นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

บริษัท เพเนเล่ส์มาติก โซลูชั่นส์ จำกัด (มหาชน)

สารบัญ หน้า

สารบัญ หน้า

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

(Information Technology Security Policy)

1. บทนำ

บริษัทได้ตระหนักถึงความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จึงได้มีการวางแผนจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ขึ้น เพื่อให้ระบบสารสนเทศของบริษัทมีการควบคุมภายในทางที่ดี มีความมั่นคงปลอดภัย ถูกต้อง เชื่อถือได้ สามารถดำเนินงานได้อย่างต่อเนื่อง และสามารถป้องกันระบบสารสนเทศที่เป็นความลับของบริษัท ข้อมูลลูกค้า และข้อมูลส่วนบุคคลอื่นๆ ซึ่งนโยบายและแนวปฏิบัตินี้ จะเป็นกรอบแนวทางปฏิบัติของพนักงานทุกคนในบริษัท ให้มีความเข้าใจงานแต่ละระดับและร่วมมือ ในการใช้และเก็บรักษาข้อมูล ระบบ และเครื่องใช้เทคโนโลยีสารสนเทศ อย่างมีประสิทธิภาพให้ถูกต้องตามกฎหมาย

2. วัตถุประสงค์

2.1 เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของบริษัท ทำให้สามารถดำเนินงานได้อย่างมีประสิทธิภาพ และวัตถุประสงค์ที่กำหนดไว้

2.2 เพื่อกำหนดแนวปฏิบัติให้ผู้บริหาร ผู้ดูแลระบบ ผู้ใช้งาน และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัท ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท

2.3 เพื่อป้องกันไม่ให้ระบบสารสนเทศ และสารสนเทศของบริษัท ถูกบุกรุก ขโมยทำลาย แทรกแซง หรือโจรกรรมในรูปแบบต่างๆ ที่อาจสร้างความเสียหายต่อการดำเนินธุรกิจของบริษัท

2.4 เพื่อป้องกันพนักงานและบุคคลที่เกี่ยวข้อง ไม่ให้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ พ.ศ. 2560

2.5 เพื่อเผยแพร่ให้ผู้ใช้งาน และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัท ซึ่งบริษัทหรือหน่วยงานในบริษัทให้มีสิทธิ์การเข้าถึงข้อมูล หรือระบบสารสนเทศ ได้รับทราบและถือปฏิบัติอย่างเคร่งครัด

เพื่อให้การปฏิบัติงานด้านเทคโนโลยีสารสนเทศของบริษัท เพเนเลส์มาติก โซลูชั่นส์ จำกัด (มหาชน) เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ พ.ศ. 2560 ได้

กำหนดนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ประกอบด้วยนโยบายหลัก 3 ด้าน และแนวปฏิบัติภายในกรอบนโยบายหลัก ดังต่อไปนี้

1. นโยบายการเข้าถึงหรือควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ
   เป็นนโยบายในการกำหนดการอนุญาต การกำหนดสิทธิ์หรืออาจมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทางการอนุญาต เช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึง โดยมิชอบ
2. นโยบายการบริหารจัดการระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน
   เป็นนโยบาย ในการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่นๆ ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) ความน่าเชื่อถือ (Reliability) รวมถึงกรณีที่เกิดเหตุการณ์ สภาพของบริการเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย
3. นโยบายการตรวจสอบและประเมินความเสี่ยง
   เป็นนโยบายในการตรวจสอบและประเมินความเสี่ยง เพื่อกำกับดูแลการบริหารระบบสารสนเทศให้เกิดประสิทธิภาพและประสิทธิผล ตลอดจนการกำหนดแนวทางการแก้ไขปัญหาและอุปสรรคต่างๆที่เกิดขึ้น อย่างน้อยปีละ 1 ครั้ง เพื่อทบทวนนโยบายและข้อปฏิบัติให้เป็นปัจจุบัน

3 คำจำกัดความ

คำศัพท์	คำนิยาม
บริษัท (Company)	บริษัท เพเนเล่ส์มาติก โซลูชั่นส์ จำกัด (มหาชน)
ผู้ใช้งาน (User)	ผู้บริหาร พนักงานบริษัท ลูกจ้าง ผู้ดูแลระบบของบริษัท รวมทั้งผู้รับบริการ ผู้ใช้งานทั่วไป ที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหารหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของบริษัท โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท ที่บริษัทกำหนดไว้

คำศัพท์	คำนิยาม
ผู้ดูแลระบบ (System Administrator)	เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมหรือเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
ผู้บริหารระดับสูง	ผู้อำนวยการหรือรองผู้อำนวยการ ที่ได้รับมอบหมายในฐานะผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ
สิทธิของผู้ใช้งาน	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของบริษัท
สินทรัพย์ (Asset)	สิ่งใดก็ตามที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศที่มีคุณค่าสำหรับบริษัท
การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสาระสนเทศ ทั้งอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาต สำหรับบุคคลภายนอกตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบ
ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)	การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งาน ของสารสนเทศรวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ
เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)	กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่าย ที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)	สถานการณ์ซึ่งอาจทำให้ระบบของบริษัทถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
สำนักงาน	บริษัทที่ประกอบไปด้วย สำนักงานใหญ่ และโรงงาน
ศูนย์เทคโนโลยีสารสนเทศ	ห้องเซิร์ฟเวอร์ของบริษัท
การรักษาความมั่นคงปลอดภัย	การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท

คำศัพท์	คำนิยาม
ผู้ถือครองเครื่องคอมพิวเตอร์	ผู้ได้รับเครื่องคอมพิวเตอร์ไว้ใช้ประจำในการปฏิบัติงาน และถือครองรับ ผิดชอบดูแล เครื่องและอุปกรณ์คอมพิวเตอร์
ข้อมูลคอมพิวเตอร์	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึง ข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
ระบบเทคโนโลยีสารสนเทศ (Information Technology System)	ระบบงานของบริษัทที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศอื่นๆ
ระบบเครือข่ายสื่อสาร	ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการเชื่อมโยง หรือการส่งข้อมูลสารสนเทศ ระหว่างระบบเทคโนโลยีสารสนเทศต่างๆของบริษัท ซึ่งการเชื่อมโยงเป็นไปได้ทั้งในรูปแบบใช้สาย และแบบไร้สาย โดยระบบเครือข่ายสื่อสาร ระบบเครือข่ายระยะใกล้ (Local Area Network : LAN) เครือข่ายระยะไกล (Wide Ares Network : WAN) ระบบอินทราเน็ต (Intranet) และระบบอินเทอร์เน็ต (Internet)
เจ้าของข้อมูล	เจ้าหน้าที่ของหน่วยงานในบริษัท ผู้ได้รับมอบหมายจากผู้บังคับบัญชาให้ รับผิดชอบ ดูแล ปรับปรุงข้อมูลของระบบงานนั้นๆ ซึ่งเป็นผู้ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
จดหมายอิเล็กทรอนิกส์ (E-Mail)	ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิค ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP,POP3 และ IMAP

คำศัพท์	คำนิยาม
รหัสผ่าน (Password)	ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศ
ชุดคำสั่งไม่พึงประสงค์	ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
บุคคลภายนอก	บุคคล นิติบุคคล ซึ่งบริษัทหรือหน่วยงานในบริษัทอนุญาตให้มีสิทธิ์ในการเข้าถึงข้อมูลหรือระบบสารสนเทศ โดยได้รับสิทธิตามประเภทการใช้งาน และต้องรับผิดชอบในการไม่เปิดเผยความลับของบริษัทโดยไม่ได้รับอนุญาต
ผู้รับการว่าจ้าง	บุคคล นิติบุคคล หรือหน่วยงานภายนอก ซึ่งได้รับการว่าจ้างจากบริษัทให้ทำงานในระยะเวลาหนึ่ง หรือทำงานในฐานะเป็นผู้ใช้งานของบริษัท รวมถึงลูกจ้างชั่วคราว โดยทั่วไปการว่าจ้างจะมีการทำสัญญาจ้างเพื่อควบคุมให้ผู้รับจ้างปฏิบัติตามเงื่อนไขหรือข้อตกลงการจ้างงานนั้น

4 หน้าที่ความรับผิดชอบ

4.1 หน้าที่ของคณะกรรมการบริหาร

4.1.1 กำหนดกลยุทธ์และภาพรวม ควบคุมการปฏิบัติงานในบริษัท และอนุมัตินโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

4.1.2 กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท โดยกำหนดให้ไปในทิศทางเดียวกันกับแผนและเป้าหมายของบริษัท

4.1.3 จัดการพัฒนานโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย Policy , Standard , Procedure และ Guideline เพื่อให้บริษัทได้มาซึ่งการรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และเสถียรภาพความมั่นคงของระบบ (Availability)

4.1.4 การนำเสนอผู้บริหารระดับสูง เช่น ประธานเจ้าหน้าที่บริหาร เรื่องแผนการปฏิบัติงาน นโยบาย งบประมาณ อัตรากำลังพล ในด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

4.1.5 จัดให้มีการประเมิน และการบริหารความเสี่ยง ด้านสารสนเทศของบริษัท รายงานต่อคณะกรรมการบริหาร และคณะกรรมการตรวจสอบ เพื่อนำเสนอต่อคณะกรรมการบริษัท

4.1.6 เตรียมพร้อมรับสถานการณ์ และเรียนรู้เทคนิคใหม่ๆ ทางด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

4.2 หน้าที่ของผู้อำนวยการฝ่ายปฏิบัติงานและบริหารงานกลาง และผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

4.2.1 ร่างนโยบาย แนวปฏิบัติ และระเบียบในการดำเนินการด้านนโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

4.2.2 ประเมินความต้องการใช้ทรัพยากรด้านสารสนเทศ ความคุ้มค่า รวมทั้ง การจัดหา และพัฒนาระบบสารสนเทศให้สอดคล้องกับกลยุทธ์ของบริษัท

4.2.3 ดูแลทรัพยากรด้านสารสนเทศของบริษัท ให้สามารถสนับสนุนการปฏิบัติงานภายในอย่างมีประสิทธิภาพ

4.3 หน้าที่ของผู้ใช้งาน

4.3.1 ต้องเรียนรู้ ทำความเข้าใจ ปฏิบัติตามนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทโดยเคร่งครัด

4.3.2 ให้ความร่วมมือกับบริษัทอย่างเต็มที่ ในการป้องกันระบบคอมพิวเตอร์ และข้อมูลสารสนเทศของบริษัท สอดส่องดูแล ปกป้องข้อมูลและสารสนเทศของบริษัทให้มีความปลอดภัย

4.3.3 รายงานต่อบริษัททันที เมื่อพบเห็น การบุกรุก ขโมย ทำลาย หรือโจรกรรมสารสนเทศ รวมถึงระบบสารสนเทศที่อาจสร้างความเสียหายต่อบริษัท

4.4 หน้าที่ของหัวหน้า ผู้จัดการของหน่วยงาน

4.4.1 ชี้แจงและส่งเสริมให้ผู้ใช้งาน ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และตักเตือนลงโทษทางวินัย กรณีที่พบเห็นการปฏิบัติที่ไม่ถูกต้องเหมาะสม

4.5 หน้าที่ของเจ้าของข้อมูลและสารสนเทศ

4.5.1 จัดให้มีการทำเอกสาร และขั้นตอนการควบคุมการเข้าถึงข้อมูล ให้เป็นไปตามนโยบาย ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท

4.5.2 ดูแลให้พนักงาน ปฏิบัติตามนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท

4.5.3 ควบคุม อนุมัติการเข้าถึงข้อมูลและสารสนเทศ และระบบคอมพิวเตอร์ภายใต้หน้าที่และความรับผิดชอบ

4.5.4 รายงานเมื่อมีเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยของข้อมูลและสารสนเทศ

4.5.5 แจ้งหน่วยงานเทคโนโลยีสารสนเทศเพื่อลบ เปลี่ยนแปลงสิทธิ์ เมื่อมีการเปลี่ยนแปลงพนักงานอำนาจหน้าที่ หรือโอนย้าย

4.6 หน้าที่ของผู้ตรวจสอบภายใน

4.6.1 ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามความจำเป็นเหมาะสม

นโยบายการเข้าถึงหรือควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ

การควบคุมการเข้าถึงหรือการใช้ระบบเทคโนโลยีสารสนเทศ (Access Control)

แนวปฏิบัติ

1. การควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ

1.1 ผู้ดูแลระบบต้องดำเนินการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่ผู้ใช้งานได้รับอนุญาตหรือได้รับการมอบอำนาจ ตามที่กำหนดใน “การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่านของเจ้าหน้าที่”

1.2 ผู้ดูแลระบบมีการกำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้องดังนี้ อ่านข้อมูล สร้างข้อมูล นำเข้าข้อมูล แก้ไขข้อมูล อนุมัติ และไม่มีสิทธิ์

1.3 ผู้ดูแลระบบดำเนินการควบคุมการเข้าถึงที่เหมาะสมต่อหมวดหมู่ของสารสนเทศที่จัดไว้ตามระดับชั้นความลับ

1.4 ผู้ดูแลระบบมีการถอดสิทธิ์การเข้าถึง การใช้งานสารสนเทศ ตามที่กำหนดใน “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

1.5 ผู้ดูแลระบบ เป็นผู้ควบคุมการเข้าถึงจากประเภทของการเชื่อมต่อทั้งหมด

1.6 ผู้ใช้งานที่ต้องการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน จะต้องได้รับการพิจารณาจากผู้บริหารของหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษร หรือตามแบบฟอร์มที่หน่วยงานเทคโนโลยีสารสนเทศกำหนด

1.7 ผู้ดูแลระบบกำหนดประเภทของข้อมูล ได้แก่ ข้อมูลภายนอกสามารถเปิดเผยได้ ข้อมูลภายในเป็นไปตามลำดับชั้นความลับของข้อมูล

1.8 ผู้ดูแลระบบกำหนดลำดับชั้นความลับของข้อมูลได้แก่ ลับที่สุด ลับมาก ลับ บริษัท และทั่วไป

1.9 ผู้ดูแลระบบกำหนดระดับชั้นการเข้าถึงได้แก่ ผู้บริหาร ผู้ดูแลระบบ เจ้าของระบบ และผู้ใช้ระบบ

1.10 ผู้ดูแลระบบ กำหนดเวลาและช่องทางที่เข้าถึงได้ ให้เหมาะสมตามแต่ระบบงาน

2. การควบคุมการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

2.1 ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้บริหารของหน่วยงานต้นสังกัด และเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงาน เพื่อเข้าใช้งานระบบ สาระสนเทศเป็นลายลักษณ์อักษร หรือตามแบบฟอร์มที่หน่วยงานเทคโนโลยีสารสนเทศกำหนด ตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

2.2 ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบ การอนุมัติและกำหนดสิทธิ์ ในการผ่านเข้าสู่ระบบเฉพาะในส่วนที่จำเป็น โดยต้องคำนึงถึงประเภทข้อมูลและชั้นความลับ โดยมีการอนุญาตเข้าใช้งานเป็นลายลักษณ์อักษร จากต้นสังกัด เพื่อการเก็บไว้เป็นหลักฐาน

2.3 เจ้าของข้อมูล หรือเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบ เฉพาะในส่วนที่จำเป็นต้องรู้ ตามหน้าที่งาน หรือความจำเป็นขั้นต่ำเท่านั้น โดยไม่อนุญาตให้กำหนดสิทธิ์เกินความจำเป็นในการใช้งาน โดยต้องมีการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลหรือเจ้าของระบบงาน

3. การบริหารจัดการการเข้าถึงของผู้ใช้ (User Access Management)

3.1 การลงทะเบียนเจ้าหน้าที่ใหม่ กำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียน เจ้าหน้าที่ใหม่เพื่อให้มีสิทธิต่างๆในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์

การใช้งานเมื่อลาออกไป หรือเมื่อเปลี่ยนแปลงตำแหน่งงาน ภายใน 15 วันทำการ นับจากวันที่ผู้มีอำนาจลงนามในคำสั่ง

3.2 ผู้ดูแลระบบกำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ ได้แก่ ระบบสาระสนเทศ โปรแกรมประยุกต์ (Application) ภายในบริษัท จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายระยะใกล้ (Local Area Network : LAN) เครือข่ายระยะไกล (Wide Ares Network : WAN) ระบบอินทราเน็ต (Intranet) และระบบอินเทอร์เน็ต (Internet) โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บริหารของหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษร รวมทั้ง ต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

4. การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่านของเจ้าหน้าที่

4.1 ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้นๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศ และการสื่อสารแต่ละระบบ รวมทั้ง กำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติตามที่กำหนดไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

4.2 การเปลี่ยนแปลงและการยกเลิกรหัสผ่าน ผู้ดูแลระบบต้องปฏิบัติตามที่กำหนดไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

4.3 กรณีผู้ดูแลระบบมีความจำเป็นต้องให้สิทธิเพิ่มเป็นกรณีพิเศษแก่ผู้ใช้งานที่มีสิทธิพื้นฐาน ต้องได้รับความเห็นชอบและอนุมัติ จากหัวหน้าหน่วยงานต้นสังกัด และต้องมีการควบคุมผู้ใช้งานที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ โดยต้องดำเนินการอย่างน้อยดังนี้

4.3.1 ควบคุมการใช้งานอย่างเข้มงวดและอนุญาตให้เข้าใช้งานเฉพาะกรณีที่จำเป็นเท่านั้น

4.3.2 กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

4.3.3 กรณีมีการใช้งานไม่ต่อเนื่อง ให้มีการเปลี่ยนรหัสผ่านทุกครั้ง ภายหลังจากเสร็จสิ้นการใช้งานในแต่ละครั้ง หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ให้มีการเปลี่ยนรหัสผ่านทุกๆ 3 เดือน

4.4 กำหนดขั้นตอนในการลงทะเบียนผู้ใช้งาน (User Registration) ดังนี้

4.4.1 มีการระบุชื่อบัญชีผู้ใช้งานแยกเป็นรายบุคคล

4.4.2 การกำหนดชื่อผู้ใช้กำหนดจากชื่อภาษาอังกฤษไม่ต่ำกว่า 4 อักขระ

4.4.3 มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานต้นสังกัด

4.4.4 มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสาระสนเทศ การตัดออกจากทะเบียนผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอนย้าย หรือสิ้นสุดสัญญาจ้าง เป็นต้น

5. วิธีการบริหาร จัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

5.1 ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทฉันความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

5.2 เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆที่ให้ไว้ยังคงมีความเหมาะสมถูกต้อง

5.3 ผู้ดูแลระบบควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงข้อมูลโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับข้อมูล

5.4 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ SSL หรือ VPN

5.5 มีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด ของระดับความสำคัญของข้อมูลตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

การกำหนดชั้นความลับของข้อมูล

1. ขั้นที่ 1 ข้อมูลเปิดเผยได้
   - ข้อมูลที่บุคคลทั่วไปสามารถทราบได้โดยไม่ต้องมีการปิดกั้น เป็นข้อมูลที่ไม่มีผลต่อการปฏิบัติงานของบริษัท สามารถนำเสนอต่อบุคคลทั่วไป สาธารณชน หรือเป็นข้อมูลที่กฎหมายระบุว่าต้องเปิดเผย
   - การเปิดเผยข้อมูลทั้งหมดหรือบางส่วน จะไม่เกิดผลเสียหายต่อบริษัท เช่น ข้อมูลที่เผยแพร่บนเว็บไซต์ของบริษัท เป็นต้น

2. ขั้นที่ 2 ข้อมูลใช้ภายในบริษัท
    - ข้อมูลที่เจ้าของข้อมูลพิจารณาแล้วว่า สามารถเปิดเผยให้ผู้ใช้งานภายในบริษัทรับทราบได้ แต่ไม่สมควรเปิดเผยต่อบุคคลภายนอก เพราะอาจจะสร้างความเสียหายให้กับบริษัทได้
    - การเปิดเผยข้อมูล เจ้าของข้อมูลต้องใช้ดุลยพินิจในการอนุญาตหรือได้รับความเห็นชอบจากผู้บริหาร คณะทำงาน หรือหน่วยงาน
3. ขั้นที่ 3 ข้อมูลลับ
    - ข้อมูลที่บริษัทพิจารณาแล้วว่าไม่สามารถเปิดเผยให้ผู้ใช้งานทุกคนทราบได้ กำหนดให้เฉพาะผู้ที่เกี่ยวข้องและจำเป็นต้องใช้ในการปฏิบัติงานทราบเท่านั้น และเป็นการใช้งานตามสิทธิ์ ความจำเป็นที่ควรทราบ เพื่อให้เพียงพอต่อการปฏิบัติงาน ข้อมูลมีความสำคัญต่อการดำเนินการของบริษัท เป็นข้อมูลภายใน และไม่สามารถเปิดเผยต่อบุคคลภายนอกที่ไม่เกี่ยวข้องตามกฎหมายได้ เนื่องจากข้อมูลนี้จะสร้างความเสียหายให้กับบริษัทได้
    - การเปิดเผยข้อมูลจะต้องได้รับความเห็นชอบจากเจ้าของข้อมูล หรือคณะทำงาน หรือกรรมการผู้จัดการ หรือคณะกรรมการ
4. ขั้นที่ 4 ข้อมูลลับมาก
    - ข้อมูลที่ใช้ภายในบริษัท แต่เป็นข้อมูลลับ ใช้งานโดยผู้ใช้งานบางกลุ่มของบริษัท และไม่สามารถเปิดเผยต่อบุคคลภายนอกได้ เนื่องจากข้อมูลมีความจำเป็นต่อการปฏิบัติงานของบริษัท จะทำให้เกิดผลเสียหายร้ายแรงต่อบริษัท
    - การเปิดเผยข้อมูล จะต้องได้รับความเห็นชอบจากเจ้าของข้อมูล หรือคณะทำงาน หรือกรรมการผู้จัดการ หรือคณะกรรมการ
5. ขั้นที่ 5 ข้อมูลลับที่สุด
    - ข้อมูลที่ใช้ภายในบริษัท แต่เป็นข้อมูลลับ ใช้งานโดยผู้บริหารระดับสูงของบริษัทเท่านั้น และเป็นการใช้เพื่อการวินิจฉัย และตัดสินใจที่สำคัญของบริษัท ไม่สามารถเปิดเผยต่อบุคคลภายนอกได้ เนื่องจากข้อมูลมีความจำเป็นต่อการปฏิบัติงานของบริษัท ทำให้เกิดผลเสียหายร้ายแรงต่อบริษัท
    - การเปิดเผยข้อมูล ไม่สามารถทำได้ เว้นแต่บังคับตามกฎหมาย

6. การควบคุมการเข้าใช้งานระบบจากภายนอก

6.1 ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผล หรือความจำเป็นในการดำเนินงานกับบริษัทอย่างเพียงพอ เพื่อขอใช้สิทธิในการเข้าถึงระบบจากระยะไกล และต้องได้รับอนุมัติจากบริษัท

6.2 เจ้าหน้าที่หน่วยงานเทคโนโลยีสารสนเทศที่เป็นผู้ควบคุมการเข้าถึงระบบจากระยะไกล (Remote Access)

6.3 ผู้ใช้งานที่มีความจำเป็นต้องเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกล ต้องได้รับอนุมัติจากผู้จัดการหน่วยงานเทคโนโลยีสารสนเทศ และมีการควบคุมอย่างเข้มงวด โดยผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าถึงระบบและข้อมูลอย่างเคร่งครัด

6.4 ผู้ดูแลระบบต้องควบคุมพอร์ต (Port) ที่ระบบสาระสนเทศให้บริการ ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบ และวิธีการเข้าถึงต้องได้รับการอนุมัติอย่างถูกต้อง และเหมาะสมแล้วเท่านั้น

6.5 การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ผู้ดูแลระบบต้องอนุญาตตามพื้นฐานของความจำเป็นเท่านั้น

7. การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก

ผู้ใช้งานระบบทุกคนเมื่อเข้าใช้งานระบบของบริษัท ต้องผ่านการพิสูจน์ตัวตนจากระบบของบริษัท โดยมีแนวทางปฏิบัติดังนี้

7.1 การแสดงตัวตน ด้วยชื่อผู้ใช้งาน (Username)

7.2 การพิสูจน์ยืนยันตัวตน ด้วยการใช้รหัสผ่าน (Password)

7.3 การเข้าสู่ระบบสาระสนเทศของบริษัทจากอินเทอร์เน็ตนั้น จะต้องมีการตรวจสอบผู้ใช้งาน

7.4 การเข้าสู่ระบบจากระยะไกล (Remote Access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน โดยใช้รหัสผ่าน หรือวิธีการเข้ารหัส

การบริหารการจัดการสิทธิ์การใช้งานและระบบรหัสผ่าน

การบริหารรหัสผ่าน

1. หน่วยงานเทคโนโลยีสารสนเทศต้องกำหนดชื่อผู้ใช้ (Username) ระบบคอมพิวเตอร์เฉพาะบุคคลไม่ซ้ำกัน และกำหนดชื่อผู้ใช้ในส่วนของชื่อผู้ใช้ ชื่อผู้ใช้ของผู้ดูแลระบบ ชื่อผู้ใช้ของผู้ดูแลฐานข้อมูล ชื่อผู้ใช้ของผู้พัฒนาระบบ ชื่อผู้ใช้ของเจ้าหน้าที่ทางเทคนิค หรืออื่นๆให้มีความแตกต่างกัน
2. การส่งมอบรหัสให้กับผู้ใช้งานต้องใส่ซองปิดผนึก ส่งไปยังผู้ใช้งาน พร้อมแจ้งช่องทางการเข้าถึง “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ” เพื่อสร้างความรู้ ความเข้าใจ และให้ผู้ใช้งานปฏิบัติตามโดยเคร่งครัด
3. หน่วยงานเทคโนโลยีสารสนเทศกับหน่วยงานต่างๆของบริษัท จะทบทวนสิทธิ์การเข้าถึงระบบสารสนเทศของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง

การใช้งานรหัสผ่าน

1. ผู้ใช้งาน ต้องเก็บรักษารหัสผ่าน (Password) ของตนเอง ไว้เป็นความลับ
2. ห้ามทำการบันทึกรหัสผ่าน (Password) ไว้ในไปรษณีย์อิเล็กทรอนิกส์ หรือแบบฟอร์มต่างๆ
3. ไม่จดหรือบันทึกรหัสผ่าน (Password) ส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
4. ผู้ใช้งานทุกคนต้องเปลี่ยนรหัสผ่าน (Password) เริ่มต้นทันที หลังจากได้รับมอบรหัสผ่านเริ่มต้นจากผู้ดูแลระบบ ของศูนย์เทคโนโลยีสารสนเทศ
5. กำหนดให้รหัสผ่าน (Password) ต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยควรมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน และไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้พจนานุกรม
6. ไม่ใช้รหัสผ่าน (Password) ส่วนบุคคลกับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่น ผ่านเครื่อข่ายคอมพิวเตอร์
7. ไม่ใช้โปรแกรมคอมพิวเตอร์ ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่เจ้าหน้าที่ครอบครองอยู่

8. ในกรณีที่ลืมรหัสผ่าน หรือสงสัยว่ารหัสผ่าน (Password) ถูกผู้อื่นทราบ ให้รีบทำการเปลี่ยนแปลงรหัสผ่านทันที หรือแจ้งให้หน่วยงานเทคโนโลยีสารสนเทศทราบ เพื่อทำการเปลี่ยนรหัสผ่าน (Password) ทั้งหมดที่เกี่ยวข้อง
9. หากมีการกระทำความผิดเกิดขึ้นจากชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของบุคคลใด บุคคลนั้นต้องเป็นผู้รับผิดชอบต่อการกระทำความผิดนั้น ตามกฎหมาย ระเบียบ ข้อบังคับ ที่เกี่ยวข้อง
10. กรณีผู้ใช้งานของหน่วยงานภายในบริษัทลาออก ให้หน่วยงานเทคโนโลยีสารสนเทศทำการยกเลิกสิทธิของผู้ที่ลาออก ออกจากระบบทันที
11. กรณีผู้ใช้งานของหน่วยงานภายในบริษัท มีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบ ในระบบที่ขอสิทธิ์การใช้งาน ให้หน่วยงานต้นสังกัด แจ้งหน่วยงานเทคโนโลยีสารสนเทศเพื่อทำการเปลี่ยนแปลงสิทธิ์ในการใช้งาน
12. ผู้ใช้งานทุกคนของบริษัท มีหน้าที่ระมัดระวังความปลอดภัยการใช้เครือข่าย โดยต้องไม่ยินยอมให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากชื่อผู้ใช้ (Username) ระบบคอมพิวเตอร์ของตนเอง

การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

แนวปฏิบัติ

1. **การบริหารจัดการทางกายภาพ (Physical Security Management)**
   1.1 กำหนดระดับความสำคัญของพื้นที่ในศูนย์เทคโนโลยีสารสนเทศ
   1.2 มีระบบป้องกันให้ครอบคลุมพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน หรือบริเวณที่มีความสำคัญ
   1.3 ผู้ดูแลระบบต้องปิดประตูและหน้าต่างห้องแม่ข่ายให้ล็อคอยู่เสมอ

2. **การควบคุมการเข้า-ออก (Physical Entry Controls)**
   2.1 ให้มีการบันทึก ชื่อ วันที่ เวลา เบอร์โทรศัพท์ และเหตุผลการเข้า-ออกพื้นที่สำคัญ ของผู้มาเยือน (Visitors)
   2.2 กำหนดผู้ถือกุญแจหรือผู้รับผิดชอบห้องเครื่องแม่ข่าย เป็นลายลักษณ์อักษร

2.3 ผู้ถือกุญแจหรือผู้รับผิดชอบ จะต้องดูแลผู้ที่มาเยือนในพื้นที่บริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของสินทรัพย์หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

2.4 มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และควรมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

2.5 มีการควบคุมการเข้าถึงพื้นที่ ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

2.6 จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เพื่อใช้ในการตรวจสอบภายหลัง หากมีความจำเป็น

2.7 บริษัทผู้ได้รับการว่าจ้าง ต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

2.8 ผู้มาเยือนต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในศูนย์เทคโนโลยีสารสนเทศ

2.9 จัดให้มีการทบทวน หรือยกเลิกสิทธิ์การเข้าพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

2.10 จัดให้มีการทบทวน หรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

3. การจัดบริเวณการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public Access , Delivery , and Loading Areas)

3.1 จำกัดพื้นที่หรือบริเวณสำหรับการเข้าถึง เพื่อการส่งมอบหรือขนถ่ายผลิตภัณฑ์โดยบุคคลภายนอก

3.2 ดูแลบุคลากรซึ่งสามารถเข้าถึงพื้นที่บริเวณส่งมอบหรือขนถ่ายผลิตภัณฑ์

3.3 ลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอกและเจ้าหน้าที่จัดซื้อ

4. การจัดวางและการป้องกันอุปกรณ์ (Equipment Setting and Protection)

4.1 จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของผู้ปฏิบัติงานในศูนย์เทคโนโลยีสารสนเทศให้น้อยที่สุด

4.2 อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่ง ที่มีความมั่นคงปลอดภัย

4.3 ไม่ให้มีการทานอาหาร เครื่องดื่ม และสูบบุหรี่ ในบริเวณพื้นที่ที่มีระบบเทคโนโลยีสนเทศอยู่ภายใน

4.4 ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณ

5. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

5.1 มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของบริษัท พี่เพียงพอต่อความต้องการใช้งาน โดยให้มีระบบสำรองกระแสไฟฟ้า (UPS) และระบบปรับอากาศ

5.2 ให้มีการตรวจสอบ หรือทดสอบระบบสนับสนุน ตามข้อ 5.1 อย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ ลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

6. การเดินสายไฟ สายสื่อสาร และเคเบิ้ลอื่นๆ (Cabling Security)

6.1 ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์ เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

6.2 จัดทำผังสายสัญญาณสื่อสารต่างๆให้ครบถ้วนและถูกต้อง

6.3 ตู้ Rack ที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

7. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

7.1 กำหนดให้มีการบำรุงรักษาอุปกรณ์อย่างน้อยปีละ 1 ครั้ง

7.2 ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

7.3 จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์ สำหรับการให้บริการทุกครั้งเพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

7.4 จัดเก็บบันทึกปัญหา และข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

7.5 ควบคุมและสอดส่องดูแลการปฏิบัติงานของบริษัทผู้รับจ้างเหมาบำรุงรักษา ระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ภายในบริษัท

7.6 ควบคุมการส่งอุปกรณ์ออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

7.7 จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่มาทำการบำรุงรักษาอุปกรณ์เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

8. การนำสินทรัพย์ของบริษัท ออกไปภายนอกสถานที่ (Removal of Property)

8.1 ผู้ใช้งานต้องขออนุญาตจากหัวหน้าหน่วยงานต้นสังกัด ก่อนนำอุปกรณ์หรือทรัพย์สินออกภายนอกบริษัท

8.2 ผู้ใช้งานต้องบันทึกข้อมูลการนำอุปกรณ์ของบริษัท ออกไปภายนอกสถานที่ เพื่อเก็บไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

9. การป้องกันสินทรัพย์ที่ใช้งานภายนอกบริษัท (Security of Equipment Off-Premises)

9.1 กำหนดความปลอดภัยของสินทรัพย์ เพื่อป้องกันความเสี่ยงจากการนำสินทรัพย์ของบริษัทออกไปใช้งานภายนอก

9.2 ไม่ทิ้งสินทรัพย์ของบริษัทไว้ในที่สาธารณะโดยไม่มีผู้ดูแลรับผิดชอบ

9.3 ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบดูแลสินทรัพย์ของบริษัท เสมือนเป็นสินทรัพย์ของตนเอง

10. การกำจัดสินทรัพย์หรือการนำสินทรัพย์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-Use of Equipment)

10.1 ให้ทำลายข้อมูลสำคัญในสินทรัพย์ก่อนที่จะกำจัดสินทรัพย์ดังกล่าว

10.2 มีเทคนิคในการลบ หรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในสินทรัพย์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำสินทรัพย์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้น

นโยบายการบริหารจัดการระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน

การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ (Communications and Operations Management)

แนวปฏิบัติ

1. **ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented Operating Procedures)**

   1.1 มีการจัดทำคู่มือการปฏิบัติงานระบบเทคโนโลยีสาราสนเทศ โดยมีรายละอียดอย่างน้อย ดังนี้

   - การปฏิบัติงานในห้องแม่ข่าย
   - การเปิดและปิดระบบงาน ได้แก่ การเปิด - ปิด เครื่องแม่ข่าย , ระบบงาน , ระบบให้บริการ
   - การสำรองข้อมูล
   - การบำรุงรักษาอุปกรณ์
   - การจัดการกับสื่อบันทึกข้อมูล ได้แก่ การทำป้ายชื่อบ่งชี้ การลบ การป้องกันการนำสื่อบันทึกข้อมูลกลับมาใช้งานอีกครั้ง
   - การส่งงานเข้าไปประมวลผลในเครื่องคอมพิวเตอร์ และการจัดการกับข้อผิดพลาดที่เกิดขึ้น
   - การรายงานและการจัดการกับปัญหาที่เกิดขึ้น
   - การจัดการกับการทำงานล้มเหลวของระบบคอมพิวเตอร์ ระบบงาน และระบบเครือข่าย
   - การกู้คืนระบบงานและระบบเครือข่าย

   1.2 มีการแจกจ่ายและควบคุมดูแลให้มีการปฏิบัติงานตามแนวทางที่กำหนดในคู่มือการปฏิบัติงาน

   1.3 มีการทบทวนปรับปรุงคู่มือการปฏิบัติงานให้เหมาะสมอยู่เสมอ

2. **ควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบเทคโนโลยีสารสนเทศ (Change Management)**
   ต้องมีการกำหนดผู้รับผิดชอบและผู้มีอำนาจในการควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบเทคโนโลยีสารสนเทศของบริษัท

3. **การแบ่งหน้าที่ความรับผิดชอบ (Segregation of Duties)**

   3.1 มีการกำหนดแบ่งแยกหน้าที่ความรับผิดชอบในการปฏิบัติงานของแต่ละบุคคลไว้อย่างชัดเจน โดยมิให้มีการกำหนดหน้าที่ที่สำคัญไว้ที่บุคคลเพียงคนเดียว

3.2 ให้ผู้บังคับบัญชามีการควบคุมดูแลอย่างใกล้ชิดสำหรับงานที่มีความเสี่ยงต่อการเกิดความเสียหาย

3.3 ให้มีการจัดเก็บหลักฐานการปฏิบัติงานที่สามารถใช้ในการตรวจสอบได้ในภายหลัง

4. การแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of Development , Test and Operational Facilities)

4.1 ให้มีการแยกเครื่องคอมพิวเตอร์ของระบบงาน สำหรับการพัฒนา การทดสอบ และการให้บริการ ออกจากกันตามความจำเป็น เพื่อป้องกันผลกระทบจากการทำงาน

4.2 กำหนดให้มีการควบคุมการถ่ายโอนระบบงานจากเครื่องที่ใช้สำหรับการพัฒนา ไปสู่เครื่องที่ใชสำหรับการให้บริการ

4.3 กำหนดให้มีการแยกบัญชีผู้ใช้งานออกจากกัน สำหรับระบบงานที่ใช้ในการพัฒนาทดสอบและใช้ระบบงานจริง

การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls Against Malicious Code)

แนวปฏิบัติ

1. ห้ามทำการติดตั้งซอฟต์แวร์อื่นๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งการใช้แฟ้มข้อมูล (File) อื่นที่บริษัทไม่อนุญาตให้มีการใช้งาน
2. ให้ติดตั้งซอฟต์แวร์ เพื่อป้องกันโปรแกรมไม่ประสงค์ดีให้กับระบบเทคโนโลยีสารสนเทศของบริษัท
3. ให้ผู้ดูแลระบบดำเนินการตรวจสอบโปรแกรมไม่ประสงค์ดีในเครื่องเซิร์ฟเวอร์ให้บริการ และอุปกรณ์เทคโนโลยีสารสนเทศอื่นๆ ณ จุดทางเข้า – ออกเครือข่าย เพื่อดักจับโปรแกรมไม่ประสงค์ดีที่เข้าสู่ระบบ
4. กำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติสำหรับการจัดการกับโปรแกรมไม่ประสงค์ดี ได้แก่ การรายงานการเกิดขึ้นของโปรแกรมไม่ประสงค์ดี การวิเคราะห์ การจัดการ การกู้คืนระบบจากความเสียหายที่พบ เป็นต้น
5. มีการติดตามข้อมูลข่าวสารเกี่ยวกับโปรแกรมไม่ประสงค์ดีอย่างสม่ำเสมอ

6. ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ ความเข้าใจและสามารถป้องกันตนเองได้ และให้รับทราบขั้นตอนปฏิบัติ เมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร
7. เครื่องคอมพิวเตอร์ทั้งหมด ได้แก่ เครื่องคอมพิวเตอร์แม่ข่าย (Server) เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ (PC Desktop) และเครื่องคอมพิวเตอร์แบบพกพา (Laptop) ต้องได้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัสรุ่นล่าสุดของบริษัทจากจ้าหน้าที่หน่วยงานเทคโนโลยีสารสนเทศ และจะต้องเปิดใช้งานโปรแกรมตรวจสอบและกำจัดไวรัสตลอดเวลา
8. เครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่ให้บริการการตรวจสอบและกำจัดไวรัส ต้องมีการปรับปรุงข้อมูลล่าสุดของไวรัสอยู่เสมอ และต้องเป็นผู้ให้บริการปรับปรุงข้อมูลไวรัสล่าสุด ให้แก่ เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ (PC Desktop) และเครื่องคอมพิวเตอร์แบบพกพา (Laptop) ทุกเครื่องโดยอัตโนมัติ
9. ต้องทำการตรวจสอบไวรัสกับแฟ้มข้อมูล (File) ต่างๆ , ที่ทำการบันทึกลงมา (Download) , แฟ้มข้อมูลที่แนบมากับไปรษณีย์อิเล็กทรอนิกส์ (Email) , แฟ้มข้อมูลที่ได้มาจากสื่อบันทึกข้อมูลภายนอก (CD , Thumb Drive , Diskette or Share file)

การเข้าถึงระบบโปรแกรมประยุกต์และสารสนเทศ (Information Handling Procedures)

แนวปฏิบัติ

1. การจัดการสาระสนเทศ

1.1 มีการกำหนดข้อมูลตามระดับชั้นความลับ

1.2 มีขั้นตอนปฏิบัติเพื่อจัดการเก็บข้อมูลตามระดับชั้นความลับ ควรประกอบด้วยวิธีการประมวลผลการควบคุมการเข้าถึง การจัดเก็บ ระยะเวลาที่สามารถเข้าถึง และช่องทางการเข้าถึง

1.3 มีการจำกัดการเข้าถึงข้อมูลตามระดับชั้นความลับ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

1.4 มีการตรวจสอบว่าข้อมูลที่นำออกจากระบบงานมีความถูกต้องและสมบูรณ์ก่อนที่จะนำไปใช้งานต่อไป

1.5 มีการจัดทำบัญชีรายชื่อผู้มีสิทธิ์เข้าถึงข้อมูลและสื่อบันทึกข้อมูลสำคัญ และมีการทบทวนสิทธิ์บัญชีรายชื่ออย่างสม่ำเสมอ

1.6 การเข้าถึงต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

1.7 ระบบไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน จะต้องดำเนินการดังนี้

- ต้องแยกระบบซึ่งไวต่อการบกวนดังกล่าวออกจากระบบอื่นๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อหน่วยงาน
- มีการควบคุมสภาพแวดล้อม ได้แก่ มีห้องแม่ข่ายเฉพาะ มีระบบไฟสำหรับระบบเฉพาะ มีระบบป้องกันผู้มีสิทธิ์เข้า – ออกห้องแม่ข่าย
- มีการควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา และมีการป้องกันความเสี่ยงที่มีต่ออุปกรณ์

1.8 การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) จะต้องดำเนินการ ดังนี้

- ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของผู้ใช้งานจากระยะไกล ตามแนวปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอก รวมถึงการเตรียมการระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เพื่อให้มีความมั่นคงปลอดภัย
- ผู้ดูแลระบบ เตรียมการป้องกันทางกายภาพสำหรับสถานที่ที่จะอนุญาตการปฏิบัติงานของผู้ใช้งานจากระยะไกล ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล
- ผู้ดูแลระบบ มีการรักษาความมั่นคงปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ ที่จะมีการปฏิบัติงานจากระยะไกล และระบบงานต่างๆภายในบริษัท ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล ตามแนวปฏิบัติการควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ
- ผู้ปฏิบัติงานจากระยะไกลต้องรักษาความลับของหน่วยงาน ไม่อนุญาตให้ครอบครัวหรือบุคคลอื่นๆได้ เข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท
- การขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกล กำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบงาน ต้องปฏิบัติตามการ “บริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

2. การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection Time)

2.1 กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งาน เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น ได้แก่ กำหนดให้ใช้งานได้ 2 ชั่วโมง ต่อการเชื่อมต่อ 1 ครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานตามปกติเท่านั้น หรือช่วงนอกเวลาทำงาน เป็นต้น

2.2 กำหนดให้ระบบเทคโนโลยีสารสนเทศ ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกบริษัท) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

3. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operation System Access Control)

3.1 กำหนดขั้นตอนปฏิบัติเพื่อเข้าใช้งานที่มั่นคงปลอดภัย

- ต้องจัดให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆของระบบ ก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์
- ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง
- จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน
- จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

3.2 ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจง ซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิค ในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติ ดังนี้

- ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน
- สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม

3.3 กำหนดหลักเกณฑ์ยุติการเชื่อมต่อ เมื่อว่างเว้นจากการใช้งานเป็นเวลา 15 นาทีเป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

4. **การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit Logging)**
   จัดให้มีการบันทึกข้อมูลพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบเทคโนโลยีสารสนเทศ ที่แสดงให้ทราบว่าใครทำอะไร ที่ไหน เมื่อไหร่ และอย่างไร

การบริหารจัดการการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

แนวปฏิบัติ

1. **การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย**
   1.1 กำหนดให้มีรหัสผู้ใช้/รหัสผ่าน (Username/Password) ในการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและระบบปฏิบัติการ
   1.2 กำหนดจำนวนครั้งที่สามารถพิมพ์รหัสผิดได้ หากเกินกว่าที่กำหนดระบบ ต้องทำการล็อคไม่ให้ใช้งานเป็นระยะเวลาหนึ่ง
   1.3 ผู้ดูแลระบบควรกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”
   1.4 ผู้ดูแลระบบ ควรตั้งระบบการล็อคหน้าจอเมื่อไม่มีการใช้งาน เมื่อต้องการใช้งาน ผู้ใช้ต้องใส่รหัสผ่าน
   1.5 ผู้ดูแลระบบ ต้องทำการ Log out ออกจากระบบทันที เมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

2. **การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ (Control of Operational Software)**
   2.1 มีการควบคุมการเปลี่ยนแปลงต่อระบบงานของบริษัท เพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบงานนั้น
   2.2 ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบงานของบริษัท
   2.3 การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงาน ต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ
   2.4 กำหนดให้ผู้ใช้งาน หรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบงานตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน

2.5 ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบงานอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน

3. ให้มีการทบทวนการทำงานของระบบงานภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications After Operating System Changes)

3.1 แจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้ทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบ และทบทวน ก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

3.2 พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบงาน รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในกรณีที่บริษัทต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

4. การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced Software Development)

4.1 จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

4.2 ให้กำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนา โดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

4.3 ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดีในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

5. การเฝ้าดูและตรวจสอบ

5.1 ต้องดำเนินการเก็บ Log ของเหตุการณ์ละเมิดความมั่นคงปลอดภัย ดังต่อไปนี้

- Log ทั้งหมดที่เกี่ยวข้องกับเหตุการณ์ละเมิดความมั่นคงปลอดภัยต้องเก็บไว้อย่างน้อยเป็นเวลา 90 วัน
- ต้องมีระบบจัดเก็บ Log ที่มีอยู่เกินกว่า 90 วัน ให้มีความปลอดภัยและพร้อมให้เรียกใช้งานได้เมื่อพนักงานเจ้าหน้าที่ต้องการ ต้องสามารถนำออกมามอบให้กับพนักงานเจ้าหน้าที่ได้

5.2 ผู้ดูแลระบบ ต้องตรวจสอบ Log และเหตุการณ์ละเมิดความมั่นคงปลอดภัย และรายงานให้กับผู้บังคับบัญชาทราบ ดังนี้

- การเข้าสู่ระบบของผู้ใช้งานที่ไม่มีสิทธิในการใช้งานระบบนั้น

- เหตุการณ์ผิดปกติของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่เกิดขึ้น
- ต้องดำเนินการบำรุงรักษา (Maintenance) เป็นประจำ
- ต้องมีการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง พร้อมจัดทำรายงานผลการประเมินความเสี่ยงเสนอผู้บังคับบัญชา

การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer)

แนวปฏิบัติ

1. การปฏิบัติทั่วไป

1.1 เครื่องคอมพิวเตอร์ที่บริษัทอนุญาตให้ผู้ใช้งานใช้งานเป็นสินทรัพย์ของบริษัท ดังนั้น ผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของบริษัท

1.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของบริษัท ต้องเป็นโปรแกรมที่บริษัทได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย

1.3 ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆของบริษัท และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

1.4 ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม ในเครื่องคอมพิวเตอร์ส่วนบุคคลของบริษัท เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากเจ้าหน้าที่ของหน่วยงานเทคโนโลยีสารสนเทศ

1.5 การส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อม จะต้องได้รับการพิจารณาจากหน่วยงานเทคโนโลยีสารสนเทศ

1.6 ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

1.7 ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครอง เมื่อใช้งานประจำวันเสร็จสิ้น

1.8 ผู้ใช้งาน ต้องใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 15 นาที เพื่อให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่านเพื่อป้องกันบุคคลอื่นเข้ามาใช้งานที่เครื่องคอมพิวเตอร์

1.9 ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายบริษัท ยกเว้นจะได้รับการพิจารณาอนุมัติจากผู้จัดการหน่วยงานเทคโนโลยีสารสนเทศ ก่อนการใช้งาน

1.10 ระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ส่วนบุคคล ต้องมีการ Update Service Pack ที่เป็น

Version ล่าสุดเสมอ โดยเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศหรือผู้ดูแลระบบ

1.11 การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) ส่วนบุคคลจะต้องกำหนดโดยเจ้าหน้าที่หน่วยงานเทคโนโลยีสารสนเทศเท่านั้น

1.12 การเคลื่อนย้ายเครื่องคอมพิวเตอร์จากจุดเชื่อมต่อเครือข่ายเดิมไปยังจุดเชื่อมต่อเครือข่ายใหม่ภายในบริษัท จะต้องแจ้งหน่วยงานเทคโนโลยีสารสนเทศดำเนินการให้เท่านั้น

1.13 กรณีส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมโดยผู้รับจ้าง เมื่อตรวจซ่อมเสร็จ ต้องให้เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้ติดตั้งโปรแกรมที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศของบริษัท

1.14 ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆของเครื่องคอมพิวเตอร์ส่วนบุคคลของบริษัททุกเครื่อง เว้นแต่ได้รับความเห็นชอบจากเจ้าหน้าที่หน่วยงานเทคโนโลยีสารสนเทศ

1.15 เครื่องคอมพิวเตอร์ทุกเครื่อง ต้องได้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัส โดยโปรแกรมป้องกันไวรัสของบริษัท จากเจ้าหน้าที่หน่วยงานเทคโนโลยีสารสนเทศ

1.16 ผู้ใช้งานไม่ควรสร้าง Short-Cut หรือปุ่มกดบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของบริษัท

1.17 ผู้ใช้งานมีหน้าที่และความรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์โดยต้องปฏิบัติ ดังนี้

- ไม่ทานอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์
- ไม่ว่างสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

1.18 ห้ามเจ้าหน้าที่ทุกคนทำการปรับแต่งการตั้งค่าเวลาของเครื่องคอมพิวเตอร์ส่วนบุคคลของบริษัททุกเครื่อง และต้องดูแลมิให้เครื่องที่ถือครอบครองถูกแก้ไขการตั้งค่าเวลา ในกรณีที่เวลาของเครื่องคอมพิวเตอร์ส่วนบุคคลถูกแก้ไข เจ้าของเครื่องจะปฏิเสธความรับผิดชอบไม่ได้ และเมื่อรู้ว่าเครื่องมีการแก้ไขการตั้งค่าเวลาต้องแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันที

1.19 ต้องทำการล้างข้อมูลในเครื่องคอมพิวเตอร์ทุกครั้ง ที่มีการเปลี่ยนแปลงเครื่องคอมพิวเตอร์ให้กับเจ้าของเครื่องรายใหม่ พร้อมทั้งต้องทำการปลด Password สำหรับการเข้าใช้เครื่องคอมพิวเตอร์ (ระบบปฏิบัติการ) และต้องทำการแจ้งการเปลี่ยนแปลงแก่ผู้ดูแลการใช้เครื่องคอมพิวเตอร์ทุกครั้ง

2. แนวทางปฏิบัติในการเข้าใช้เครื่องคอมพิวเตอร์ (ระบบปฏิบัติการ) และรหัสผ่าน

2.1 ผู้ใช้งานต้องกำหนดชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

2.2 ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตาม “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

2.3 ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

3. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

3.1 ผู้ใช้งานควรตรวจสอบหาไวรัสจากสื่อต่างๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

3.2 ผู้ใช้งานควรตรวจสอบแฟ้มข้อมูล (File) ที่แนบมากับจดหมายอิเล็คทรอนิกส์ (Email) หรือแฟ้มข้อมูล (File) ที่ทำการบันทึก (Download) มาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

3.3 ผู้ใช้งานควรตรวจสอบข้อมูลคอมพิวเตอร์ใดๆที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

4. การสำรองข้อมูลและการกู้คืน

4.1 ผู้ใช้งานเครื่องคอมพิวเตอร์ทุกเครื่อง มีหน้าที่ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกข้อมูลส่วนบุคคล ได้แก่ Cloud เป็นต้น

4.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

การใช้งานเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ (Mobile Computing)

แนวปฏิบัติ

1. การใช้งานทั่วไป

1.1 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ของบริษัท ต้องเป็นโปรแกรมที่บริษัทได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆและนำไปติดตั้งบนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

1.2 ผู้ใช้งานควรศึกษาการปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

1.3 กรณีส่งเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ตรวจซ่อมโดยผู้รับจ้าง เมื่อตรวจซ่อมแล้วเสร็จต้องให้เจ้าหน้าที่หน่วยงานเทคโนโลยีสารสนเทศ เป็นผู้ติดตั้งโปรแกรมที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศของบริษัท

1.4 ระบบปฏิบัติการบนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ต้องมีการ Update Service Pack ที่เป็น Version ล่าสุดเสมอ โดยเจ้าหน้าที่หน่วยงานเทคโนโลยีสารสนเทศเท่านั้น

1.5 ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม ในเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ของบริษัท เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ

1.6 ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ทุกเครื่อง เว้นแต่ได้รับความเห็นชอบจากเจ้าหน้าที่หน่วยงานเทคโนโลยีสารสนเทศ และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ให้มีสภาพเดิม

1.7 เครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ทุกเครื่อง ต้องได้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัส โดยโปรแกรมป้องกันไวรัสของบริษัทจากเจ้าหน้าที่หน่วยงานเทคโนโลยีสารสนเทศ

1.8 การนำเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ทุกเครื่องออกไปใช้งานนอกบริษัท เมื่อนำกลับมาที่บริษัท ต้องทำการเชื่อมต่อระบบเครือข่ายภายในบริษัท เพื่อทำการอัปเดต (Update) ข้อมูลไวรัสล่าสุด และต้องมีการป้องกันความเสี่ยงจากการเข้าถึงสารสนเทศโดยไม่ได้รับอนุญาต จากบุคคลภายนอกบริษัท ซึ่งรวมถึงครอบครัวและเพื่อน

1.9 ห้ามผู้ใช้งานทุกคนทำการปรับแต่งการตั้งค่าเวลาของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ของบริษัททุกเครื่อง และต้องดูแลมิให้เครื่องที่ถือครอบครองถูกแก้ไขการตั้งค่าเวลา ในกรณีที่ค่าเวลาของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ถูกแก้ไข เจ้าของเครื่องจะปฏิเสธความรับผิดชอบไม่ได้ และเมื่อรู้ว่าเครื่องมีการแก้ไขการตั้งค่าเวลาต้องแจ้งให้หน่วยงานเทคโนโลยีสารสนเทศทราบทันที

1.10 การเชื่อมต่อเพื่อใช้งานระบบจากภายนอกให้ปฏิบัติตามนโยบายการควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ (Access Control)

1.11 ต้องทำการลบข้อมูลทุกครั้ง ที่มีการเปลี่ยนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ ให้กับเจ้าของเครื่องรายใหม่ พร้อมทั้งต้องทำการปลด Password สำหรับการเข้าใช้เครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ และต้องทำการ แจ้งการเปลี่ยนแปลงแก่ผู้ดูแลการใช้งานเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ทุกครั้ง

2. ความปลอดภัยทางด้านกายภาพ

2.1 ผู้ใช้งาน มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย โดยการล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

2.2 ผู้ใช้งาน ไม่ควรเก็บหรือใช้งานเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ในสถานที่ที่มีความร้อน ความชื้น ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

2.3 ไม่ควรใส่เครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ ไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่องหรืออาจถูกจับโยนได้

2.4 ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน

2.5 หลีกเลี่ยงการนำของแข็งกดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ แตกเสียหายได้

2.6 ไม่วางของทับบนหน้าจอและแป้นพิมพ์

2.7 การเช็ดทำความสะอาดหน้าจอควรเช็ดอย่างเบามือที่สุดและควรเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้มีรอยขีดข่วน

2.8 การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดอยู่ให้ทำการยกจากท่านภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

2.9 ไม่เคลื่อนย้ายเครื่องในขณะที่ฮาร์ดดิสก์กำลังทำงาน

2.10 ไม่ใช่หรือวางเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ใกล้สิ่งที่เป็นของเหลว

2.11 ไม่ใช่หรือวางเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ ไว้ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส

2.12 ไม่ควรวางเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูง

2.13 ไม่ควรติดตั้งหรือวาง คอมพิวเตอร์แบบพกพาในที่ที่มีการสั่นสะเทือน

3. การเข้าใช้เครื่องคอมพิวเตอร์ (ระบบปฏิบัติการ) และรหัสผ่าน

3.1 ผู้ใช้งานต้องกำหนดชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ ของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่

3.2 ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพดีตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

3.3 ผู้ใช้งาน ต้องใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 15 นาที ในการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน

3.4 ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

3.5 ผู้ใช้งาน ต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

4. การสำรองข้อมูลและการกู้คืน

4.1 เจ้าหน้าที่หน่วยงานเทคโนโลยีสารสนเทศ มีหน้าที่ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่นฮาร์ดดิสก์แบบติดตั้งภายนอก เป็นต้น

4.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

5. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

5.1 ผู้ใช้งานควรตรวจสอบหาไวรัสจากสื่อต่างๆก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

5.2 ผู้ใช้งานควรตรวจสอบแฟ้มข้อมูล (File) ที่แนบมากับจดหมายอิเล็กทรอนิกส์ (Email) หรือแฟ้มข้อมูล (File) ที่ทำการบันทึก (Download) มาจากอินเทอร์เน็ต ด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

5.3 ผู้ใช้งานควรตรวจสอบข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

การใช้งานอินเทอร์เน็ต (Use of the Internet)

แนวปฏิบัติ

1. ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย
2. เครื่องคอมพิวเตอร์ส่วนบุคคล (PC Desktop) และเครื่องคอมพิวเตอร์พกพา (Laptop) ก่อนทำการเชื่อมต่ออินเทอร์เน็ต ผ่านเว็บบราวเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บบราวเซอร์ติดตั้งอยู่
3. ผู้ใช้งานต้องไม่ใช่เครือข่ายอินเทอร์เน็ตของบริษัท เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม
4. ผู้ใช้งานจะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของบริษัท โดยผ่านความเห็นชอบจากผู้บริหารของหน่วยงานต้นสังกัด
5. ผู้ใช้งานต้องไม่กระทำการเปิดเผยข้อมูลสำคัญเกี่ยวกับงานของบริษัท ที่ไม่เข้าหลักเกณฑ์การเปิดเผยประกาศอย่างเป็นทางการ ผ่านทางอินเทอร์เน็ต
6. ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ ที่อยู่บนอินเทอร์เน็ต ก่อนนำข้อมูลไปใช้งาน
7. หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

8. ผู้ใช้งานต้องปฏิบัติตาม พ.ร.บ. การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และ พ.ศ.2560 อย่างเคร่งครัด

การใช้งานจดหมายอิเล็คทรอนิกส์ (Use of Electronic Mail)

แนวปฏิบัติ

1. ให้ใช้ระบบจดหมายอิเล็คทรอนิกส์ของบริษัทเท่านั้น ในการติดต่อหรือรับ - ส่ง ข้อมูลกับหน่วยงานภายนอก ทั้งทางราชการ และเอกชน ผ่านทางจดหมายอิเล็กทรอนิกส์
2. หน่วยงานเทคโนโลยีสารสนเทศ เป็นผู้กำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็คทรอนิกส์ของบริษัท ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งานระบบ และหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เมื่อมีการลาออก เป็นต้น
3. การรับ - ส่งข้อมูล ของบริษัทที่เป็นความลับ ห้ามรับ - ส่ง ผ่านทางระบบจดหมายอิเล็กทรอนิกส์
4. ผู้ใช้งานรายใหม่จะต้องทำการเปลี่ยนรหัสผ่าน (Password) โดยทันทีเมื่อได้รับรหัสผ่าน (Default Password) ในการผ่านเข้าสู่ระบบจดหมายอิเล็คทรอนิกส์เป็นครั้งแรก โดยต้องกำหนดรหัสผ่านให้มีคุณภาพดีตามที่ระบุไว้ใน “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”
5. ห้ามผู้ใช้งานตั้งค่าการใช้งานโปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์
6. ผู้ใช้งานควรมีการเปลี่ยนแปลงรหัสผ่านอย่างเคร่งครัดโดยเปลี่ยนรหัสผ่านทุก 3 เดือน
7. ผู้ใช้งานต้องไม่ใช่จดหมายอิเล็คทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อบริษัท หรือละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม หรือส่งต่อข้อความกล่าวร้าย ทำให้เสื่อมเสีย หรือข้อความที่หยาบคาย ลามก ข่มขู่ ก่อกวน หรือสร้างความเสียหายให้กับผู้อื่น รวมถึงไม่แสวงหาผลประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจ จากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของบริษัท
8. หลังจากการใช้งานระบบจดหมายอิเล็คทรอนิกส์เสร็จสิ้น ให้ทำการ ออกจากระบบ (Logout) ทุกครั้งเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็คทรอนิกส์
9. ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทมีการจัดการใช้งานของผู้ใช้งาน (Logout หน้าจอ) เมื่อผู้ใช้งานไม่ได้ใช้งานระบบเป็นเวลา 30 นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านครั้ง

10. ผู้ใช้งานควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็คทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบแฟ้มข้อมูล (File) โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดข้อมูล ที่เป็น Executable File
11. ผู้ใช้งานไม่เปิดหรือส่งต่อจดหมายอิเล็คทรอนิกส์หรือข้อความที่ได้รับจาก ผู้ส่งที่ไม่รู้จัก ในเครื่องที่อยู่ในระบบเครือข่ายของบริษัท
12. ผู้ใช้งาน ควรตรวจสอบตู้เก็บจดหมายอิเล็คทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็คทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด
13. ผู้ใช้งาน ควรลบจดหมายอิเล็คทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็คทรอนิกส์
14. ผู้ใช้งาน ต้องไม่ส่งหรือส่งต่อจดหมายอิเล็คทรอนิกส์ที่มีข้อมูลคอมพิวเตอร์ โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ประเภท ดังต่อไปนี้
    - ข้อมูลคอมพิวเตอร์อันเป็นเท็จ
    - ข้อมูลคอมพิวเตอร์อันเป็นเท็จที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน
    - ข้อมูลคอมพิวเตอร์ใดๆอันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา
    - ข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกอนาจาร
15. ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็คทรอนิกส์ (Email Address) ของผู้อื่น เพื่ออ่าน รับส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งาน และให้ถือว่าเจ้าของจดหมายอิเล็คทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆในจดหมายอิเล็คทรอนิกส์ของตน
16. ผู้ใช้งาน ต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเลคทรอนิคส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของบริษัท ทำให้เกิดความแตกแยกระหว่างบริษัท ผ่านทางจดหมายอิเล็คทรอนิกส์
17. ผู้ใช้งานควรโอนย้ายจดหมายอิเล็คทรอนิกส์ ที่ใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้น ไม่ควรจัดเก็บข้อมูล หรือจดหมายอิเล็คทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็คทรอนิกส์

การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

แนวปฏิบัติ

1. ห้ามใช้ระบบเครือข่ายไร้สายภายในอาคารของบริษัท ในระหว่างที่บริษัท ยังไม่มีการติดตั้งระบบบริหารจัดการและระบบรักษาความปลอดภัยสำหรับเครือข่ายไร้สายโดยเฉพาะ
2. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายชั่วคราวของบริษัท จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับการพิจารณาอนุมัติจากผู้จัดการหน่วยงานเทคโนโลยีสารสนเทศ ตามความจำเป็นในการใช้งาน
3. ผู้ดูแลระบบ ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย
4. ผู้ดูแลระบบ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย แล้วป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้
5. ผู้ดูแลระบบต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน
6. ผู้ดูแลระบบ ต้องเปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบ สำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และควรจะเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย
7. ผู้ดูแลระบบต้องกำหนดค่าใช้ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) และเพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากขึ้น
8. ผู้ดูแลระบบต้องเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง
9. ผู้ดูแลระบบ ควรมีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

10. ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย ให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้งานระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ
11. ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบ ความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้รายงานต่อผู้บริหารทราบโดยทันที

ความมั่นคงปลอดภัยของ Firewall

แนวปฏิบัติ

1. หน่วยงานเทคโนโลยีสารสนเทศ มีหน้าที่ในการบริหารจัดการการติดตั้งและกำหนดค่าของไฟร์วอลล์ (Firewall) ทั้งหมด
2. ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบายจะต้องถูกบล็อก (Block)โดยไฟร์วอลล์
3. ผู้ใช้งานอินเทอร์เน็ตจากภายนอกจะต้องมี Login Account ก่อนการใช้งานทุกครั้ง
4. ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง
5. การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น
6. ข้อมูลจราจรทางคอมพิวเตอร์ ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน
7. การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย จะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่หน่วยงานเทคโนโลยีสารสนเทศอนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับการพิจารณาอนุมัติจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ
8. เครื่องคอมพิวเตอร์แม่ข่าย ที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อ เพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

9. ฝ่ายเทคโนโลยีสารสนเทศ มีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่าย ที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข
10. การเชื่อมต่อลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์แม่ข่าย
11. ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ต

ความมั่นคงปลอดภัยของการตรวจจับการบุกรุก

แนวปฏิบัติ

1. จัดให้ทำ Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของบริษัท และเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทางซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง
2. ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS
3. IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ
4. พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ
5. มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต
6. หน่วยงานเทคโนโลยีสารสนเทศ มีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งให้ผู้ใช้งานทราบล่วงหน้า

นโยบายการตรวจสอบและประเมินความเสี่ยง

การตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

แนวปฏิบัติ

1. บริษัท ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ และเครือข่ายการสื่อสารข้อมูลอย่างน้อยปีละ 1 ครั้ง
2. บริษัทต้องจัดให้มีการตรวจสอบและประเมินการรักษาความมั่นคงปลอดภัยสารสนเทศทั้งจากผู้ตรวจสอบภายใน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)
3. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศของบริษัท ได้รับความเสียหายหรืออันตรายใดๆอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท ผู้กระทำการดังกล่าว ต้องรับผิดชอบ และชดใช้ค่าเสียหายที่เกิดขึ้นทั้งหมด
4. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศของบริษัท ก่อให้เกิดความเสียหาย หรืออันตรายใดๆแก่บริษัท หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้กระทำการดังกล่าวต้องรับผิดชอบชดใช้ค่าเสียหายที่เกิดขึ้นทั้งหมด
5. กำหนดให้ผู้บริหารระดับสูง และคณะอนุกรรมการบริหารความเสี่ยง มีหน้าที่กำกับดูแลรับผิดชอบการดำเนินงานด้านสารสนเทศ และผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายใดๆที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศของบริษัท

การใช้สิทธิ์ในการเข้าถึงข้อมูลสารสนเทศในการตรวจสอบและประเมินความเสี่ยง

แนวปฏิบัติ

1. เจ้าหน้าที่หน่วยงานเทคโนโลยีสารสนเทศ มีหน้าที่เก็บและตรวจสอบข้อมูลสารสนเทศที่มีอยู่ในระบบ รวมทั้งมีหน้าที่เก็บบันทึกข้อมูลจราจรทางคอมพิวเตอร์ของผู้ใช้งานภายในบริษัท ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่นๆที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ โดยจากเก็บรักษาไว้ไม่น้อยกว่า 90 วัน

2. หน่วยงานเทคโนโลยีสารสนเทศ และหน่วยงานที่เกี่ยวข้อง มีหน้าที่กำหนดสิทธิ์การเข้าใช้งานระบบสารสนเทศของบริษัททุกระบบ ให้แก่ผู้ใช้งานทั้งผู้ใช้งานภายในและผู้ใช้งานภายนอกทุกระดับ ได้แก่ ระดับผู้ใช้งานทั่วไป ระดับเจ้าของระบบงาน และระดับผู้ดูแลระบบ หรือได้รับการมอบหมายจากผู้บริหาร
3. เจ้าหน้าที่ของบริษัททุกคน เมื่อพบข้อบกพร่องด้านความมั่นคงปลอดภัยของบริษัท หรือเหตุการณ์ละเมิดความมั่นคงปลอดภัยต่างๆ หรือการละเมิดข้อกำหนดนี้ ให้แจ้งหน่วยงานเทคโนโลยีสารสนเทศ หรือหน่วยงานที่รับผิดชอบทันที
4. ห้ามเจ้าหน้าที่กระทำการใดๆ ที่มีผลให้เกิดอันตราย เป็นภัยคุกคาม หรือเป็นโทษกับผู้อื่น ได้แก่ การทำให้ลดประสิทธิภาพในการทำงานของเครือข่ายคอมพิวเตอร์ การกีดกัน ถอดถอนสิทธิในการใช้งานเครือข่ายคอมพิวเตอร์ของเจ้าหน้าที่ที่มีสิทธิ์ในการใช้งาน การเพิ่มสิทธิในการใช้งานเกินกว่าสิทธิที่กำหนดไว้ หรือการใช้อุบายดักการตรวจสอบความมั่นคงปลอดภัยของคอมพิวเตอร์ของบริษัท
5. เจ้าหน้าที่ของบริษัททุกคน ต้องไม่พยายามที่จะเข้าถึงข้อมูลใดๆ หรือระบบงานใดๆ ที่มีอยู่ในระบบเครือข่ายคอมพิวเตอร์ของบริษัท ที่เจ้าหน้าที่นั้น ไม่มีสิทธิในข้อมูลหรือระบบงานนั้นๆ เว้นแต่จะได้รับอนุญาตจากผู้มีอำนาจอนุมัติ
6. การเข้าใช้งานระบบสารสนเทศ ต้องมีการกำหนดชื่อผู้ใช้งาน และรหัสผ่าน และสิทธิ์การเข้าใช้งาน
7. รหัสผู้ใช้งาน และรหัสผ่าน หรือข้อมูลประเภทที่คล้ายกัน หรืออุปกรณ์ที่ใช้ในการยืนยันสิทธิในการใช้งานซึ่งยืนยันตัวตนบุคคลถือว่าเป็นข้อมูลความลับ โดยห้ามกระทำการเผยแพร่ต่อบุคคลภายนอก และเจ้าของรหัส ไม่สามารถปฏิเสธความรับผิดชอบได้ ในกรณีที่เกิดความเสียหายของข้อมูลหรือระบบดังกล่าว

การให้การสนับสนุนต่อ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และ พ.ศ.2560 และ พ.ร.บ. รักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

แนวปฏิบัติ

ผู้ใช้งานเครือข่าย และสารสนเทศของบริษัท ต้องไม่กระทำการอันเป็นการกระทำความผิดตาม พ.ร.บ. คอมพิวเตอร์ และ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้

1. เข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกัน การเข้าถึงโดยเฉพาะของผู้อื่น โดยไม่ชอบด้วยนโยบายด้านการเก็บรักษาข้อมูลการจราจรทางคอมพิวเตอร์
2. พยายามหรือทำให้ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะแล้วนำไปเปิดเผยโดยมิชอบ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น
3. เข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน
4. จะทำด้วยประการใดโดยมิชอบ โดยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่น ที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์
5. ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติม ไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ
6. จะทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้
7. ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเลคทรอนิคส์แก่บุคคลอื่น โดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข
8. กระทำความผิดตามข้อ 5 หรือ 6 แล้ว
    - ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือภายหลัง
    - เป็นการกระทำที่เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในเศรษฐกิจของประเทศ และการกระทำความผิดดังที่กล่าวมาแล้วเป็นเหตุให้ผู้อื่นถึงแก่ความตาย
9. จำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะ เพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามข้อ 1 ถึงข้อ 7
10. นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ตามที่ระบุไว้ดังต่อไปนี้

    10.1 ปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

10.2 ข้อมูลอันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

10.3 ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

10.4 ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

10.5 เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตามข้อ 10.1 – 10.4

10.6 จงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามข้อ 10 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

11. นำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

12. ไม่ทำการใดๆที่เข้าข่ายลักษณะของภัยคุกคามทางไซเบอร์ ที่มีการแบ่งเป็น 3 ระดับ ดังต่อไปนี้

12.1 ภัยคุกคามทางไซเบอร์ในระดับเฝ้าระวัง หมายถึง ภัยคุกคามทางไซเบอร์ในระดับที่อาจก่อให้เกิดความเสียหาย แต่ยังไม่ก่อให้เกิดผลกระทบต่อบุคคล ทรัพย์สิน หรือข้อมูลที่เกี่ยวข้องที่สำคัญในระดับร้ายแรง

12.2 ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามในระดับร้ายแรงที่มีลักษณะดังต่อไปนี้

(ก) เป็นภัยคุกคามที่ก่อให้เกิดความเสี่ยงที่จะทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือการให้บริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ข) เป็นภัยคุกคามที่ก่อให้เกิดความเสี่ยงภัยจนอาจทำให้คอมพิวเตอร์ ระบบคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่เกี่ยวข้องกับภัยคุกคามต่อความมั่นคงของรัฐ การป้องกันประเทศ ความสัมพันธ์ระหว่างประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชน ถูกแทรกแซงอย่างมีนัยสำคัญ หรือถูกระงับการทำงาน

(ค) เป็นภัยคุกคามที่มีความรุนแรงที่ก่อหรืออาจก่อให้เกิดความเสี่ยงภัย หรือความเสียหายต่อบุคคล หรือต่อข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ที่สำคัญจำนวนมาก

12.3 ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะดังต่อไปนี้

(ก) เป็นภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ฉุกเฉินเร่งด่วน ที่ใกล้จะเกิด และส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศสาธารณูปโภคขั้นพื้นฐาน ความมั่นคงของรัฐ หรือชีวิตความเป็นอยู่ของประชาชน

(ข) เป็นภัยคุกคามทางไซเบอร์ที่ฉุกเฉิน เร่งด่วน ที่ใกล้จะเกิดอันอาจเป็นผลให้บุคคลจำนวนมากเสียชีวิต หรือระบบคอมพิวเตอร์จำนวนมากถูกทำลายในวงกว้างระดับประเทศ

(ค) เป็นภัยคุกคามทางไซเบอร์ อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศ หรือส่วนหนึ่งส่วนใดของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วน เพื่อรักษาไว้ซึ่งการปกครองระบบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต และผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องกัน หรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

การแจกจ่ายเอกสารนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

1. แผนการเผยแพร่นโยบาย

   1.1 เอกสารนโยบายและแนวปฏิบัติฉบับนี้ จะจัดทำให้ผู้ใช้งานทุกคนได้อ่าน และทำความเข้าใจ

2. แผนการฝึกอบรม

   2.1 รวบรวมข้อมูล วิเคราะห์ว่าพนักงานหน่วยงานใดได้รับผลกระทบจากนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

2.2 พนักงานที่ได้รับผลกระทบดังกล่าว ต้องได้รับการฝึกอบรมเรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

2.3 ต้องสร้างความรู้ความเข้าใจกับผู้ใช้งานให้ทราบถึงความมั่นคงปลอดภัยสารสนเทศ เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัย และผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศ โดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ โดยฝึกอบรมการใช้งานระบบสารสนเทศของบริษัท หรือฝึกอบรมนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามความจำเป็น

บทลงโทษ

ผู้ใช้งานคนใด ฝ่าฝืนนโยบายและแนวปฏิบัติฉบับนี้ บริษัท จะพิจารณาลงโทษทางวินัย ตามระเบียบบริหารงานบุคคล รวมทั้งอาจมีความรับผิดทั้งทางแพ่ง และทางอาญา

การทบทวนนโยบาย

ผู้จัดการหน่วยงานเทคโนโลยีสารสนเทศ ต้องดำเนินการทบทวนนโยบายฉบับนี้เป็นประจำ อย่างน้อยปีละ 1 ครั้ง และต้องเสนอให้คณะกรรมการอนุมัติ หากมีการเปลี่ยนแปลง

ทั้งนี้ ให้มีผลตั้งแต่วันที่ 10 พฤษภาคม พ.ศ. 2566

(พิเศษ จียาศักดิ์)

ประธานกรรมการบริษัท