณาแนวทางในข้อ (1) - (6) เป็นขั้นต่ำ พร้อมทั้งจัดให้มีมาตรการควบคุมที่เทียบเคียงหรือทดแทนแนวทางในข้อ (6) - (9) ได้ เช่น กำหนดให้มีการตรวจสอบอุปกรณ์คอมพิวเตอร์ประเภทพกพาอย่างสม่ำเสมอ กำหนดบทลงโทษหรือตัดสิทธิการใช้งาน Application Service ในกรณีที่พนักงานละเมิดข้อกำหนด เป็นต้น

2. ในกรณีที่มีการปฏิบัติงานขององค์กรจากระยะไกล (Teleworking Site) ฝ่ายเทคโนโลยีสารสนเทศกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอสำหรับข้อมูลสารสนเทศที่ถูกเข้าถึง ประมวลผล และจัดเก็บในพื้นที่ปฏิบัติงาน โดยพิจารณาถึง

- (1) การกำหนดมาตรการรักษาความมั่นคงปลอดภัยด้านกายภาพที่เหมาะสม รัดกุมเพียงพอ สำหรับพื้นที่ปฏิบัติงานนอกองค์กร
- (2) การควบคุมสิทธิการใช้งานและการเข้าถึงข้อมูลสารสนเทศของผู้ใช้งานอย่างเหมาะสม และมีการทบทวนสิทธิอย่างสม่ำเสมอ
- (3) กำหนดให้มีการลงทะเบียน และขออนุมัติการปฏิบัติงานจากเครือข่ายภายนอกบริษัทจากผู้มีอำนาจหรือผู้บริหารที่เกี่ยวข้อง
- (4) การรักษาความมั่นคงปลอดภัยกรณีมีการเชื่อมต่อระบบงานที่สำคัญ หรือรับส่งข้อมูลที่เป็นความลับ หรือมีความสำคัญจากระยะไกล (Remote Access)
- (5) การป้องกันการรั่วไหลของข้อมูลสารสนเทศในกรณีใช้เทคโนโลยี Virtual Desktop
- (6) การป้องกันการเข้าถึงข้อมูลสารสนเทศจากบุคคลที่ไม่มีสิทธิ์ในการใช้งาน เช่น ญาติพี่น้อง และเพื่อน เป็นต้น
- (7) การตรวจสอบสิทธิการเข้าถึงของพนักงานที่ได้รับอนุญาตให้ปฏิบัติงานจากภายนอกบริษัท
- (8) การป้องกันโปรแกรมไม่ประสงค์ดี

2.2.3 ในกรณีที่ให้บริการ Cloud Computing กับระบบสารสนเทศที่มีความสำคัญฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดทำมีข้อกำหนดเกี่ยวกับการใช้งาน โดยขั้นต่ำต้องมีรายละเอียด ดังนี้

1. การให้บริการ Cloud Computing บริษัทฯได้มีข้อกำหนดเกี่ยวกับการใช้งาน ดังนี้

- (1) ประเมินความเสี่ยงเกี่ยวกับการให้บริการ
- (2) กำหนดประเภทงานที่จะให้บริการ
- (3) กำหนดรูปแบบของการให้บริการ เช่น Software as a service (SAAS), Platform as a service (PAAS) และ Infrastructure as a service (IAAS)
- (4) กำหนดวิธีการคัดเลือกและประเมินผู้ให้บริการ (Due Diligence) เช่น ผู้ให้บริการต้องได้รับมาตรฐานการรับรองความมั่นคงปลอดภัยด้านสารสนเทศในระดับสากล เช่น ได้รับมาตรฐาน ISO 27001
- (5) กำหนดการทบทวนคุณสมบัติของผู้ให้บริการอย่างสม่ำเสมอ เช่น ฐานะทางการเงิน ความเพียงพอของการให้บริการ (Capacity Planning) เพื่อประเมินความพร้อมในการให้บริการ
- (6) จัดให้มีการเผยแพร่นโยบายเกี่ยวกับการให้บริการ และจัดอบรมให้ความรู้แก่พนักงาน เพื่อให้ตระหนักถึงความมั่นคงปลอดภัยจากการให้บริการ Cloud Computing
- (7) กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้ให้บริการอย่างชัดเจน เช่น การสำรองข้อมูล การรับเรื่องแก้ไขปัญหา ขั้นตอนและกระบวนการแก้ไขปัญหา รายชื่อและช่องทางสำหรับติดต่อ เป็นต้น
- (8) กำหนดความปลอดภัยของข้อมูลแต่ละประเภทที่จะใช้ใน Cloud โดยแบ่งชั้นความลับของข้อมูล และกำหนดวิธีปฏิบัติแต่ละระดับชั้นความลับของข้อมูล
- (9) กำหนดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามการใช้งานแต่ละประเภท เพื่อป้องกันภัยคุกคามและการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
- (10) กำหนดเงื่อนไขสำหรับผู้ให้บริการในการเข้าถึงและเปิดเผยข้อมูลของผู้ใช้บริการ
- (11) กำหนดให้มีการตรวจสอบบันทึกหลักฐานต่าง ๆ และติดตามปัญหาที่อาจส่งผลกระทบต่อการใช้งาน

2. กำหนดข้อตกลงระหว่างผู้ให้บริการและผู้ให้บริการ โดยมีลักษณะดังนี้

- (1) ผู้ให้บริการถือเป็นเจ้าของข้อมูลสารสนเทศ
- (2) กำหนดประเภทบริการที่จะใช้ Cloud Computing
- (3) กำหนดมาตรฐานความปลอดภัยด้านเครือข่าย เช่น การเข้ารหัสข้อมูลที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์ การป้องกันการโจมตีในลักษณะ DDoS (Distributed Denial of Service) การป้องกันการบุกรุกจากโปรแกรมไม่ประสงค์ดี การป้องกันภัยคุกคามในรูปแบบใหม่ (Advanced Persistent Threat) การแบ่งแยกเครือข่าย การเข้ารหัสระหว่างแอปพลิเคชัน (Application) การป้องกันการบุกรุกแบบลำดับขั้น (Defense-in-Depth) และการสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศ (Hardening) เป็นต้น
- (4) ระบุข้อตกลงในการควบคุมการเข้าถึงข้อมูล เช่น วิธีการเข้าใช้งานระบบ วิธีการกำหนดสิทธิ์การใช้งาน การติดตามการแก้ปัญหา การรายงานข้อผิดพลาด ประสิทธิภาพ และ สภาพโดยรวมของระบบ อย่างชัดเจน
- (5) กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้ให้บริการในด้านการสำรองข้อมูล กระบวนการ แก้ไขปัญหา ระดับการให้บริการ (Service Level Agreement: SLA) ระยะเวลาในการกลับคืนสู่สภาพ การดำเนินงานปกติของระบบสารสนเทศ (Recovery Time Objective: RTO) และกำหนดเป้าหมายในการกู้คืนข้อมูล เช่น กำหนดประเภทของข้อมูล และชุดข้อมูลล่าสุดที่จะกู้คืนได้ (Recovery Point Objective: RPO) อย่างชัดเจน
- (6) กำหนดเงื่อนไขความรับผิดชอบในกรณีที่ผู้ให้บริการไม่สามารถให้บริการตามสัญญาที่กำหนด

- (7) กำหนดให้มีการลงนามในสัญญาที่เกี่ยวกับนโยบายการป้องกันการรั่วไหลของข้อมูลที่เกิดขึ้นจากผู้ให้บริการ
- (8) ผู้ให้บริการต้องไม่มีสิทธิเข้าถึงและเปิดเผยข้อมูลของผู้ใช้บริการ เว้นแต่จะแจ้งและได้รับความยินยอมจากผู้ให้บริการ หรือแจ้งให้ทราบหากเป็นไปตามกฎหมายของประเทศที่ผู้ให้บริการไปตั้งศูนย์ข้อมูล (Cloud Server Hosting Country) หรือเป็นไปตามกฎหมายเกี่ยวกับความมั่นคงของประเทศผู้ให้บริการ (Origin Country)
- (9) ผู้ให้บริการต้องปรับปรุงการปฏิบัติงานให้เป็นไปตามมาตรฐานการรับรองความมั่นคงปลอดภัยด้านสารสนเทศในระดับสากลฉบับปัจจุบันโดยไม่ชักช้า หากมาตรฐานดังกล่าว ได้ถูกปรับปรุงให้เป็นปัจจุบัน (Update)
- (10) ฝ่ายเทคโนโลยีสารสนเทศต้องมีมาตรการเพื่อให้มั่นใจได้ว่าผู้ให้บริการจัดให้มีการตรวจสอบขั้นตอนการปฏิบัติงานอย่างน้อยปีละ 1 ครั้ง จากผู้ตรวจสอบอิสระ
- (11) มีข้อกำหนดเมื่อสิ้นสุดการใช้บริการ (Exit Plan) เช่น กำหนดระยะเวลารักษาข้อมูลและวิธีการทำลายข้อมูล เพื่อให้มั่นใจว่าไม่สามารถกู้คืนข้อมูลกลับมาได้
- (12) มีการเปิดเผยขั้นตอนปฏิบัติงาน และเงื่อนไขการใช้บริการ Cloud Computing ต่อจากผู้ให้บริการรายอื่น (Subcontract) อย่างชัดเจน โดยอย่างน้อยต้องมีเงื่อนไขเป็นไปตามข้อ (3)

3. กรณีที่ผู้ให้บริการมีการใช้บริการ Cloud Computing ต่อจากผู้ให้บริการรายอื่น (Subcontract) ต้องจัดให้มีข้อกำหนดดังนี้

- (1) แจ้งส่วนที่ Subcontract ให้ผู้ให้บริการทราบ และให้ถือว่าบริการดังกล่าวเป็นส่วนหนึ่งของบริการของผู้ให้บริการด้วย โดยต้องมีคุณสมบัติด้านความปลอดภัยเทียบเท่ากับผู้ให้บริการ
- (2) มีการเข้ารหัสในกรณีที่มีการรับส่งข้อมูลระหว่าง Cloud Provider กับ Subcontract Provider
- (3) มีการกำหนดขั้นตอนปฏิบัติงาน และเงื่อนไขการ Subcontract อย่างชัดเจน

4. การติดตาม ประเมิน และทบทวนการให้บริการของผู้ให้บริการ มีดังนี้

- (1) ติดตามตรวจสอบประสิทธิภาพของการให้บริการ รวมทั้งมาตรการด้านความมั่นคงปลอดภัยให้สอดคล้องกับข้อกำหนดตามสัญญาต่าง ๆ หรือข้อตกลงในการให้บริการ
- (2) ประเมินความเพียงพอของระบบงานของผู้ให้บริการ (Capacity Planning) อย่างสม่ำเสมอ
- (3) ทบทวนเงื่อนไขการบริการในกรณีที่มีการเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าการให้บริการยังคงสอดคล้องกับการใช้งานและนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของฝ่ายเทคโนโลยีสารสนเทศ
- (4) ทบทวนคุณสมบัติของผู้ให้บริการอย่างต่อเนื่อง เช่น การตรวจสอบความมั่นคงในฐานะทางการเงิน กระบวนการปฏิบัติงาน และประสิทธิภาพการปฏิบัติงาน เป็นต้น

2.3 ความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศด้านบุคลากร

วัตถุประสงค์

เพื่อให้พนักงานและบุคคลภายนอกที่ปฏิบัติงานโดยมีการเข้าถึงข้อมูลหรือระบบงานภายในองค์กรมีความตระหนักรู้ และปฏิบัติงานโดยคำนึงถึงการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

แนวทางการปฏิบัติ

1. พนักงานและบุคคลภายนอกที่ปฏิบัติงานโดยมีการเข้าถึงข้อมูลหรือระบบงานภายในองค์กรมีหน้าที่ศึกษาทำความเข้าใจวิธีปฏิบัติเกี่ยวกับการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศที่บริษัทฯ กำหนด เพื่อนำไปปฏิบัติในการรักษาความปลอดภัยสินทรัพย์คอมพิวเตอร์ในส่วนที่ตนเองใช้งานหรือดูแลรับผิดชอบ

2. สื่อสารให้ความรู้แก่ พนักงาน เจ้าหน้าที่ และบุคคลภายนอกที่ปฏิบัติงานโดยมีการเข้าถึงข้อมูลหรือระบบงานภายในองค์กรเกี่ยวกับความตระหนักรู้ (Awareness Education) และวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศ ซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัย และการเปลี่ยนแปลงที่เกิดขึ้นด้านเทคโนโลยีสารสนเทศของบริษัทฯ ด้วย โดยบุคคลภายนอกจะต้องลงนามรับทราบนโยบายและแนวทางปฏิบัติ
3. กำหนดบทลงโทษทางวินัยสำหรับผู้ฝ่าฝืนนโยบาย กฎ และ/หรือระเบียบปฏิบัติของบริษัทฯ โดยบทลงโทษของพนักงานพิจารณาตามระเบียบขั้นตอนของบริษัทฯ และบทลงโทษของบุคคลภายนอกที่ปฏิบัติงานโดยมีการเข้าถึงข้อมูลหรือระบบงานภายในองค์กรให้เป็นไปตามเงื่อนไขสัญญา แต่หากเป็นการละเมิดข้อกฎหมาย บทลงโทษจะเป็นไปตามฐานความผิดที่ได้กระทำตามที่ระบุไว้ในแต่ละข้อกฎหมายนั้น ๆ

2.4 การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)

2.4.1 หน้าที่ความรับผิดชอบต่อทรัพย์สินด้านเทคโนโลยีสารสนเทศ (Responsibility for Assets)

วัตถุประสงค์

เพื่อให้ทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีความสำคัญได้รับการป้องกันอย่างเหมาะสม และมีการระบุและกำหนดหน้าที่ความรับผิดชอบในการรักษาความมั่นคงปลอดภัยของทรัพย์สินด้านเทคโนโลยีสารสนเทศ

แนวทางการปฏิบัติ

1. มีการจัดทำและเก็บทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศ เช่น อุปกรณ์คอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบและอุปกรณ์เครือข่ายคอมพิวเตอร์ และข้อมูลสารสนเทศ เป็นต้น รวมทั้งตรวจสอบและทบทวนรายการทรัพย์สินอย่างสม่ำเสมอ เพื่อให้เกิดความถูกต้องเป็นปัจจุบัน โดยดำเนินการตรวจสอบและทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ
2. มีการระบุผู้ถือครองทรัพย์สินและกำหนดผู้รับผิดชอบทรัพย์สินด้านเทคโนโลยีสารสนเทศแต่ละประเภท เพื่อดูแลความมั่นคงปลอดภัยตลอดอายุการใช้งานของทรัพย์สิน
3. มีข้อกำหนดในการใช้งานทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม เพื่อให้มั่นใจได้ว่าผู้ได้ว่าผู้ใช้งานทรัพย์สินด้านเทคโนโลยีสารสนเทศมีการเข้าถึงและใช้งานอย่างถูกต้องปลอดภัย
4. ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ส่วนตัวของตนเข้ากับระบบเครือข่ายของบริษัทฯ รวมถึงต้องไม่ติดตั้งซอฟต์แวร์ใด ๆ ลงในเครื่องคอมพิวเตอร์ของบริษัทฯ ก่อนได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ
5. การอนุญาตให้ใช้งานสินทรัพย์ด้านโปรแกรม มีดังนี้
 - (1) ห้ามพนักงานทำการติดตั้งหรือเผยแพร่โปรแกรมที่จะผลิตลิขสิทธิ์บนระบบคอมพิวเตอร์ของบริษัทฯ
 - (2) โปรแกรมที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลลับหรือข้อมูลสำคัญของบริษัทฯ ทั้งที่ได้มาจากการพัฒนาขึ้นโดยผู้ใช้งาน หรือที่ได้รับการจัดซื้อ มา ต้องได้รับการตรวจสอบ ควบคุม และอนุมัติอย่างเหมาะสมโดยฝ่ายเทคโนโลยีสารสนเทศ ก่อนนำมาติดตั้งใช้งานบนระบบเทคโนโลยีสารสนเทศของบริษัทฯ และระบบเทคโนโลยีสารสนเทศทั้งหมดที่ถูกใช้งานโดยพนักงานของบริษัทฯ ต้องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอ เพื่อให้พนักงานของบริษัทฯ มีความเข้าใจและสามารถใช้งานระบบสารสนเทศได้มีประสิทธิภาพ
 - (3) รายชื่อโปรแกรม หรือระบบเทคโนโลยีสารสนเทศ ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของพนักงานให้เป็นไปตามประกาศเรื่อง การใช้ซอฟต์แวร์มาตรฐานในบริษัทฯ
6. การอนุญาตให้ใช้งานอินเทอร์เน็ต ให้คำนึงถึงความเสี่ยง และผลกระทบที่มีต่อบริษัทฯ ทั้งในด้านชื่อเสียงและกฎหมาย โดยกำหนดเป็นมาตรฐานการใช้งานอินเทอร์เน็ตภายในบริษัทฯ

7. การอนุญาตให้ใช้งานอีเมล ให้มีมาตรฐานเดียวกันทั้งบริษัทฯ

2.4.2 การจำแนกประเภททรัพย์สินด้านเทคโนโลยีสารสนเทศ (Asset Classification) และการจัดการสื่อ บันทึกข้อมูล (Media Handling)

วัตถุประสงค์

เพื่อให้ข้อมูลและทรัพย์สินสารสนเทศที่มีความสำคัญได้รับการปกป้องในระดับที่เหมาะสมตามระดับความสำคัญของสารสนเทศนั้นที่มีต่อบริษัทฯ และเพื่อป้องกันการเปิดเผย เปลี่ยนแปลงแก้ไข หรือสร้างความเสียหายต่อข้อมูลสารสนเทศสำคัญที่ถูกจัดเก็บในสื่อบันทึกข้อมูล

แนวทางการปฏิบัติ

1. มีการจำแนกประเภททรัพย์สินด้านเทคโนโลยีสารสนเทศตามระดับชั้นความลับ บุคคลที่สามารถเข้าถึงข้อมูล และความสำคัญต่อบริษัทฯ โดยมีการทบทวนการจำแนกประเภทดังกล่าวอย่างสม่ำเสมอ โดยแบ่งข้อมูลทั้งหมดของ บริษัทฯ ออกตามระดับความสำคัญ ดังนี้
 - (1) ข้อมูลที่เผยแพร่ได้ (Public) เป็นข้อมูลที่บริษัทฯ มีเจตนาต้องการให้ลูกค้า หรือบุคคลภายนอกทราบ เช่น News Release, Brochure ที่บริษัทฯ จัดทำออกมาเพื่อประชาสัมพันธ์ เป็นต้น
 - (2) ข้อมูลภายใน (Internal) เป็นข้อมูลสำหรับให้พนักงานของบริษัทฯ ใช้เท่านั้น และไม่มีเจตนาให้บุคคลภายนอกทราบ แต่ถ้าหากถูกนำไปเผยแพร่ จะไม่ทำให้เกิดความเสียหายมากนัก โดยมากจึงมักไม่ต้องการระบบการป้องกัน เช่น ระเบียบบริษัทฯ, ประกาศจากฝ่ายงานต่างๆ เป็นต้น
 - (3) ข้อมูลลับ (Confidential) มักเป็นข้อมูลสำหรับเฉพาะพนักงานของบริษัทฯ ที่ได้รับมอบหมายเท่านั้น หากถูกเผยแพร่ออกไปสู่บุคคลอื่นที่ไม่เกี่ยวข้อง จะทำให้เกิดความเสียหายแก่บริษัทฯ ลูกค้าหรือพนักงาน จึงต้องเก็บรักษาป้องกันมิให้รั่วไหลออกไป เช่น รายงานที่ใช้เฉพาะฝ่ายงาน เช่นรายงาน NCR, งบประมาณและงบกำไรขาดทุนของบริษัทฯ เป็นต้น
 - (4) ข้อมูลลับเฉพาะ (Highly Restricted) เป็นข้อมูลลับที่สำคัญที่สุด หากถูกเผยแพร่ออกไปสู่บุคคลอื่นหรือพนักงานอื่นที่ไม่เกี่ยวข้อง จะทำให้บริษัทฯ ลูกค้าหรือพนักงานเสื่อมเสียชื่อเสียง ได้รับการกล่าวโทษหรือฟ้องร้อง หรือเกิดความเสียหายอย่างยิ่ง จึงต้องมีการระวังรักษาป้องกันอย่างเข้มงวด เช่น ข้อมูลเกี่ยวกับการบริการใหม่ที่ยังไม่ถึงเวลาประกาศ, ข้อมูลงบการเงินบริษัทฯ ที่ยังไม่ถึงเวลาประกาศ, ข้อมูลการควบคุมรวมกิจการหรือการเพิ่มทุนที่ยังไม่ถึงเวลาประกาศ, password ของระบบต่างๆ ข้อมูลส่วนบุคคล, เงินเดือนโบนัสพนักงาน เป็นต้น
2. จัดให้มีมาตรการดูแลรักษาความมั่นคงปลอดภัยที่สอดคล้องเหมาะสมกับแต่ละกลุ่มประเภทของทรัพย์สินด้านเทคโนโลยีสารสนเทศ เช่น การควบคุมการเข้าถึง การจัดให้มีการเข้ารหัสข้อมูลที่เป็นความลับหรือต้องการความถูกต้องในระดับสูง การจัดเก็บในสถานที่ที่มีการควบคุมการเข้าออกด้วยกุญแจหรือรหัส เป็นต้น
3. มีการบริหารจัดการสื่อบันทึกข้อมูล โดยดำเนินการดังนี้
 - (1) กรณีที่ไม่มีความจำเป็นต้องใช้ข้อมูล ต้องมีการล้างข้อมูลออก, Format ใหม่ หรือทำลายข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูล และไม่ให้สามารถกู้คืนข้อมูลได้
 - (2) จัดให้มีกระบวนการทำลายสื่อบันทึกข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูลที่เป็นความลับหรือมีความสำคัญ
 - (3) ในกรณีที่มีการจัดเก็บข้อมูลเป็นระยะเวลานาน ต้องคำนึงถึงความเสี่ยงที่สื่อบันทึกข้อมูลอาจเสื่อมสภาพ รวมทั้งวิธีการนำข้อมูลมาใช้งานใหม่
 - (4) จัดเก็บสื่อบันทึกข้อมูลในพื้นที่ที่มีความมั่นคงปลอดภัย และเป็นไปตามคำแนะนำของผู้ผลิต

- (5) มีกระบวนการดูแลรักษาความปลอดภัยกรณีที่มีการเคลื่อนย้ายสื่อบันทึกข้อมูลออกจากพื้นที่ทำการ และต้องมีวิธีการป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การนำไปใช้ผิดวัตถุประสงค์ หรือความเสียหายในระหว่างที่นำส่งหรือขนย้ายสื่อบันทึกข้อมูล
- (6) จัดทำขั้นตอนการปฏิบัติสำหรับการบริหารสื่อบันทึกข้อมูลที่ถอดแยกได้ และปฏิบัติตามวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่บริษัทฯ ได้กำหนดไว้ (Management of Removable Media)

2.5 การรักษาความมั่นคงปลอดภัยของข้อมูล (Data security)

วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อให้ข้อมูลมีความถูกต้องครบถ้วน และมีสภาพพร้อมใช้งาน รวมถึงสามารถรักษาความลับของข้อมูลได้อย่างเหมาะสม

แนวทางการปฏิบัติ

1. มีการกำหนดบุคคลหรือหน่วยงานซึ่งเป็นเจ้าของข้อมูล
2. มีการจัดชั้นความลับของข้อมูล (Data Classification) และแนวทางการรักษาความปลอดภัยของ ข้อมูลที่สอดคล้องตามชั้นความลับ โดยครอบคลุมข้อมูลดังนี้
 - (1) ข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (Data at Endpoint)
 - (2) ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (Data in Transit)
 - (3) ข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (Data at Rest)
3. กำหนดแนวทางในการนำเข้า ประมวลผล และทำลายข้อมูลอย่างปลอดภัย
4. จัดทำทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศประเภทข้อมูล (Data Inventory) ให้ครบถ้วน และมีการทบทวนให้เป็นปัจจุบัน

2.6 การควบคุมการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ (Access Control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัย

แนวทางการปฏิบัติ

1. บริษัท มีนโยบายในการ ควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศโดยมีเนื้อหาครอบคลุมเรื่องดังต่อไปนี้
 - (1) มีการกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการเข้าใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ และยกเลิกสิทธิ์ของบุคคลที่ไม่มีความจำเป็นในการเข้าถึงโดยทันที
 - (2) มีการแบ่งแยกบทบาทและหน้าที่ของบุคคลที่เกี่ยวข้อง เช่น บุคคลผู้ร้องขอ (Access Request) บุคคลผู้มีอำนาจอนุมัติ (Access Authorization) และบุคคลผู้บริหารสิทธิ์การเข้าถึง (Access Administration) รวมทั้งต้องมีการบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทฯ
 - (3) มีการควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ โดยต้องครอบคลุมถึงการระบุประเภทหรือบริการทางเครือข่าย (Network Services) และบุคคลที่ได้รับอนุญาตให้เข้าถึง กระบวนการควบคุมและป้องกันการเข้าถึงวิธีการเข้าถึงแบบปลอดภัย เทคนิคการระบุตัวตน และการติดตาม การใช้งานของบุคคลที่ได้รับอนุญาตให้เข้าถึง มีการบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทฯ และเฝ้าระวังการละเมิดความปลอดภัยที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ

- (4) ในกรณีมีการใช้หมายเลขประจำเครื่องแบบพลวัต (Dynamic IP Address) มีระบบที่สามารถระบุผู้ใช้งานในระบบเครือข่ายคอมพิวเตอร์ได้อย่างชัดเจน
- (5) จัดให้มีกระบวนการยืนยันตัวตนผู้ใช้งาน (authentication) ที่เหมาะสมกับความเสี่ยง และป้องกันการปฏิเสธความรับผิดชอบ
- (6) กำหนดมาตรการควบคุม จำกัด และติดตามการใช้งานบัญชี privileged user (privileged user management) ดังนี้
 - มีการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) เมื่อเข้าใช้งานและเปลี่ยนรหัสผ่าน สำหรับระบบปฏิบัติการและระบบฐานข้อมูล ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศที่มีนัยสำคัญ
 - กรณีบริษัทมีข้อกำหนดสำหรับ MFA สามารถใช้วิธีการอื่นใดที่เทียบเท่าทดแทน และจัดให้มีการประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงก่อนดำเนินการเพื่อขออนุมัติยกเว้น (exception)
 - มีการควบคุมและติดตามตรวจสอบการใช้งานบัญชี privileged user อย่างเข้มงวด

2.6.1 การบริหารจัดการบัญชีผู้ใช้งาน (User Access Management)

วัตถุประสงค์

เพื่อให้มีการควบคุมสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศอย่างเหมาะสมและป้องกันไม่ให้ผู้ที่ไม่มียุติการใช้งานสามารถเข้าถึงระบบเทคโนโลยีสารสนเทศได้

แนวทางการปฏิบัติ

1. มีระเบียบปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนผู้ใช้งานใหม่ (User Registration) เพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งระเบียบปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออก หรือเมื่อเปลี่ยนตำแหน่งงานภายในบริษัท เป็นต้น
2. กำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบตามหน้าที่และความรับผิดชอบ โดยต้องจัดสรรสิทธิในการเข้าถึงระดับสูง (Privileged Access Rights) อย่างจำกัดและอยู่ภายใต้การควบคุมอย่างเคร่งครัด
3. ผู้ใช้งานต้องได้รับการตรวจพิสูจน์ตัวตนทุกครั้งเมื่อทำการ Log-on เข้าสู่ระบบสารสนเทศ โดยมีการกำหนดรหัสผ่านที่เป็นไปตามประกาศของบริษัท เรื่องการกำหนดรหัสผ่าน
4. มีการทบทวนสิทธิในการเข้าถึงระบบเทคโนโลยีสารสนเทศตามระยะเวลาที่ได้กำหนดไว้ อย่างน้อย 1 ครั้งในรอบ 6 เดือน

2.6.2 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

วัตถุประสงค์

เพื่อป้องกันไม่ให้ผู้ที่ไม่มียุติ สามารถเข้าถึงระบบเทคโนโลยีสารสนเทศได้

แนวทางการปฏิบัติ

มีข้อกำหนดให้ผู้ใช้งานดูแลรับผิดชอบบัญชีผู้ใช้งาน (user ID) และรหัสผ่าน (password) รวมทั้งข้อมูลส่วนบุคคลที่อาจนำมาใช้เพื่อขอเปลี่ยนแปลงข้อมูลบัญชีการใช้งานระบบได้อย่างมั่นคงปลอดภัย (accountable for safeguard) ตามนโยบายการควบคุมการเข้าถึงที่ได้กำหนดไว้

2.6.3 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและแอปพลิเคชัน (system and application access control)

วัตถุประสงค์

เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศและแอปพลิเคชันโดยไม่ได้รับอนุญาต

แนวทางการปฏิบัติ

1. ผู้ใช้งานต้องปฏิบัติตามการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ การกำหนด การเปลี่ยนแปลงและการยกเลิก รหัสผ่านและการจัดการควบคุมการใช้รหัสผ่าน กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งาน หมายถึง ผู้ใช้งานที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา
 - (1) ได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาและผู้ดูแลระบบงานนั้น ๆ
 - (2) มีการควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
 - (3) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
 - (4) มีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ก็ควรมีการเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น
 - (5) ผู้ใช้งานมีหน้าที่ดูแลรับผิดชอบบัญชีผู้ใช้งาน (User ID) และรหัสผ่าน (Password) และต้องเก็บรักษารหัสผ่านเป็นความลับ ห้ามใช้บัญชีผู้ใช้งาน (User ID) ร่วมกันหรือให้ผู้อื่นเข้าใช้งานบัญชีผู้ใช้งาน (User ID) ของตนโดยเด็ดขาด ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่กระทำผ่านบัญชีผู้ใช้งาน (User ID) และรหัสผ่านของตนเองทั้งหมด หากผู้ใช้งานสงสัยว่าบัญชีผู้ใช้งาน (User ID) หรือรหัสผ่านของตนถูกล่วงละเมิดให้ผู้ใช้งานแจ้งเหตุต่อฝ่ายเทคโนโลยีสารสนเทศและทำการเปลี่ยนแปลงรหัสผ่านทั้งหมดทันที
 - (6) รหัสผ่านต้องได้รับการเปลี่ยนเมื่อเข้าใช้งานครั้งแรก และเปลี่ยนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดไว้ในเอกสารขั้นตอนการปฏิบัติงานมาตรฐานการใช้รหัสผ่าน (Password Standard) และรหัสผ่านต้องมีความมั่นคงปลอดภัยตามที่ได้กำหนดไว้ใน เอกสารขั้นตอนการปฏิบัติงานมาตรฐานการใช้รหัสผ่าน
 - (7) การ Reset Password หรือการ Enable disabled user IDs ต้องมีการร้องขอผ่าน User Request Form และต้องได้รับการอนุมัติจากหัวหน้าฝ่ายของ user ก่อนส่งแบบฟอร์มการร้องขอนั้นมาที่ฝ่ายเทคโนโลยีสารสนเทศเพื่อดำเนินการ เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศต้องไม่ Enable user IDs โดยไม่มีแบบฟอร์มการร้องขอที่มีการอนุมัติจากผู้มีอำนาจแล้ว
 - (8) เจ้าหน้าที่ต้องกำหนดการควบคุมเอกสาร ข้อมูล หรือสื่อต่าง ๆ ที่มีข้อมูลสำคัญจัดเก็บ หรือบันทึกอยู่ ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือในสถานที่ไม่ปลอดภัยในขณะที่ไม่ได้นำมาใช้งาน ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ (Desktop Screen) ไม่ให้มีข้อมูลสำคัญ ปรากฏในขณะที่ไม่ได้ใช้งาน
 - (9) ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดกระบวนการในการเข้าถึงระบบให้มีความมั่นคงปลอดภัย เช่น กำหนดให้ระบบให้บริการจะปฏิเสธการใช้งานหากผู้ใช้พิมพ์รหัสผ่านผิดพลาดเกิน 3 ครั้ง เป็นต้น
 - (10) ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้มีการพิสูจน์ตัวตนสำหรับผู้ใช้งานระบบเป็นรายบุคคล ก่อนที่จะอนุญาตให้เข้าใช้งานระบบ

- (11) ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้ผู้ใช้งานระบบเปลี่ยนรหัสผ่านใหม่อย่างน้อยทุก 6 เดือน
- (12) ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้ผู้ใช้งานแต่ละรายต้องรับผิดชอบ (Accountable) บัญชีผู้ใช้งาน (User ID) และรหัสผ่าน (Password) ของตนเอง และสามารถตั้งค่าหรือเปลี่ยนแปลงรหัสผ่านได้ด้วยตนเอง และระบบต้องมีขั้นตอนให้ยืนยันความถูกต้องด้วย
- (13) ฝ่ายเทคโนโลยีสารสนเทศต้องบังคับให้ผู้ใช้งานตั้งรหัสผ่านที่ยากต่อการคาดเดา เช่น มีความยาวขั้นต่ำ 6-8 ตัวอักษร โดยอาจมีอักขระพิเศษ (เช่น "#") ประกอบด้วย และในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำกับรหัสที่ใช้งานครั้งล่าสุด รวมทั้งในขณะที่ผู้ใช้งานใส่รหัสผ่าน ระบบต้องไม่แสดงให้เห็นว่ารหัสผ่านบนหน้าจอด้วย
- (14) ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้มีการควบคุมการใช้โปรแกรมอรรถประโยชน์ (Utility Program) เพื่อป้องกันการเปลี่ยนแปลงและการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่
 - (ก) ต้องทำการพิสูจน์ตัวตนก่อนทำการใช้งาน
 - (ข) ให้ทำการแยกโปรแกรมอรรถประโยชน์ออกจากโปรแกรมระบบงาน
 - (ค) จำกัดการใช้งานโปรแกรมอรรถประโยชน์ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
 - (ง) ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมอรรถประโยชน์ต่างๆ อาทิ ผู้ใช้งานระบบ
- (15) ฝ่ายเทคโนโลยีสารสนเทศต้องมีวิธีการตัดเวลาการใช้งานเครื่อง คอมพิวเตอร์ลูกข่าย เมื่อเครื่องคอมพิวเตอร์ลูกข่ายนั้นไม่ได้มีการใช้งานเป็นระยะเวลาหนึ่ง อาทิ กลไกการล็อกหน้าจอ และต้องใช้รหัสผ่านในการเข้าสู่ระบบอีกครั้ง
- (16) ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุมการเข้าใช้งาน (Log-on) ระบบเทคโนโลยีสารสนเทศด้วยวิธีการแบบปลอดภัย เช่น มีการป้องกันการเข้าใช้งานโดยวิธีเดาสุ่ม (Brute Force) การแจ้งเตือนกรณีที่มีความพยายาม เข้าใช้งานอย่างไม่เหมาะสม (Breach of Log-on Control) และต้องจัดเก็บหลักฐานดังกล่าว
- (17) ฝ่ายเทคโนโลยีสารสนเทศต้องมีการควบคุมการใช้งานข้อมูลสารสนเทศในระบบเทคโนโลยีสารสนเทศ ได้แก่ กำหนดสิทธิ์ในการใช้งาน อาทิ เขียน อ่าน ลบ ได้ กำหนดกลุ่มของผู้ใช้ที่สามารถ ใช้งานได้ ตรวจสอบว่าข้อมูลสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้
- (18) บัญชีผู้ใช้งานที่มีสิทธิ์การเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator โดยต้องได้รับการพิจารณาให้แก่ผู้ใช้งานตามความจำเป็นและมีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น
- (19) บุคคลภายนอกต้องแสดงความยินยอมปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) ของบริษัทอย่างเคร่งครัด ก่อนที่จะได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท
- (20) ฝ่ายเทคโนโลยีสารสนเทศต้องมีการแยกระบบเทคโนโลยีสารสนเทศที่มีความสำคัญ หรือมีความเสี่ยงสูงไว้อีกบริเวณหนึ่ง เช่น การแบ่งระหว่างระบบที่เชื่อมต่ออินเทอร์เน็ตกับระบบอินเทอร์เน็ตภายในที่ใช้งานในบริษัท เป็นต้น

2.7 การควบคุมการเข้ารหัสข้อมูล (Cryptographic Control)

วัตถุประสงค์

เพื่อให้การใช้งานระบบการเข้ารหัสข้อมูลมีความเหมาะสม มีประสิทธิภาพ และสามารถป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลที่เป็นความลับหรือมีความสำคัญ

แนวทางการปฏิบัติ

1. บริษัทฯ ต้องจัดให้มีการเข้ารหัสข้อมูลที่เป็นความลับหรือมีความสำคัญโดยคำนึงถึงค่านึงถึงชนิด และขั้นตอนวิธีการเข้ารหัสข้อมูล (Algorithm) และการใช้กุญแจเพื่อเข้ารหัสข้อมูล (Key)
2. จัดให้มีการบริหารกุญแจเพื่อการเข้ารหัสข้อมูล ตลอดช่วงระยะเวลาการใช้งาน (Key Management whole Life Cycle) โดยกำหนดแนวปฏิบัติเพื่อการคัดเลือกวิธีการเข้ารหัส การกำหนดความยาวของรหัส การใช้งานและการยกเลิกการใช้งานกุญแจเพื่อการเข้ารหัส รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและแนวทางปฏิบัติดังกล่าว อย่างสม่ำเสมอ
3. กำหนดมาตรการการควบคุมกุญแจเข้ารหัสที่ให้บริการโดยบุคคลภายนอก ซึ่งต้องตรวจสอบเพื่อให้มั่นใจได้ว่ากุญแจการเข้ารหัสที่สร้างขึ้นไม่มีการนำมาใช้ร่วมกับบุคคลอื่น
4. กำหนดกระบวนการรองรับกรณีเกิดการรั่วไหลของกุญแจเข้ารหัส

2.8 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental)

2.8.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas)

วัตถุประสงค์

เพื่อเป็นมาตรฐานในการรักษาความมั่นคงปลอดภัยทางกายภาพ ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงพื้นที่หวงห้าม เช่น ศูนย์คอมพิวเตอร์ (Data Center), ศูนย์สำรอง (Backup Site) และพื้นที่ติดตั้งอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ เช่น Switch, Router รวมถึงพื้นที่ใช้งานของระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นทรัพย์สินของบริษัทฯ

แนวทางการปฏิบัติ

1. ให้ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้ประเมินความเสี่ยงและกำหนดความสำคัญของรายละเอียดสถานที่พื้นที่หวงห้าม (Physical Security Perimeter) อุปกรณ์ป้องกันความเสียหาย และการควบคุมการเข้าออกในเขตพื้นที่หวงห้ามให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ เหมาะสมกับสถานที่หรือพื้นที่ที่ต้องรักษาความปลอดภัย
2. ต้องจัดให้มีการควบคุมการเข้า-ออกในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัยและอนุญาตให้ผ่านเข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น โดยจะต้องมีการทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ
3. หากมีบุคคลอื่นใดที่ไม่ใช่ “เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ” ขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า ต้องตรวจสอบเหตุผลและความจำเป็น ก่อนที่จะอนุญาต หรือไม่อนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราว ทั้งนี้บุคคลจะต้องมีการแลกบัตรประจำตัวที่ราชการออกให้กับบัตร Visitor ที่ทางบริษัทออกให้
4. ฝ่ายเทคโนโลยีสารสนเทศต้องจัดบันทึกบุคคลและการขอเข้าออกไว้เป็นหลักฐาน (ทั้งในกรณีที่ได้รับอนุญาต และไม่อนุญาตให้เข้าพื้นที่) และต้องมีการบันทึกข้อมูลการเข้าออกห้องคอมพิวเตอร์ (Data Center) ของบุคคลภายนอกทุกครั้ง พร้อมทั้งจัดเก็บบันทึกดังกล่าวไว้อย่างน้อย 1 ปี
5. บุคคลภายนอกต้องทำการแลกบัตรประจำตัวของตนที่ออกให้โดยหน่วยงานของรัฐ เช่น บัตรประชาชน ใบขับขี่ พาสปอร์ต กับบัตรผู้มาติดต่อของหน่วยงาน ก่อนได้รับอนุญาตให้เข้าถึงพื้นที่ของบริษัทฯ และจะต้องมีการติดตามควบคุมบุคคลภายนอกที่เข้ามาปฏิบัติงานภายในพื้นที่หวงห้ามอย่างใกล้ชิด

6. บุคคลภายนอกต้องติดบัตรผู้มาติดต่อตลอดเวลาที่อยู่ในพื้นที่สำนักงาน ทั้งนี้บัตรผู้มาติดต่อ ไม่อนุญาตให้อิออนกรรมสิทธิ์หรือหยิบยืมกันใช้งาน
7. ต้องไม่เปิดประตูสำนักงานทิ้งไว้ หรือยินยอมให้บุคคลอื่น ติดตามเข้าภายในพื้นที่สำนักงานโดยเด็ดขาด เว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัว หรือบัตรผู้มาติดต่อได้ เพื่อเป็นการป้องกันการเข้าถึงพื้นที่สำนักงาน และพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับอนุญาต
8. ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้บนโต๊ะทำงาน ในห้องประชุม หรือในตู้ที่ไม่ได้ล็อกกุญแจโดยเด็ดขาด
9. เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาด เว้นแต่บุคคลผู้นั้นเป็นเจ้าหน้าที่ที่ได้รับอนุญาตให้ดำเนินการ และเป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องของหน่วยงานเท่านั้น
10. เพื่อประโยชน์ในการรักษาความปลอดภัยของสถานที่ติดตั้งและเก็บรักษาสินทรัพย์ด้านเทคโนโลยีสารสนเทศ บริษัทฯ จัดให้มีระบบการป้องกันต่อภัยคุกคามต่าง ๆ ได้แก่ อุปกรณ์เตือนไฟไหม้ ระบบดับเพลิงอัตโนมัติ ระบบไฟฟ้าสำรอง ระบบควบคุมอุณหภูมิและความชื้นที่เหมาะสม หรือหายนะอื่น ๆ ทั้งที่เกิดจากมนุษย์และภัยธรรมชาติ
11. ฝ่ายเทคโนโลยีสารสนเทศต้องรับผิดชอบในการบำรุงรักษาสถานที่ อุปกรณ์ป้องกันความเสียหาย และอุปกรณ์ป้องกันภัยต่าง ๆ ภายในเขตรักษาความปลอดภัย ตามระยะเวลาอันสมควร
12. ให้ฝ่ายเทคโนโลยีสารสนเทศจำกัดพื้นที่การเข้าถึงของบุคคลภายนอกที่อาจเข้ามาในพื้นที่ โดยต้องมีการแบ่งแยกพื้นที่ที่เกี่ยวข้องกับการทำงานออกจากพื้นที่ที่บุคคลภายนอกเข้ามาได้ เช่น พื้นที่จัดรับส่งสินค้า (Delivery and Loading Area) พื้นที่เก็บรายงานที่ฝ่ายเทคโนโลยีสารสนเทศ ได้จัดพิมพ์ให้หน่วยงานอื่น

2.8.2 ทรัพย์สินสารสนเทศประเภทอุปกรณ์ (Equipment)

วัตถุประสงค์

เพื่อป้องกันอุปกรณ์สารสนเทศทั้งหมด มิให้สูญหาย ถูกโจรกรรม ก่อให้เกิดความเสียหาย เข้าถึงหรือถูกใช้งาน โดยไม่ได้รับอนุญาต โดยบุคคลที่ไม่เกี่ยวข้อง และเพื่อให้มั่นใจได้ว่า อุปกรณ์สารสนเทศดังกล่าว สามารถทำงานได้อย่างต่อเนื่อง และมีการป้องกันอย่างเพียงพอจากภัยธรรมชาติ การโจรกรรม และความเสียหายอื่น ๆ

แนวทางการปฏิบัติ

1. เจ้าหน้าที่หรือผู้ใช้งานต้องจัดวางและป้องกันอุปกรณ์ของบริษัทฯ เพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่าง ๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต
2. กำหนดให้มีการบำรุงรักษาอุปกรณ์ต่าง ๆ อย่างสม่ำเสมอเพื่อให้อุปกรณ์นั้น สามารถทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน
3. ฝ่ายเทคโนโลยีสารสนเทศ มีการจัดเตรียมแผนรองรับ หากอุปกรณ์สารสนเทศได้รับความเสียหาย และมีการทดสอบแผนรองรับตามระยะเวลาอันสมควร
4. เจ้าหน้าที่หรือผู้ใช้งานต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้ง หรือปรับค่าต่าง ๆ ไปสู่ค่าตั้งต้น (Restore from Factory) ด้วยวิธีการที่ทำให้มั่นใจว่า ไม่สามารถกู้คืนได้อีก ก่อนที่จะทิ้งอุปกรณ์ หรือส่งอุปกรณ์ดังกล่าวไปซ่อมบำรุง
5. มอบหมายให้ฝ่ายเทคโนโลยีสารสนเทศดูแลการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ และควบคุมการขนย้ายอุปกรณ์คอมพิวเตอร์ เพื่อป้องกันข้อมูลที่จัดเก็บในอุปกรณ์คอมพิวเตอร์รั่วไหลหรือถูกแก้ไข

6. มีการควบคุมป้องกันอุปกรณ์สารสนเทศระหว่างที่ไม่มีผู้ใช้งาน (Unattended User Equipment) ให้มีความปลอดภัย รวมทั้งกำหนดการควบคุมเอกสาร ข้อมูล หรือสื่อบันทึกข้อมูลต่าง ๆ เช่น Thumb-Drive และ External Hard-Disk ที่มีข้อมูลสารสนเทศที่จัดเก็บหรือบันทึกอยู่ไม่ให้วางทิ้งไว้บนโต๊ะทำงาน หรือสถานที่ที่ไม่ปลอดภัยในขณะที่ไม่ได้ใช้งาน (Clear Desk) ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏในขณะที่ไม่ได้ใช้งาน (Clear Screen) เช่น การตัดออกจากระบบ (Session Time-out) และการล็อกหน้าจอ (Lock Screen) อัตโนมัติ เป็นต้น

2.9 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

เพื่อให้มั่นใจว่าการปฏิบัติงานด้านระบบเทคโนโลยีสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

2.9.1 การกำหนดหน้าที่ความรับผิดชอบและวิธีการปฏิบัติงาน (Operational Procedures and Responsibilities)

วัตถุประสงค์

เพื่อให้มั่นใจว่าการปฏิบัติงานด้านระบบเทคโนโลยีสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

แนวทางการปฏิบัติ

1. จัดทำคู่มือและขั้นตอนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร เช่น ขั้นตอนในการเปิด-ปิดระบบ การตรวจสอบประสิทธิภาพการทำงานของระบบ ตารางเวลาในการปฏิบัติงาน ขั้นตอนการแจ้งเหตุขัดข้อง ขั้นตอนการกู้คืน ขั้นตอนการบำรุงรักษาและดูแลระบบ เป็นต้น รวมทั้งจัดให้ขั้นตอนการปฏิบัติงานดังกล่าวอยู่ในสภาพที่พร้อมใช้งานและเข้าถึงได้
2. มีการควบคุมการปฏิบัติงานอย่างเคร่งครัด โดยเฉพาะในกรณีที่มีการเปลี่ยนแปลงโครงสร้างองค์กร หรือขั้นตอนการปฏิบัติงาน ซึ่งอาจกระทบต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ดังเช่น
 - (1) กำหนดขั้นตอนหรือแนวทางการปฏิบัติที่เป็นลายลักษณ์อักษร ในกรณีการเปลี่ยนแปลงที่มีนัยสำคัญ
 - (2) มีแผนรองรับ และดำเนินการทดสอบภายหลังการเปลี่ยนแปลง
 - (3) มีการประเมินผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง
 - (4) มีขั้นตอนการขออนุมัติจากผู้มีอำนาจอนุมัติ
 - (5) มีขั้นตอนการตรวจสอบเพื่อให้มั่นใจว่า กระบวนการเปลี่ยนแปลงนั้นเป็นไปตามนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัทฯ
 - (6) มีการบันทึกการเปลี่ยนแปลงและสื่อสารให้หน่วยงานหรือบุคคลที่เกี่ยวข้องได้รับทราบถึง รายละเอียดของการเปลี่ยนแปลง และสามารถปฏิบัติงานได้อย่างถูกต้อง
 - (7) มีกระบวนการถอยกลับสู่สภาพเดิม (Fall-back) ของระบบงาน หากเกิดข้อผิดพลาดระหว่างการเปลี่ยนแปลง
3. มีการติดตามประสิทธิภาพการทำงานของระบบเทคโนโลยีสารสนเทศและทรัพย์สินด้านเทคโนโลยีสารสนเทศประเภทอุปกรณ์ที่สำคัญ ให้ทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ เพื่อใช้เป็นข้อมูลในการประเมินสมรรถภาพและความเพียงพอ (capacity) ของระบบเทคโนโลยีสารสนเทศ ทรัพย์สินด้านเทคโนโลยีสารสนเทศประเภทอุปกรณ์ และบุคลากร รวมถึงเพื่อให้สามารถรองรับแผนการปฏิบัติงานในอนาคตได้อย่างมีประสิทธิภาพ
4. มีการกำหนดหน้าที่ความรับผิดชอบในการดำเนินงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและเครือข่ายที่สำคัญ ให้เกิดความชัดเจน และมีการควบคุมเพื่อให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้อง เพื่อหลีกเลี่ยงการใช้งานผิดวัตถุประสงค์ หรือโดยไม่มีสิทธิ์ เช่น จัดการแบ่งแยกส่วนคอมพิวเตอร์สำหรับการพัฒนาระบบงาน (Development Environment) และสำหรับการใช้งานจริง (Production Environment) ออกจากกัน

2.9.2 การป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี (Protection from malware)

วัตถุประสงค์

เพื่อให้มั่นใจว่าระบบเทคโนโลยีสารสนเทศได้รับการป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี

แนวทางการปฏิบัติ

1. มีการป้องกันและตรวจสอบโปรแกรมไม่ประสงค์ดี รวมทั้งแก้ไขเพื่อให้ระบบกลับมาใช้งานได้ตามปกติ (recover) โดยขั้นต่ำต้องกำหนดมาตรการ ดังนี้
 - (1) กำหนดนโยบายห้ามใช้ซอฟต์แวร์ที่ไม่ได้รับอนุญาต
 - (2) มีกระบวนการป้องกัน และตรวจสอบการใช้ซอฟต์แวร์ที่ไม่ได้รับอนุญาต และการใช้งานเว็บไซต์ที่อาจมีโปรแกรมไม่ประสงค์ดี
 - (3) ติดตั้งซอฟต์แวร์ตรวจสอบโปรแกรมไม่ประสงค์ดี และปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ พร้อมทั้งกำหนดผู้มีหน้าที่รับผิดชอบให้รายงานและแก้ไขปัญหากรณีพบภัยคุกคาม
 - (4) ตรวจสอบซอฟต์แวร์ระบบงานที่มีความสำคัญอย่างสม่ำเสมอ หากพบการติดตั้งหรือเปลี่ยนแปลงที่ไม่ได้รับอนุญาตควรจัดให้มีการตรวจสอบ
 - (5) จัดให้มีการติดตามและกลั่นกรองข่าวสารเกี่ยวกับภัยคุกคาม เพื่อให้ทราบข้อเท็จจริง รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้ตระหนักถึงภัยคุกคามดังกล่าว

2.9.3 การสำรองข้อมูล (Information Back-up)

วัตถุประสงค์

เพื่อเป็นแนวทางในการกำหนดการสำรองข้อมูล เพื่อป้องกันการสูญหายของข้อมูล และใช้ในการกู้ระบบในกรณีที่เกิดเหตุการณ์ต่าง ๆ อาทิ เช่น ภัยธรรมชาติ ระบบเสียหาย เป็นต้น

แนวทางการปฏิบัติ

1. มีนโยบายการสำรองข้อมูลสำคัญทางธุรกิจ รวมถึง ระบบปฏิบัติการ (Operating System) โปรแกรมระบบงานคอมพิวเตอร์ (Application System) ทั้งระบบซื้อขายหลักทรัพย์และระบบปฏิบัติการซื้อขายหลักทรัพย์ รวมทั้งชุดคำสั่งที่ใช้ทำงาน ให้ครบถ้วนสามารถพร้อมใช้งานได้อย่างต่อเนื่อง
 - (1) กำหนดขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูล โดยต้องมีรายละเอียดเกี่ยวกับ ข้อมูลที่ต้องสำรอง ความถี่ในการสำรองข้อมูล ประเภทสื่อบันทึกข้อมูล จำนวนที่ต้องสำรอง ขั้นตอนและวิธีการสำรองข้อมูลโดยละเอียด สถานที่และวิธีเก็บรักษาสื่อบันทึกข้อมูล และกระบวนการกู้คืนข้อมูลในกรณีที่ข้อมูลสูญหาย
 - (2) มีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) ของสถานที่ที่เก็บข้อมูลสำรองนอกสถานที่ โดยสถานที่ดังกล่าวและสื่อบันทึกข้อมูลนั้นต้องได้รับการป้องกันสอดคล้องกับระดับความสำคัญของระบบเทคโนโลยีสารสนเทศ
 - (3) กำหนดเป้าหมายในการสำรองข้อมูลและการกู้คืนข้อมูล เช่น ประเภทของข้อมูล และข้อมูลล่าสุดที่จะกู้คืนได้ (Recovery Point Objective: RPO)
 - (4) จัดให้มีการทดสอบข้อมูลสำรองและกระบวนการการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่า ข้อมูลและโปรแกรมระบบต่าง ๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและสามารถใช้งานได้ภายในระยะเวลาที่กำหนด ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ควรคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย เช่น กรณีที่จัดเก็บข้อมูลในสื่อบันทึกประเภทใดควรมีการเก็บอุปกรณ์และโปรแกรมที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นได้ด้วยเช่นกัน เป็นต้น

- (5) สื่อบันทึกที่ใช้เก็บข้อมูลต้องมีป้ายบอกรายละเอียด ซึ่งจะประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้
 - (ก) ชื่อระบบข้อมูล
 - (ข) วันที่ทำการสำรองข้อมูล
 - (ค) ระดับความสำคัญของข้อมูล
 - (ง) รายละเอียดสำหรับติดต่อผู้ดูแลข้อมูล

2.9.4 การบันทึก จัดเก็บหลักฐานและติดตาม (Logging and Monitoring)

วัตถุประสงค์

เพื่อบันทึกและจัดเก็บหลักฐานการใช้งานเกี่ยวกับระบบเทคโนโลยีสารสนเทศอย่างเพียงพอสำหรับการตรวจสอบการล่วงรู้ข้อมูลภายในระหว่างหน่วยงานและบุคลากร การสอบทานการใช้งานข้อมูลและระบบเทคโนโลยีสารสนเทศตามหน้าที่ที่ผู้ปฏิบัติงานได้รับมอบหมาย การตรวจสอบการเข้าใช้งานระบบเทคโนโลยีสารสนเทศโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง การตรวจสอบและป้องกันการใช้งานระบบสารสนเทศที่มีความผิดปกติหรือไม่เป็นไปตามที่กฎหมายหรือหลักเกณฑ์ของทางราชการ และการตรวจสอบตัวตนของลูกค้า ที่ทำการซื้อขายผ่านระบบอินเทอร์เน็ต รวมทั้งเพื่อให้มีการติดตามและวิเคราะห์หลักฐานที่จัดเก็บ

แนวทางการปฏิบัติ

1. จัดให้มีการบันทึกและจัดเก็บหลักฐาน (logs) ของระบบงานที่มีความสำคัญประเภทต่าง ๆ ดังต่อไปนี้
 - (1) หลักฐานการเข้าถึงพื้นที่หวงห้าม (physical access log) โดยขั้นต่ำต้องมีรายละเอียดเกี่ยวกับบุคคลที่เข้าถึง ความพยายามในการเข้าถึง (ถ้ามี) และวันเวลาที่ผ่านเข้าออก โดยจัดเก็บเป็นระยะเวลาไม่น้อยกว่า 6 เดือน
 - (2) หลักฐานการเข้าถึงระบบปฏิบัติการ ฐานข้อมูล ระบบเครือข่ายคอมพิวเตอร์ (authentication log) โดยขั้นต่ำต้องมีรายละเอียดเกี่ยวกับบัญชีผู้ใช้งาน วันเวลาที่เข้าใช้งาน และความพยายามในการเข้าใช้งาน โดยจัดเก็บเป็นระยะเวลาไม่น้อยกว่า 6 เดือน
 - (3) หลักฐานการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศ เช่น ระบบซื้อขาย ระบบปฏิบัติการหลักทรัพย์ หรือระบบงานอื่น ๆ ที่บริษัทฯ กำหนด (application log) โดยขั้นต่ำต้องมีรายละเอียดเกี่ยวกับบัญชีผู้ใช้งาน หมายเลขประจำเครื่องที่ใช้งาน (client IP address) (ถ้ามี) วันเวลาที่มีการใช้งาน order ID และ account ID โดยจัดเก็บเป็นระยะเวลาไม่น้อยกว่า 2 ปี
 - (4) หลักฐานการใช้งานอินเทอร์เน็ตที่เกิดขึ้นจากการใช้งานผ่านเครือข่ายสารสนเทศของบริษัท (internet access log) โดยขั้นต่ำต้องมีรายละเอียดเกี่ยวกับบัญชีผู้ใช้งาน หมายเลขประจำเครื่อง ที่ใช้งาน (IP address) หมายเลขอินเทอร์เน็ตของบริษัท (organization IP address) วันเวลาที่มีการใช้งาน และที่อยู่ของเว็บไซต์ปลายทาง (full URL) โดยจัดเก็บเป็นระยะเวลาไม่น้อยกว่า 2 ปี ทั้งนี้ หากบริษัทใช้หมายเลขประจำเครื่องแบบพลวัต (dynamic IP address) บริษัทต้องมีข้อมูลที่สามารถระบุผู้ใช้งานและหมายเลข IP address ในช่วงเวลาที่ใช้งานดังกล่าวได้ด้วย
 - (5) หลักฐานการใช้งานแฟ้มข้อมูล (audit log) โดยจัดเก็บเฉพาะบุคคลที่สามารถเข้าถึงข้อมูลภายใน เช่น read, write, copy และ delete เป็นต้น ตามประกาศว่าด้วยแนวทางปฏิบัติเกี่ยวกับระบบงานในการป้องกันมิให้เกิดการกระทำที่อาจมีความขัดหรือแย้งกับประโยชน์ของลูกค้า โดยจัดเก็บเป็นระยะเวลาไม่น้อยกว่า 6 เดือน
 - (6) หลักฐานการบริหาร (event log) และระบบปฏิบัติการ และ network firewall หลักฐานบันทึกข้อมูลจราจรคอมพิวเตอร์ (traffic log) ของ network firewall (network firewall log) และหลักฐานการจัดการบริหารข้อมูล (database log) โดยให้เป็นไปตามการประเมินความเสี่ยงขององค์กรและเพียงพอต่อการตรวจสอบ

- (7) หลักฐานการติดต่อสนทนาผ่านช่องทางอิเล็กทรอนิกส์ (electronic message) โดยจัดเก็บเฉพาะบุคคลที่สามารถเข้าถึงข้อมูลภายใน โดยขั้นต้นต้องมีรายละเอียดเกี่ยวกับบัญชีผู้ใช้งาน วันเวลาที่เข้าใช้งาน ข้อมูลการติดต่อตลอดระยะเวลาการสนทนา โดยจัดเก็บเป็นระยะเวลาไม่น้อยกว่า 6 เดือน
2. จัดให้มีการป้องกันข้อมูลและระบบการบันทึกและจัดเก็บหลักฐานการใช้งานเกี่ยวกับระบบเทคโนโลยีสารสนเทศของผู้ใช้งานทั่วไป รวมถึง system administrator logs และ system operator logs จากการถูกเปลี่ยนแปลงแก้ไข ทำความเสียหาย หรือเข้าถึงโดยไม่ได้รับอนุญาต และมีการตรวจสอบอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ
 3. กำหนดระบบเวลาของอุปกรณ์และระบบเทคโนโลยีสารสนเทศที่เกี่ยวกับการซื้อขายหลักทรัพย์และการชำระราคาให้ตรงกับเวลาอ้างอิงของระบบซื้อขายหลักทรัพย์ของตลาดหลักทรัพย์ ทั้งนี้ เพื่อให้การตรวจสอบธุรกรรมที่ไม่เหมาะสมทั้งหมดเป็นไปอย่างถูกต้องและมีประสิทธิภาพ

2.9.5 การควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน (Installation of Software on Operational Systems)

วัตถุประสงค์

เพื่อควบคุมให้ระบบงานทำงานโดยมีความถูกต้อง ครบถ้วน และน่าเชื่อถือ (integrity of operational system)

แนวทางการปฏิบัติ

มีขั้นตอนเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน รวมทั้งจัดให้มีมาตรการเพื่อจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งาน เพื่อให้ระบบปฏิบัติงานต่าง ๆ มีความถูกต้องครบถ้วนและน่าเชื่อถือ

2.9.6 การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศ เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ

แนวทางการปฏิบัติ

1. จัดให้มีการติดตามข้อมูลข่าวสารเกี่ยวกับช่องโหว่ทางเทคนิคที่อาจเป็นความเสี่ยงต่อ ระบบเทคโนโลยีสารสนเทศอย่างทันต่อเหตุการณ์ รวมทั้งต้องจัดให้มีการตรวจสอบหาช่องโหว่ดังกล่าวและมีมาตรการดำเนินการเพื่อปิดช่องโหว่หรือกำหนดแผนรองรับกรณีที่ระบบถูกบุกรุก ผ่านช่องโหว่
2. กำหนดผู้มีหน้าที่รับผิดชอบในการจัดการเกี่ยวกับช่องโหว่ทางเทคนิค โดยครอบคลุมถึงการประเมินความเสี่ยงของทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องซึ่งอาจได้รับผลกระทบจากช่องโหว่ดังกล่าว โดยเฉพาะทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง การดำเนินการเพื่อปิดช่องโหว่ (Patching) และการประสานงานกับบุคคลที่เกี่ยวข้อง
3. มีการประเมินความเสี่ยงของโปรแกรมเพื่อปิดช่องโหว่ (Patches) โดยก่อนการติดตั้งโปรแกรม ต้องมีการทดสอบและประเมินผลกระทบที่อาจเกิดจากการติดตั้งโปรแกรดังกล่าว ทั้งนี้ กรณีที่ไม่มีโปรแกรมเพื่อปิดช่องโหว่ ให้ปฏิบัติตามคำแนะนำของบริษัท ผู้ผลิตทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง
4. มีการประเมินความเสี่ยงระบบอื่น ๆ จากการบุกรุกผ่านระบบเครือข่ายคอมพิวเตอร์ที่ใช้สื่อสารภายในองค์กร เพื่อกำหนดขอบเขตการทดสอบการเจาะระบบตามความเหมาะสม
5. มีการกำหนดกรอบระยะเวลาการติดตั้ง patch โดยคำนึงถึงความจำเป็นและความเสี่ยงจากการถูกโจมตีจากช่องโหว่
6. มีการตรวจสอบความถูกต้องและการทดสอบ patch ก่อนการดำเนินการติดตั้งบนระบบที่ให้บริการจริง เพื่อป้องกันผลกระทบที่ไม่พึงประสงค์จากการติดตั้ง patch

7. มีการทดสอบการบุกรุกระบบ (Penetration Test) กับระบบงานที่มีความสำคัญทุกระบบ โดยอาจพิจารณาเลือกจัดทำ การทดสอบกับบางระบบงานตามการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) โดยต้องจัดทำ การทดสอบอย่างน้อยทุก 3 ปี และ/หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ อย่างไรก็ตาม ยังคงต้องจัดให้มีการทดสอบกับ ระบบงานที่มีความสำคัญอื่น ๆ ให้ครบถ้วน อย่างน้อยทุก 6 ปี
8. มีการกำหนดให้จัดให้มีการทดสอบการเจาะระบบที่ครอบคลุมระบบงาน (application system) และระบบเครือข่ายที่มี ช่องทางเชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงระบบ ดังกล่าวอย่างมีนัยสำคัญ
9. กระบวนการจัดการช่องโหว่ด้านเทคนิคต้องสอดคล้องกับกระบวนการจัดการเหตุการณ์ ที่อาจส่งผลกระทบต่อความ มั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (Incident Management) เพื่อเตรียมความพร้อมรองรับกรณีที่ระบบถูก บุกรุกผ่านช่องโหว่ ทั้งนี้ ให้รวมถึงกรณีที่ต้องตรวจพบ ช่องโหว่แต่ยังไม่สามารถหาวิธีปิดช่องโหว่ได้
10. มีการบันทึกและจัดเก็บหลักฐานเพื่อการตรวจสอบในการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับการจัดการช่องโหว่ทางเทคนิค
11. มีการประเมินช่องโหว่ของระบบ (vulnerability assessment) กับระบบงานที่มีความสำคัญทุกระบบอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ และรายงานผลไปยังหน่วยงานกำกับกับการปฏิบัติงาน หรือหน่วยงานตรวจสอบภายในโดยไม่ชักช้า

2.9.7 การตรวจสอบระบบเทคโนโลยีสารสนเทศ (Information Systems Audit)

วัตถุประสงค์

เพื่อให้จัดให้มีการวางแผนการตรวจสอบระบบเทคโนโลยีสารสนเทศอย่างเพียงพอเหมาะสม โดยการตรวจสอบดังกล่าวต้อง ส่งผลกระทบต่อการใช้งานน้อยที่สุด

แนวทางการปฏิบัติ

1. มีการวางแผนการตรวจสอบระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้
2. กำหนดขอบเขตการตรวจสอบทางเทคนิค (technical audit test) ให้ครอบคลุมจุดเสี่ยงที่สำคัญ และต้องควบคุมการ ตรวจสอบดังกล่าวไม่ให้กระทบต่อการปฏิบัติงานตามปกติ
3. ในกรณีที่การตรวจสอบระบบเทคโนโลยีสารสนเทศมีโอกาสกระทบต่อความพร้อมใช้งานของระบบ (system availability) ต้องจัดให้ตรวจสอบระบบเทคโนโลยีสารสนเทศนอกเวลาทำการ

2.9.8 การตั้งค่าด้านความมั่นคงปลอดภัย (Security Configuration Standard)

วัตถุประสงค์

เพื่อให้มั่นใจว่ามีการกำหนดให้จัดทำมาตรฐานการตั้งค่าด้านความมั่นคงปลอดภัยสำหรับระบบปฏิบัติการ ระบบฐานข้อมูล และอุปกรณ์เครือข่ายที่มีความเหมาะสม

แนวทางการปฏิบัติ

1. กำหนดให้มีการลบบัญชีผู้ใช้งานเริ่มต้น (default user) หรือการเปลี่ยนแปลงรหัสผ่านเริ่มต้น (default password)
2. มีการกำหนดวิธีการยืนยันตัวตนที่มีความรัดกุมปลอดภัย
3. การกำหนดให้ตั้งค่าความมั่นคงปลอดภัยของระบบและอุปกรณ์ตามมาตรฐานที่กำหนดไว้ (security hardening) ก่อน การนำไปใช้งาน
4. มีการกำหนดบริการ แอปพลิเคชัน และพอร์ตการเชื่อมต่อเท่าที่จำเป็น
5. มีการจัดเก็บข้อมูลบันทึกเหตุการณ์ (log)
6. มีการปรับปรุงเวอร์ชันของซอฟต์แวร์และ firmware ให้เป็นปัจจุบันอยู่เสมอ

7. กำหนดให้มีการสอบทานการตั้งค่าด้านความมั่นคงปลอดภัยของระบบปฏิบัติการ ระบบฐานข้อมูล และอุปกรณ์เครือข่าย อย่างสม่ำเสมอ และทุกครั้งที่มีการเปลี่ยนแปลงระบบและอุปกรณ์ดังกล่าวอย่างมีนัยสำคัญ

2.10 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (Communications Security)

2.10.1 การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ (Network Security Management)

วัตถุประสงค์

เพื่อป้องกันการกระทำที่มีความเสี่ยงสูงต่อข้อมูลสารสนเทศในระบบเครือข่ายคอมพิวเตอร์ และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯ

แนวทางการปฏิบัติ

1. มีการบริหารจัดการและควบคุมระบบเครือข่ายคอมพิวเตอร์อย่างมั่นคงและปลอดภัย โดยต้องสามารถป้องกันมิให้เกิดการกระทำที่มีความเสี่ยงต่อข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ โดยมีการดำเนินการขั้นต่ำ ดังนี้
 - (1) แบ่งแยกหน้าที่ความรับผิดชอบระหว่าง network administrator และ computer administrator ออกจากกัน พร้อมทั้งกำหนดหน้าที่ความรับผิดชอบและขั้นตอนในการบริหารจัดการระบบ และอุปกรณ์เครือข่ายให้ชัดเจน
 - (2) จำกัดการเชื่อมต่อระบบคอมพิวเตอร์ระหว่างเครือข่าย เช่น จำกัดการใช้งานจุดเชื่อมต่อระบบเครือข่าย (port outlet)
 - (3) เปิดใช้งาน service port ที่เชื่อมต่อตามความจำเป็น พร้อมทั้งมีวิธีการเพื่อระบุถึงอุปกรณ์ที่เชื่อมต่อ (authenticate) อย่างชัดเจน เช่น IP address และประเภทของอุปกรณ์ เป็นต้น
 - (4) มีการควบคุมการเชื่อมต่อกับระบบเครือข่ายสาธารณะ (public network) และระบบเครือข่ายไร้สาย (wireless network) อย่างรัดกุม เพื่อป้องกันการรั่วไหลหรือเปลี่ยนแปลงแก้ไขข้อมูลที่ส่งผ่านระบบเครือข่ายดังกล่าว รวมทั้งเพื่อป้องกันระบบที่เชื่อมต่อและแอปพลิเคชันที่ใช้งาน เช่น การเข้ารหัสเครือข่าย หรือการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ออกจากกัน เป็นต้น นอกจากนี้ ควรจัดให้มีการควบคุมเป็นพิเศษเพื่อให้ระบบเครือข่ายดังกล่าวอยู่ในสภาพที่พร้อมใช้งานอยู่เสมอ เช่น จัดให้มีระบบเครือข่ายคอมพิวเตอร์ที่ใช้งานทดแทนกันได้ (network load balance) เป็นต้น
 - (5) มีการบันทึกและจัดเก็บหลักฐาน (logs) เพื่อติดตามตรวจสอบการทำงานที่เกี่ยวข้อง หรืออาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์
2. จัดทำข้อตกลงการใช้บริการผ่านระบบเครือข่ายคอมพิวเตอร์ที่เกี่ยวกับวิธีการบริหารจัดการคุณภาพการให้บริการ และกระบวนการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์กับผู้รับดำเนินการ
3. แบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยระบุขอบเขตของระบบเครือข่ายย่อยอย่างชัดเจน และมีกระบวนการควบคุมการเข้าถึงขอบเขตดังกล่าวอย่างเหมาะสม

2.10.2 การควบคุมการรับส่งข้อมูลสารสนเทศ (Information Transfer)

วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยในการรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายภายในองค์กร และระหว่างระบบเครือข่ายภายในองค์กรกับระบบเครือข่ายภายนอก

แนวทางการปฏิบัติ

1. มีนโยบายการรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายภายในองค์กร และระหว่างเครือข่ายภายในองค์กรกับระบบ

เครือข่ายภายนอกองค์กร ให้มีความมั่นคงปลอดภัย และกำหนดมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่มีการรับส่งผ่านระบบเครือข่ายคอมพิวเตอร์ โดยมีการดำเนินการ ดังต่อไปนี้

- (1) จัดให้มีนโยบายและหลักปฏิบัติเพื่อปกป้องข้อมูลสารสนเทศที่รับส่งผ่านระบบและอุปกรณ์ในการสื่อสารทุกประเภท โดยมีเนื้อหาขั้นต่ำครอบคลุมถึง
 - (ก) แนวปฏิบัติที่ดีในการรับส่งข้อมูลสารสนเทศผ่านช่องทางการสื่อสารอิเล็กทรอนิกส์ประเภทต่าง ๆ
 - (ข) กระบวนการป้องกันการรับส่งข้อมูลสารสนเทศนอกเส้นทางที่ได้กำหนดไว้ (mis-routing) การดักจับสัญญาณ การเปลี่ยนแปลงแก้ไขหรือทำความเสียหายกับข้อมูล และโปรแกรมไม่ประสงค์ดี (malware) ที่ถูกส่งผ่านช่องทางการสื่อสาร
 - (ค) กระบวนการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญที่รับส่งในรูปแบบของไฟล์แนบ (attachment files) และการส่งต่อจดหมายอิเล็กทรอนิกส์แบบอัตโนมัติออกสู่ภายนอกองค์กร
 - (ง) การนำเทคนิคการเข้ารหัสข้อมูลมาใช้ในการรับส่งข้อมูลสารสนเทศที่เป็นความลับและมีความสำคัญผ่านช่องทางการสื่อสารบางประเภทที่ต้องการการรักษาความมั่นคงปลอดภัย เช่น การใช้งานระบบ cloud computing เป็นต้น
- (2) ในการใช้งานระบบรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (electronic messaging) บริษัทฯ ได้กำหนดมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่รับส่งผ่านช่องทางดังกล่าว โดยจัดให้มีมาตรการป้องกันการเปลี่ยนแปลงแก้ไข ทำความเสียหาย หรือเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และมีกระบวนการตรวจสอบผู้ใช้งานอย่างเข้มงวดในกรณีที่ใช้งานผ่านเครือข่ายสาธารณะรวมทั้งจัดการและควบคุมให้ระบบทำงานรับส่งข้อมูลได้อย่างถูกต้องและพร้อมใช้งานอยู่เสมอ ทั้งนี้ การใช้งานระบบรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ที่ให้บริการโดยบุคคลภายนอก เช่น โปรแกรมสนทนาผ่านบิตทอร์นิกส์ (instant messaging) ระบบเครือข่ายสังคมออนไลน์ (social networking) หรือโปรแกรมเรียกใช้แฟ้มข้อมูลร่วมกัน (file sharing) บริษัทฯ จัดให้มีการควบคุมดูแลอย่างเหมาะสมเพียงพอ เช่น มีการขออนุมัติก่อนการใช้งาน รวมถึงควรปฏิบัติตามกฎหมายและหลักเกณฑ์ของทางราชการอย่างเคร่งครัด
2. ผู้ใช้งานและผู้รับดำเนินการ (ถ้ามี) มีข้อตกลงเกี่ยวกับการรักษาความลับหรือไม่เปิดเผยข้อมูลที่มีความสำคัญตาม โดยมีเนื้อหาขั้นต่ำครอบคลุมถึง
 - (1) การระบุความเป็นเจ้าของข้อมูลสำคัญทางธุรกิจ ทรัพย์สินทางปัญญา และวิธีป้องกันการรั่วไหลของข้อมูล
 - (2) การป้องกันการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต โดยจัดให้มีการลงนามโดยผู้รับผิดชอบ
 - (3) การกำหนดขั้นตอนการขออนุญาตเข้าถึงข้อมูลหรือกำหนดสิทธิการเข้าถึงข้อมูลตามที่ได้ลงนาม
 - (4) การกำหนดสิทธิการเข้าถึงข้อมูลเพื่อตรวจสอบหรือติดตามการใช้งานข้อมูลที่มีความสำคัญ
 - (5) การกำหนดกระบวนการแจ้งเตือนและรายงานผู้เกี่ยวข้องหากพบการรั่วไหลหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
 - (6) การกำหนดมาตรการดำเนินการกรณีละเมิดหรือยกเลิกข้อตกลง รวมทั้ง ข้อกำหนดในการคืนหรือทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดข้อตกลง

2.11 การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ

2.11.1 การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Security Requirements of Information Systems)

วัตถุประสงค์

เพื่อกำหนดให้กระบวนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นส่วนหนึ่งของระบบสารสนเทศของทั้งภายในองค์กรและที่เกี่ยวข้องกับการให้บริการภายนอกผ่านเครือข่ายสาธารณะ ตลอดช่วงอายุการใช้งานระบบสารสนเทศ (entire life cycle) ได้แก่ กระบวนการจัดหา กระบวนการพัฒนาระบบ (system development life cycle) การใช้งาน และการดูแลรักษา

แนวทางการปฏิบัติ

1. มีการกำหนดความต้องการด้านความมั่นคงปลอดภัยไว้อย่างชัดเจนในระบบที่จะพัฒนาขึ้นมาใช้งาน หรือซื้อมาใช้งาน
2. ทำการวิเคราะห์ระบบเทคโนโลยีสารสนเทศ ว่ามีความเสี่ยงใดบ้างที่จะทำให้ข้อมูลเกิดความเสียหาย โดยมุ่งเน้นในส่วนต่าง ๆ ดังนี้
 - (1) มาตรการปฏิบัติก่อนที่จะเกิดความเสียหาย อาทิ การสำรองข้อมูล ระบบเครือข่ายสำรอง
 - (2) มาตรการปฏิบัติหลังจากเกิดความเสียหาย อาทิ แผนการกู้คืนข้อมูล ระยะเวลาในการกู้คืนข้อมูล
3. จัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่ผ่านระบบให้บริการ การใช้งาน (Application Service) ทั้งในกรณีทั่วไปและกรณีผ่านเครือข่ายสาธารณะ เพื่อป้องกัน การกระทำผิดในลักษณะทุจริต (Fraudulent Activities) การทำธุรกรรมที่ไม่สมบูรณ์หรือผิดพลาด (Incomplete Transmission or Mis-routing) หรือการเปิดเผย คัดลอก หรือเปลี่ยนแปลงแก้ไขข้อมูล โดยไม่ได้รับอนุญาต

2.11.2 การรักษาความมั่นคงปลอดภัยในกระบวนการพัฒนาระบบสารสนเทศ (Security in development and support process)

วัตถุประสงค์

เพื่อให้การพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศประมวลผลได้อย่างถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน (change management) รวมถึง การรักษาไว้ซึ่งความมั่นคงปลอดภัยของระบบสารสนเทศตลอดช่วงการพัฒนากระบวนการงานสารสนเทศ (system development life cycle)

แนวทางการปฏิบัติ

1. มีการควบคุมการพัฒนาหรือการแก้ไขเปลี่ยนแปลงระบบสารสนเทศในทุกขั้นตอน โดยให้เป็นไปตามขั้นตอนการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศที่กำหนดไว้ และมีกระบวนการขั้นต่ำ ดังนี้
 - (1) ประเมินผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง
 - (2) กำหนดวิธีปฏิบัติให้คำขอให้แก้ไขหรือพัฒนาต้องมาจากผู้ที่มีสิทธิและอนุมัติคำขอโดยผู้มีอำนาจ ควบคุมผลข้างเคียงที่อาจเกิดขึ้นเนื่องจากการแก้ไข ตรวจสอบจากผู้มีอำนาจภายหลังการแก้ไขหรือพัฒนาแล้วเสร็จก่อนโอนย้ายระบบงาน รวมทั้ง จัดเก็บรายละเอียดของคำขอไว้
 - (3) กำหนดวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน บันทึกเหตุผลความจำเป็น และขออนุมัติจากผู้มีอำนาจทุกครั้ง
 - (4) ปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้มีการแก้ไขเปลี่ยนแปลง เพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม และควรจัดเก็บเอกสารดังกล่าวในที่ปลอดภัยและสะดวก ต่อการใช้งาน

- (5) จัดเก็บโปรแกรม version ก่อนการเปลี่ยนแปลงไว้ใช้งาน หรือมีกระบวนการถอยกลับสู่สภาพเดิม (fall-back) ของระบบงาน ในกรณีระบบงานผิดพลาดหรือไม่สามารถใช้งานได้
 - (6) สื่อสารให้กับบุคคลที่เกี่ยวข้องได้รับทราบและสามารถปฏิบัติงานได้อย่างถูกต้อง
 - (7) บันทึกและจัดเก็บหลักฐานทั้งหมด (audit trail) ที่เกี่ยวข้องกับการเปลี่ยนแปลง เพื่อใช้ประกอบในกรณีที่มีการตรวจสอบ
2. มีการทดสอบระบบสารสนเทศที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าระบบสารสนเทศดังกล่าวทำงานได้อย่างมีประสิทธิภาพ สามารถประมวลผลได้อย่างถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน
 3. มีการทดสอบระบบสารสนเทศที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน พร้อมทั้งปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจ (business continuity plan)
 4. มีการควบคุมบุคลากร ขั้นตอน และเทคโนโลยีสำหรับการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัยตลอดขั้นตอนการพัฒนาระบบ
 - (1) การรักษาความลับของข้อมูลที่น่ามาประมวลผล จัดเก็บ และส่งผ่านระบบ และการควบคุม การนำข้อมูลเข้าและออกจากระบบที่อยู่ระหว่างการพัฒนา
 - (2) การควบคุมการเข้าถึงสภาพแวดล้อมของการพัฒนาระบบสารสนเทศอย่างรัดกุมเหมาะสม
 5. มีการดูแล ติดตาม และควบคุมการพัฒนาระบบสารสนเทศของผู้รับดำเนินการให้เป็นไปตามข้อตกลงการใช้บริการ
 6. มีการทดสอบการทำงานของระบบสารสนเทศที่ได้รับการพัฒนาโดยผู้ใช้งานหรือผู้ทดสอบที่เป็นอิสระจากผู้พัฒนาระบบสารสนเทศ เพื่อให้มั่นใจได้ว่าระบบที่ได้รับการพัฒนาดังกล่าวสามารถทำงานได้อย่างถูกต้องตรงตามความต้องการของผู้ใช้งาน และจัดให้มีแนวทางควบคุมและป้องกันการรั่วไหลของข้อมูลที่ใช้ในการทดสอบ หากข้อมูลดังกล่าวเป็นความลับหรือมีความสำคัญ

2.12 การให้บริการระบบสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing)

2.12.1 การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศจากผู้รับดำเนินการ (Information Security in IT Outsourcing)

วัตถุประสงค์

เพื่อป้องกันทรัพย์สินสารสนเทศของบริษัทฯ จากการเข้าถึงโดยผู้รับดำเนินการอย่างไม่เหมาะสม

แนวทางการปฏิบัติ

1. จัดให้มีมาตรการในการควบคุมดูแลผู้รับดำเนินการในงานที่เกี่ยวข้องกับระบบสารสนเทศของบริษัทฯ อย่างเป็นลายลักษณ์อักษรเพื่อลดความเสี่ยงจากการเข้าถึงทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างไม่เหมาะสม ทั้งนี้ มาตรการดังกล่าวมีเนื้อหาขั้นต่ำครอบคลุมประเด็น ดังต่อไปนี้
 - (1) กำหนดวิธีการคัดเลือกและประเมินผู้รับดำเนินการ (Due diligence) โดยให้ความสำคัญในเรื่องการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่สำคัญ (Confidentiality) ความถูกต้องเชื่อถือได้ของข้อมูลและระบบสารสนเทศ (Integrity) และความพร้อมใช้งานของระบบสารสนเทศที่ใช้บริการ (Availability) เช่น ผู้รับดำเนินการควรมีแผนรองรับกรณีเกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (incident response policy) โดยคำนึงถึงแผนของบริษัทฯ รวมทั้งมีกระบวนการการกู้คืนระบบงานให้เป็นไปตามข้อตกลงที่ได้กำหนดไว้ เพื่อให้ข้อมูลและการประมวลผลข้อมูลอยู่ในสภาพที่พร้อมใช้งานเสมอ เป็นต้น

- (2) กำหนดการทบทวนคุณสมบัติของผู้รับดำเนินการอย่างสม่ำเสมอ เช่น ฐานะทางการเงิน ความเพียงพอของการให้บริการ (capacity planning) เพื่อให้มั่นใจว่าผู้รับดำเนินการยังคงมีความพร้อมในการให้บริการที่เพียงพอต่อความต้องการของบริษัทอย่างต่อเนื่อง
- (3) กำหนดข้อตกลงเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและกระบวนการควบคุมอย่างเป็นลายลักษณ์อักษร และการลงนามร่วมกันระหว่างบริษัท และผู้รับดำเนินการ ทั้งนี้ บริษัท ต้องมั่นใจได้ว่าผู้รับดำเนินการมีหน้าที่รับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเสมือนกับบริษัท ดำเนินการด้วยตนเอง
- (4) กำหนดหน้าที่ความรับผิดชอบของผู้รับดำเนินการ
- (5) มีการระบุประเภทข้อมูลสารสนเทศที่อนุญาตให้ผู้รับดำเนินการเข้าถึง เพื่อให้การกำหนดมาตรการควบคุมและติดตามการเข้าถึงข้อมูลเป็นไปอย่างเหมาะสม ภายใต้หลักความจำเป็นในการรู้ข้อมูล (need-to-know basis)
- (6) จัดให้มีขั้นตอนและกระบวนการติดตามควบคุมการเข้าถึงสารสนเทศอย่างเหมาะสม
- (7) มีการรักษาความมั่นคงปลอดภัยในกรณีที่มีการเคลื่อนย้ายหรือถ่ายโอนข้อมูลสารสนเทศ
- (8) มีการควบคุมความครบถ้วนถูกต้องของข้อมูลและการประมวลผลข้อมูลที่ได้รับจากผู้รับดำเนินการ
- (9) กำหนดกระบวนการควบคุมอย่างเป็นมาตรฐานเพื่อติดตามการทำงานของผู้รับดำเนินการ
3. มีข้อตกลงเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยมีเนื้อหาขั้นต่าดังนี้
 - (1) รายละเอียดของข้อมูลที่ต้องใช้หรือเข้าถึงโดยผู้รับดำเนินการ รวมทั้ง วิธีการเข้าถึงข้อมูลดังกล่าว
 - (2) การจัดแบ่งประเภทข้อมูลซึ่งสอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
 - (3) มีมาตรการดำเนินการเพื่อให้มั่นใจได้ว่าข้อมูลที่เป็นความลับหรือมีความสำคัญ ทรัพย์สินทางปัญญา และลิขสิทธิ์ของบริษัท ได้รับการคุ้มครองอย่างปลอดภัยตามกฎหมายและหลักเกณฑ์ ของทางที่เกี่ยวข้อง
 - (4) กำหนดหน้าที่ความรับผิดชอบของผู้รับดำเนินการในการปฏิบัติงานภายใต้การควบคุมต่าง ๆ เช่น กำหนดเงื่อนไขการเข้าถึงข้อมูลของผู้ให้บริการ ติดตามตรวจสอบการปฏิบัติงานของผู้รับดำเนินการให้เป็นไปตามข้อตกลงของผู้ให้บริการ กำหนดให้ผู้รับดำเนินการรายงานผลการปฏิบัติงานให้ผู้ให้บริการทราบเมื่อร้องขอ การแก้ไขปัญหาต่าง ๆ ภายในระยะเวลาที่กำหนด รวมทั้ง การปฏิบัติงานให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของผู้ให้บริการ
 - (5) แนวทางการใช้งานข้อมูลสารสนเทศอย่างถูกต้องเหมาะสม ทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)
 - (6) แนวทางการแก้ไขปัญหากรณีที่เกิดข้อผิดพลาดจากการปฏิบัติหน้าที่
 - (7) รายชื่อและช่องทางสำหรับติดต่อบุคคลหรือหน่วยงานอื่น ๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งบุคคลหรือหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
 - (8) มีข้อกำหนดเพิ่มเติมเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศกรณีที่ได้รับดำเนินการมอบหมายการปฏิบัติงานให้กับบุคคลอื่นต่อ (sub-contracting to another supplier)
4. มีมาตรการตรวจสอบดูแลให้ผู้รับดำเนินการปฏิบัติตามหลักเกณฑ์การปฏิบัติงานที่สำนักงาน ก.ล.ต. หรือคณะกรรมการกำกับตลาดทุน กำหนดเกี่ยวกับงานที่รับดำเนินการ รวมทั้ง ระเบียบวิธีปฏิบัติที่บริษัทกำหนดขึ้นเพื่อให้เป็นไปตามหลักเกณฑ์ดังกล่าว โดยอย่างน้อยมาตรการดังกล่าวต้องสามารถควบคุมให้ผู้รับดำเนินการไม่มีลักษณะที่จะทำให้มีเหตุอันควรเชื่อได้ว่ามีข้อบกพร่องหรือมีความไม่เหมาะสมเกี่ยวกับการควบคุมและการปฏิบัติงานอันของธุรกิจ
5. มีแผนรองรับในกรณีที่เกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (incident response policy)

- กำหนดสิทธิในการเข้าตรวจสอบกระบวนการปฏิบัติงานของผู้รับดำเนินการและความคุมให้การปฏิบัติงานเป็นไปตามข้อตกลงที่กำหนดไว้ เว้นแต่ในกรณีที่ผู้รับดำเนินการมีข้อจำกัดในการเข้าตรวจสอบการปฏิบัติงานดังกล่าว บริษัทฯ ต้องมีมาตรการเพื่อให้มั่นใจได้ว่าสามารถควบคุมการปฏิบัติงานของผู้รับดำเนินการให้เป็นไปตามข้อตกลงที่กำหนดไว้ได้
- มีข้อกำหนดให้ผู้รับดำเนินการยินยอมให้สำนักงานเรียกดู ตรวจสอบเอกสารหลักฐานที่เกี่ยวข้อง หรือสามารถเข้าตรวจสอบการปฏิบัติงานของผู้รับดำเนินการ

2.12.2 การควบคุมการส่งมอบงานของผู้รับดำเนินการ (Supplier Service Delivery Management)

วัตถุประสงค์

เพื่อควบคุมผู้รับดำเนินการส่งมอบงานให้เป็นไปตามข้อตกลงที่จัดทำไว้กับบริษัทฯ

แนวทางปฏิบัติ

- มีการติดตาม ประเมิน ทบทวน และตรวจสอบผู้รับดำเนินการอย่างสม่ำเสมอ ทั้งในด้านฐานะทางการเงิน กระบวนการปฏิบัติงาน และประสิทธิภาพการให้บริการของผู้รับดำเนินการ ในกรณีที่บริษัทฯ แต่งตั้งบุคคลอื่นเป็นผู้รับดำเนินการในงานที่เกี่ยวข้องกับระบบสารสนเทศของบริษัทฯ
- ในกรณีที่ผู้รับดำเนินการ มีการเปลี่ยนแปลงกระบวนการ ขั้นตอน วิธีการปฏิบัติงานในการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน หรือเปลี่ยนตัวผู้รับดำเนินการ ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีการประเมินความเสี่ยงจากการเปลี่ยนแปลงดังกล่าว และกำหนดกระบวนการบริหารจัดการความเสี่ยงดังกล่าวให้สอดคล้องเหมาะสม

2.13 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศได้รับการดำเนินการอย่างถูกต้องมีประสิทธิภาพ ในช่วงระยะเวลาที่เหมาะสม

แนวทางการปฏิบัติ

- กำหนดขั้นตอนและกระบวนการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รวมทั้ง กำหนดผู้มีหน้าที่รับผิดชอบซึ่งมีความรู้ความสามารถและประสบการณ์ โดยกำหนดขั้นตอนและกระบวนการขั้นต่ำ ดังนี้
 - (1) กำหนดแผนรองรับในกรณีที่เกิดเหตุการณ์อย่างเป็นลายลักษณ์อักษร
 - (2) ประเมินเหตุการณ์หรือจุดอ่อนของมาตรการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และพิจารณาว่าควรจัดเป็นเหตุการณ์และมีระดับความรุนแรงที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ
 - (3) ดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่เกิดขึ้นอย่างมีประสิทธิภาพ เพื่อให้เหตุการณ์คลี่คลายหรือกลับสู่ภาวะปกติอย่างรวดเร็ว
 - (4) รวบรวมและจัดเก็บหลักฐานโดยไม่ชักช้า เมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศที่มีความสำคัญอย่างมีนัยสำคัญ เช่น ก่อให้เกิดความเสียหายกับข้อมูลหรือทรัพย์สินของลูกค้า โดยคำนึงถึงประเด็นสำคัญต่าง ๆ เช่น มีกระบวนการการจัดเก็บอย่างมั่นคงปลอดภัย การกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้อง การคัดเลือกบุคคลที่มีความรู้ความสามารถหรือมีประสบการณ์ด้านการรวบรวมและจัดเก็บหลักฐานเพื่อวิเคราะห์ตรวจสอบและจัดทำเอกสารสรุปนำเสนอต่อบุคคลที่มีหน้าที่รับผิดชอบ เป็นต้น ทั้งนี้ การรวบรวมจัดเก็บ และนำเสนอหลักฐาน ควรสอดคล้องกับหลักเกณฑ์ของกฎหมายที่ใช้บังคับ
 - (5) บันทึกและจัดเก็บหลักฐานการบริหารจัดการตามความจำเป็นและเหมาะสม

- (6) รายงานให้สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์รับทราบถึงสถานการณ์และผลการบริหารจัดการ
- (7) ตรวจสอบ ติดตาม วิเคราะห์ และรายงานเหตุการณ์ ทั้งนี้ ให้รวมถึงการวิเคราะห์ภายหลังเหตุการณ์ยุติแล้ว เพื่อระบุถึงสาเหตุของเหตุการณ์และเพื่อใช้ประโยชน์จากผลการวิเคราะห์ในการเตรียมความพร้อมรองรับเหตุการณ์ที่อาจเกิดขึ้นได้อีกในอนาคต
2. กำหนดผู้ที่มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยจัดให้มีบุคคลหรือหน่วยงานเพื่อทำหน้าที่รับแจ้งเหตุการณ์ (point of contact) และรายงานเหตุการณ์ต่อคณะผู้บริหารหรือผู้เกี่ยวข้องให้ทราบและดำเนินการต่อไป (escalation)
3. รายงานต่อผู้ที่มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ตามข้อ 2. และสำนักงาน ก.ล.ต. โดยไม่ชักช้าเมื่อเกิดเหตุการณ์ดังกล่าว โดยคณะทำงานเพื่อแก้ไขปัญหาจากเหตุการณ์ผิดปกติ ต้องมีการรายงานสถานการณ์ที่เกิดขึ้นอย่างรวดเร็วและทันต่อเหตุการณ์ บันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยจะต้องมีการดำเนินการ ดังนี้
 - (1) จัดทำรายงานที่เป็นมาตรฐานเพื่อรองรับการรายงานสถานการณ์ และสร้างความเข้าใจให้กับผู้รายงานเกี่ยวกับการดำเนินการต่าง ๆ ที่จำเป็นในกรณีที่เกิดเหตุการณ์ โดยรายงานต้องประกอบด้วย วันเวลา เหตุการณ์ ผลกระทบต่าง ๆ ที่คาดว่าจะเกิดขึ้น การดำเนินการแก้ไข ผลการแก้ไข ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางการป้องกันปัญหาในอนาคต
 - (2) รายงานต่อคณะผู้บริหารเมื่อทราบเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย เช่น การพบช่องโหว่ในการควบคุมความมั่นคงปลอดภัย (Ineffective Security Control) เกิดเหตุการณ์ที่อาจส่งผลกระทบต่อการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของระบบเทคโนโลยีสารสนเทศ ข้อผิดพลาดจากการปฏิบัติงาน (Human Errors) การบุกรุกด้านกายภาพ (Breaches of Physical Security Arrangements) การปฏิบัติงานที่ไม่เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (Non-compliance with Policies) การเปลี่ยนแปลงระบบปฏิบัติการหรือชุดคำสั่งที่ควบคุมระบบงานโดยไม่ได้รับอนุญาต (Uncontrolled System Changes) การทำงานผิดพลาดของโปรแกรมและอุปกรณ์คอมพิวเตอร์ (Malfunctions of Software or Hardware) และการเข้าถึงโดยไม่ได้รับอนุญาต (Access Violations)
 - (3) รายงานต่อสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ เมื่อมีเหตุการณ์ที่ส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศที่มีความสำคัญ ดังต่อไปนี้
 - (ก) ระบบการปฏิบัติงานหยุดชะงัก (System Disruption)
 - (ข) มีการบุกรุก เข้าถึง หรือใช้งานระบบโดยไม่ได้รับอนุญาต (System Compromised)
 - (ค) เหตุการณ์ที่ส่งผลกระทบต่อชื่อเสียงของบริษัทฯ (Harm to Reputation) เช่น ถูกปลอมแปลงหน้าเว็บไซต์ของบริษัทฯ (Website Defacement) โดยให้มีขั้นตอนการรายงาน ดังนี้
 - รายงานทันทีเมื่อทราบเหตุการณ์ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ และผลกระทบ ที่คาดว่าจะเกิดขึ้น ทั้งนี้ อาจแจ้งโดยวาจาหรือผ่านระบบรับส่งข้อความผ่านทางอิเล็กทรอนิกส์ (Electronic Messaging) ตามความเหมาะสม
 - รายงานภายในวันทำการถัดไปหลังทราบเหตุการณ์เป็นลายลักษณ์อักษร โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ที่เกิดขึ้น ผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหา และความคืบหน้าในการแก้ไขปัญหา

- รายงานเมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จเป็นลายลักษณ์อักษร โดยมีเนื้อหาครอบคลุมถึงวัน เวลา ประเภทเหตุการณ์ เหตุการณ์ที่เกิดขึ้น ผลกระทบและค่าใช้จ่ายที่เกิดขึ้น การดำเนินการแก้ไขปัญหา ผลการแก้ไขปัญหา ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางป้องกันในอนาคต
- (4) มีการแจ้งบุคคลที่เกี่ยวข้องต่าง ๆ เช่น ลูกค้า และตลาดหลักทรัพย์แห่งประเทศไทย ให้รับทราบโดยไม่ชักช้า ในกรณีที่เหตุการณ์ ส่งผลกระทบต่อบุคคลดังกล่าว
- 4. จัดให้มีการรายงานความคืบหน้าในการบริหารจัดการสถานการณ์และผลการบริหารจัดการเป็นระยะ และเมื่อเหตุการณ์ยุติแล้วมีการทดสอบขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามข้อ 1. อย่างน้อยปีละ 1 ครั้ง โดยอย่างน้อยต้องครอบคลุมถึงการบริหารจัดการความเสี่ยงไซเบอร์ (cyber security drill)
- 5. มีการพิจารณาบทวนขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ หลังจากที่มีการทดสอบตามข้อ 4. แล้วอย่างน้อยปีละ 1 ครั้ง
- 6. จัดให้มีการประเมินผลการทดสอบตามข้อ 4. และประเมินผลพิจารณาบทวนตามข้อ 5. โดยต้องรายงานผลต่อคณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการบริษัทอย่างน้อยปีละ 1 ครั้ง ทั้งนี้ การดำเนินการดังกล่าวต้องกระทำโดยบุคคลที่เป็นอิสระจากผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ตามข้อ 2.
- 7. คณะทำงานเพื่อแก้ไขปัญหาจากเหตุการณ์ผิดปกติ ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหมายหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งและทาง

2.14 การบริหารความต่อเนื่องทางธุรกิจในด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ วัตถุประสงค์

เพื่อให้การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเป็นส่วนหนึ่งของการบริหารความต่อเนื่องทางธุรกิจ (business continuity management) ของบริษัท ทั้งนี้ เพื่อให้ระบบสารสนเทศอยู่ในสภาพที่พร้อมใช้งานอยู่เสมอ

แนวทางปฏิบัติ

1. กำหนดมาตรการรองรับสำหรับกรณีที่เกิดเหตุการณ์ไม่พึงประสงค์
2. กำหนดขั้นตอน กระบวนการดำเนินการ และการควบคุม เกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศให้สอดคล้องกับแผนบริหารความต่อเนื่องทางธุรกิจ โดยมีรายละเอียดขั้นต่ำ ดังต่อไปนี้
 - (1) กำหนดขั้นตอนดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่เกิดขึ้น (incident response process) ให้เป็นไปตามนโยบายการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ
 - (2) มีขั้นตอนการแก้ไขปัญหาในแต่ละเหตุการณ์โดยละเอียด ชัดเจน พร้อมทั้งกำหนดผู้ที่มีหน้าที่รับผิดชอบที่สามารถปฏิบัติงานได้ในแต่ละเหตุการณ์
 - (3) มีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในการฉุกเฉินของแต่ละระบบงาน เช่น รุ่นของเครื่องคอมพิวเตอร์ คุณลักษณะของเครื่องคอมพิวเตอร์ (specification) ขั้นต่ำ ข้อมูลเกี่ยวกับการปรับแต่ง (configuration) และอุปกรณ์เครือข่ายคอมพิวเตอร์ เป็นต้น
 - (4) ระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรอง (ถ้ามี) ให้ชัดเจน เช่น สถานที่ตั้ง แผนที่ เป็นต้น
3. มีกำหนดระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานปกติของระบบสารสนเทศและจัดลำดับการกู้คืนระบบงานสารสนเทศที่มีความสำคัญให้สอดคล้องกับผลกระทบที่อาจเกิดขึ้น

4. มีระบบสารสนเทศสำรองที่อยู่ในสภาพพร้อมใช้งาน ซึ่งต้องสอดคล้องกับระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานตามปกติของระบบสารสนเทศตามข้อ 3.
5. จัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ โดยกระบวนการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศต้องครอบคลุมการดำเนินการ ดังนี้
 - (1) ประเมินความเสี่ยง (risk analysis) เพื่อให้สามารถระบุเหตุการณ์ความเสี่ยงที่อาจทำให้กระบวนการและระบบเทคโนโลยีสารสนเทศหยุดชะงัก ไม่สามารถให้บริการได้ตามปกติ หรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่อง
 - (2) วิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) จากเหตุการณ์ความเสี่ยงตาม ข้อ (1) เพื่อกำหนดระยะเวลาเป้าหมายในการกู้คืนระบบ IT (Recovery Time Objective: RTO) ระยะเวลาเป้าหมายสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective: RPO) และระยะเวลาสูงสุดที่ยอมให้กระบวนการทางธุรกิจหยุดชะงัก (Maximum Tolerable Downtime: MTD) อย่างเหมาะสม
6. สื่อสารให้บุคลากรที่เกี่ยวข้องมีความเข้าใจและสามารถปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม
7. ทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทบทวนและทดสอบดังกล่าว โดยรายงานผลการทบทวนและทดสอบต่อคณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการบริษัท

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ฉบับนี้ ได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัท ครั้งที่ 5/2568 เมื่อวันที่ 16 ธันวาคม 2568 โดยมีผลบังคับใช้ตั้งแต่วันที่ 16 ธันวาคม 2568



(นางสาวนีย์ กมลบุตร)

ประธานกรรมการบริษัท

บริษัทหลักทรัพย์จัดการกองทุน ไอรา จำกัด

ประวัติการทบทวนนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (IT Security Policy)

นโยบาย	ผลการทบทวน	ผู้ทบทวน	ผู้สอบทาน
นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (IT Security Policy) (ฉบับทบทวนปี 2568)	แก้ไขและเพิ่มเติมเนื้อหาในนโยบายให้สอดคล้องกับประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ที่ สธ. 33/2567 เรื่องข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ (ฉบับที่ 2) ดังนี้ - แก้ไขและเพิ่มเติมคำจำกัดความ - แก้ไขและเพิ่มเติมเลขที่ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ที่ใช้อ้างอิง ในหัวข้อ “นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ” - เพิ่มเติม หัวข้อที่ 5 การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security) - เพิ่มเติมเนื้อหาในหัวข้อ “การควบคุมการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ (Access Control)”, “การควบคุมการเข้ารหัสข้อมูล (Cryptographic Control)”, “การบริหารความต่อเนื่องทางธุรกิจในด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ”	พิมพ์พร กอเข็ม นางสาวพิมพ์พร กอเข็ม วันที่ 16 / 12 / 2568	ชนน วัฒนวิริยะ นายธนิต เวียนวัฒนะ วันที่ 16 / 12 / 2568 วิวัฒน์ นายวุฒิพงษ์ วัชรมัย วันที่ 16 / 12 / 2568