นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย เทคโนโลยีสารสนเทศ

INFORMATION TECHNOLOGY SECURITY POLICY

สารบัญ

	หน้า
1. บทนำ	1
2. วัตถุประสงค์	1
3. นิยามศัพท์	2
4. หน้าที่ความรับผิดชอบ	4
5. นโยบายการเข้าถึงหรือควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ	6
1) การควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ	6
2) การควบคุมการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ	7
3) การบริหารจัดการการเข้าถึงของผู้ใช้งาน	7
4) การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน และรหัสผ่านของเจ้าหน้าที่	7
5) วิธีการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ	8
6) การควบคุมการเข้าใช้งานระบบจากภายนอก	9
7) การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก	10
6. การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน	10
7. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม	11
8. นโยบายการบริหารจัดการระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน	14
9. การป้องกันโปรแกรมที่ไม่ประสงค์ดี	15
10. การเข้าถึงระบบโปรแกรมประยุกต์และสารสนเทศ	16
11. การบริหารจัดการการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย	18
12. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล	20
13. การใช้งานเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่	22
14. การใช้งานอินเทอร์เน็ต	24
15. การใช้งานจดหมายอิเล็กทรอนิกส์	25
16. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย	27
17. การสำรองและการกู้ข้อมูล และการเตรียมพร้อมกรณีฉุกเฉิน	28
18. ความมั่นคงปลอดภัยของ Firewall	30
19. ความมั่นคงปลอดภัยของการตรวจจับการบุกรุก	31
20. นโยบายการตรวจสอบและประเมินความเสี่ยง	32
21. การใช้สิทธิในการเข้าถึงข้อมูลสารสนเทศในการตรวจสอบและประเมินความเสี่ยง	32

สารบัญ

	หน้า
22. การให้การสนับสนุนต่อพ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2552 และพ.ศ. 2560 และพ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562	33
23. การแจกจ่ายเอกสารนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ	36
24. บทลงโทษ	36
25. การทบทวนนโยบาย	36

นโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

1. บทนำ

บริษัทได้ตระหนักดีถึงความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จึงได้มีการวางแผนจัดทำนโยบายและแนวปฏิบัติในการรักษามั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ขึ้น เพื่อให้ระบบสารสนเทศของบริษัทมีการควบคุมภายในที่ดี มีความมั่นคงปลอดภัย ถูกต้อง เชื่อถือได้ สามารถดำเนินงานได้อย่างต่อเนื่อง และสามารถป้องกันรักษาสารสนเทศที่เป็นความลับของบริษัท ทั้งที่เป็นข้อมูลของบริษัท ข้อมูลลูกค้า และข้อมูลส่วนบุคคลอื่นๆ ซึ่งนโยบายและแนวปฏิบัตินี้ จะเป็นกรอบแนวทางปฏิบัติของพนักงานทุกคนในองค์กร ให้มีความเข้าใจงานแต่ละระดับและร่วมมือ ในการใช้และเก็บรักษาข้อมูล, ระบบ และเครื่องใช้เทคโนโลยีสารสนเทศฯ อย่างมีประสิทธิภาพให้ถูกต้องตามกฎหมาย อีกทั้งปกป้องให้มีความปลอดภัย

2. วัตถุประสงค์

2.1 เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของบริษัท ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพ และประสิทธิผล และวัตถุประสงค์ที่กำหนดไว้

2.2 เพื่อกำหนดแนวปฏิบัติให้ผู้บริหาร ผู้ดูแลระบบ ผู้ใช้งาน และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัท ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท

2.3 เพื่อป้องกันไม่ให้ระบบสารสนเทศ และสารสนเทศของบริษัท ถูกบุกรุก เปลี่ยนแปลง ถูกขโมย ทำลาย หรือการประทำอื่นๆ ที่อาจสร้างความเสียหายต่อบริษัท

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

2.5 เพื่อเผยแพร่ให้ผู้ใช้งาน และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัท ซึ่งบริษัทหรือหน่วยงานในบริษัทอนุญาตให้มีสิทธิ์การเข้าถึงข้อมูล หรือระบบสารสนเทศ ได้รับทราบและถือปฏิบัติอย่างเคร่งครัด

เพื่อให้การปฏิบัติงานด้านเทคโนโลยีสารสนเทศของบริษัท ตะวันออกพาณิชย์ลีสซิ่ง จำกัด(มหาชน) เป็นไปตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2550 และ พ.ศ.2560 ได้กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ประกอบด้วยนโยบาย หลัก 3 ด้าน และแนวทางปฏิบัติภายในกรอบนโยบายหลัก ดังต่อไปนี้

1. นโยบายการเข้าถึงหรือควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ
2. นโยบายการบริหารจัดการระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน
3. นโยบายการตรวจสอบและประเมินความเสี่ยง

1. ด้านการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ เป็นนโยบายในการกำหนดการอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาต เช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

2. ด้านการบริหารจัดการระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน เป็นนโยบายในการธำรงไว้ ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่นได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability) รวมถึง กรณีที่เกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย

3. ด้านการตรวจสอบและประเมินความเสี่ยง เป็นนโยบายในการตรวจสอบและประเมินความเสี่ยง เพื่อกำกับดูแลการบริหารระบบสารสนเทศให้เกิดประสิทธิภาพและประสิทธิผล ตลอดจนการกำหนดแนวทางการแก้ไขปัญหาและอุปสรรคต่างๆ ที่เกิดขึ้น อย่างน้อยปีละ 1 ครั้ง เพื่อทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบัน

3. นิยามศัพท์

- **บริษัท** หมายถึง บริษัท ตะวันออกพาณิชย์ลีสซิ่ง จำกัด (มหาชน) (บริษัท)
- **ผู้ใช้งาน** หมายถึง กรรมการ ผู้บริหาร พนักงานของบริษัท ลูกจ้าง ผู้ดูแลระบบของบริษัท รวมทั้ง ผู้รับบริการ ผู้ใช้งานทั่วไป ที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหารหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของบริษัท โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (role) ที่บริษัทกำหนดไว้
- **ผู้ดูแลระบบ** (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
- **ผู้บริหารระดับสูง** หมายถึง ผู้อำนวยการ หรือรองผู้อำนวยการ ที่ได้รับมอบหมายในฐานะผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ
- **สิทธิของผู้ใช้งาน** หมายถึง สิทธิทั่วไป สิทธิ์จำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของบริษัท
- **สินทรัพย์** (asset) หมายถึง สิ่งใดก็ตามที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศที่มีคุณค่าสำหรับบริษัท
- **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาต เช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

- ☐ **ความมั่นคงปลอดภัยด้านสารสนเทศ** (information security) หมายถึง การธำรงไว้ ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)
- ☐ **เหตุการณ์ด้านความมั่นคงปลอดภัย** (information security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่าย ที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
- ☐ **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** (information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบของบริษัท ถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
- ☐ **สำนักงาน** หมายถึง บริษัทฯ ที่ประกอบด้วย สำนักงานใหญ่ และสาขา
- ☐ **ศูนย์เทคโนโลยีสารสนเทศ** หมายถึง ห้องเซิร์ฟเวอร์ของบริษัท
- ☐ **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท
- ☐ **ผู้ถือครองเครื่องคอมพิวเตอร์** หมายถึง ผู้ได้รับเครื่องคอมพิวเตอร์ไว้ใช้ประจำในการปฏิบัติงานและถือครอง รับผิดชอบ ดูแลเครื่อง/อุปกรณ์คอมพิวเตอร์
- ☐ **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ ระบบคอมพิวเตอร์ อาจประมวลผลได้ และให้หมายความรวมถึง ข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
- ☐ **ระบบเทคโนโลยีสารสนเทศ** (Information Technology System) หมายถึง ระบบงานของบริษัทที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ และอื่นๆ
- ☐ **ระบบเครือข่ายสื่อสาร** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการเชื่อมโยง หรือการส่งข้อมูลสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของบริษัท ซึ่งการเชื่อมโยงเป็นได้ทั้งในรูปแบบใช้สาย และแบบไร้สาย โดยระบบเครือข่ายสื่อสาร ระบบเครือข่ายระยะใกล้ (Local Area Network: LAN) ระบบเครือข่ายระยะไกล (Wide Ares Network: WAN) ระบบอินทราเน็ต (Intranet) และระบบอินเทอร์เน็ต (Internet)

- **เจ้าของข้อมูล** หมายถึง เจ้าหน้าที่ของหน่วยงานในบริษัท ผู้ได้รับมอบหมายจากผู้บังคับบัญชาให้รับผิดชอบดูแลปรับปรุงข้อมูลของระบบงานนั้นๆ ซึ่งเป็นผู้ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
- **จดหมายอิเล็กทรอนิกส์** (e-mail) หมายถึงระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP3 และ IMAP
- **รหัสผ่าน** (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
- **ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือ ระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคาสั่งที่กำหนดไว้
- **บุคคลภายนอก** หมายถึง บุคคล นิติบุคคล ซึ่งบริษัทหรือหน่วยงานในบริษัทอนุญาตให้มีสิทธิในการเข้าถึงข้อมูลหรือระบบสารสนเทศ โดยได้รับสิทธิตามประเภทการใช้งาน และต้องรับผิดชอบในการไม่เปิดเผยความลับของบริษัทโดยไม่ได้รับอนุญาต
- **ผู้รับการว่าจ้าง** หมายถึง บุคคล นิติบุคคล หรือหน่วยงานภายนอก ซึ่งได้รับการว่าจ้างจากบริษัท ให้ทำงานให้ในช่วงระยะเวลาหนึ่ง หรือทำงานในฐานะเป็นผู้ใช้งานของบริษัท ซึ่งรวมถึงลูกจ้างชั่วคราว โดยทั่วไปการว่าจ้างจะมีการทำสัญญาจ้างเพื่อควบคุมให้ผู้รับจ้างปฏิบัติตามเงื่อนไข หรือข้อตกลงการจ้างงานนั้น

4. หน้าที่ความรับผิดชอบ

4.1 หน้าที่ของคณะกรรมการบริหาร

4.1.1 กำหนดกลยุทธ์และภาพรวม ควบคุมการปฏิบัติงานในบริษัท และอนุมัตินโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท

4.2 หน้าที่ของคณะอนุกรรมการบริหารความเสี่ยง

4.2.1 กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท โดยกำหนดให้ไปในทิศทางเดียวกันกับแผนและเป้าหมายของบริษัท

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

4.2.3 นำเสนอผู้บริหารระดับสูง เช่น ประธานเจ้าหน้าที่บริหาร เรื่องแผนการปฏิบัติงาน นโยบาย งบประมาณ อัตรากำลัง ในด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

4.2.4 จัดให้มีการประเมิน และการบริหารความเสี่ยง ด้านสารสนเทศของบริษัท รายงานต่อคณะกรรมการบริหาร และคณะกรรมการตรวจสอบ เพื่อนำเสนอต่อคณะกรรมการบริษัทเป็นประจำทุกไตรมาส

4.2.5 เตรียมพร้อมรับสถานการณ์และเรียนรู้เทคนิคใหม่ๆ ทางด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

4.3 หน้าที่ของผู้อำนวยการฝ่ายปฏิบัติงานและบริหารงานกลาง และผู้จัดการแผนกไอที

4.3.1 ร่างนโยบาย แนวปฏิบัติ และระเบียบในการดำเนินการด้านนโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

4.3.2 ประเมินความต้องการใช้ทรัพยากรด้านสารสนเทศ ความคุ้มค่า รวมทั้ง การจัดหา และพัฒนาระบบสารสนเทศให้สอดคล้องกับกลยุทธ์ของบริษัท

4.3.3 ดูแลทรัพยากรด้านสารสนเทศของบริษัท ให้สามารถสนับสนุนการปฏิบัติงานภายในอย่างมีประสิทธิภาพ

4.4 หน้าที่ของผู้ใช้งาน

4.4.1 ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทโดยเคร่งครัด

4.4.2 ให้ความร่วมมือกับบริษัทอย่างเต็มที่ ในการป้องกันระบบคอมพิวเตอร์ และข้อมูลสารสนเทศของบริษัท สอดส่องดูแล ปกป้องข้อมูลและสารสนเทศของบริษัทให้มีความปลอดภัย

4.4.3 รายงานต่อบริษัททันที เมื่อพบเห็นการบุกรุก ขโมย ทำลาย หรือโจรกรรมสารสนเทศ รวมถึงระบบสารสนเทศที่อาจสร้างความเสียหายต่อบริษัท

4.5 หน้าที่ของหัวหน้า/ผู้จัดการของหน่วยงาน

4.5.1 ชี้แจงและส่งเสริมให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และตักเตือนลงโทษทางวินัย กรณีที่พบเห็นการปฏิบัติที่ไม่ถูกต้องเหมาะสม

4.6 หน้าที่ของเจ้าของข้อมูลและสารสนเทศ

4.6.1 จัดให้มีการทำเอกสาร มาตรการและขั้นตอนการควบคุมการเข้าถึงข้อมูล ให้เป็นไปตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท

4.6.2 ดูแลให้พนักงานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท

4.6.3 ควบคุมและอนุมัติการเข้าถึงข้อมูลและสารสนเทศ และระบบคอมพิวเตอร์ภายใต้หน้าที่และความรับผิดชอบ

4.6.4 รายงานเมื่อมีเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยของข้อมูลและสารสนเทศ

4.6.5 แจ้งแผนกไอทีเพื่อลบ/ เปลี่ยนแปลงสิทธิ์ เมื่อมีการเปลี่ยนแปลงพนักงาน/ อำนาจหน้าที่ / โอนย้าย

4.7 หน้าที่ของทีมตรวจสอบภายใน (Internal Audit)

4.7.1 ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ตามความจำเป็น

นโยบายการเข้าถึงหรือควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ

การควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ (Access Control)

แนวปฏิบัติ

1. การควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ

1.1 ผู้ดูแลระบบต้องดำเนินการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่ผู้ใช้งานได้รับอนุญาตหรือได้รับการมอบอำนาจ ตามที่กำหนดใน "การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่"

1.2 ผู้ดูแลระบบมีการกำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ดังนี้ อ่านข้อมูล, สร้างข้อมูล,นำเข้าข้อมูล แก้ไขข้อมูล, อนุมัติ และ ไม่มีสิทธิ

1.3 ผู้ดูแลระบบดำเนินการควบคุมการเข้าถึงที่เหมาะสมต่อหมวดหมู่ของสารสนเทศที่จัดไว้ตามระดับชั้นความลับ

1.4 ผู้ดูแลระบบมีการถอดสิทธิการเข้าถึงเข้าถึงการใช้งานสารสนเทศ ตามที่กำหนดใน "การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน"

1.5 ผู้ดูแลระบบเป็นผู้ควบคุมการเข้าถึงจากประเภทของการเชื่อมต่อทั้งหมด

1.6 ผู้ใช้งานที่ต้องการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน จะต้องได้รับการพิจารณาจากผู้บริหารของหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษรและหรือตามแบบฟอร์มที่แผนกไอทีกำหนด

1.7 ผู้ดูแลระบบกำหนดประเภทของข้อมูล ได้แก่ ข้อมูลภายนอกสามารถเปิดเผยได้ ข้อมูลภายในเป็นไปตามลำดับขั้นความลับของข้อมูล

1.8 ผู้ดูแลระบบกำหนดลำดับชั้นความลับของข้อมูล ได้แก่ ลับที่สุด ลับมาก ลับ และทั่วไป

1.9 ผู้ดูแลระบบกำหนดระดับชั้นการเข้าถึง ได้แก่ ผู้บริหาร ผู้ดูแลระบบ เจ้าของระบบ และผู้ใช้ระบบ

1.10 ผู้ดูแลระบบกำหนดเวลาและช่องทางที่เข้าถึงได้ ให้เหมาะสมตามแต่ละระบบงาน

2. การควบคุมการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

2.1 ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้บริหารของหน่วยงานต้นสังกัด และเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานเพื่อเข้าใช้งานระบบสารสนเทศเป็นลายลักษณ์อักษรและหรือตามแบบฟอร์มที่แผนกไอทีกำหนดตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

2.2 ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบเฉพาะในส่วนที่จำเป็น โดยต้องคำนึงถึงประเภทข้อมูลและชั้นความลับ โดยต้องมีการอนุญาตเข้าใช้งานเป็นลายลักษณ์อักษรจากต้นสังกัด เพื่อการจัดเก็บไว้เป็นหลักฐาน

2.3 เจ้าของข้อมูลและหรือเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานหรือตามความจำเป็นขั้นต่ำเท่านั้น โดยไม่อนุญาตให้กำหนดสิทธิ์เกินความจำเป็นในการใช้งาน โดยต้องมีการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลและหรือเจ้าของระบบงาน

3. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

3.1 การลงทะเบียนเจ้าหน้าที่ใหม่ กำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียน เจ้าหน้าที่ใหม่เพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็น รวมทั้ง ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งานเมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงาน ภายใน 15 วันทำการ นับจากวันที่ผู้มีอำนาจลงนามในคำสั่ง

3.2 ผู้ดูแลระบบกำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ ได้แก่ ระบบสารสนเทศโปรแกรมประยุกต์ (Application) ภายในบริษัท จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายระยะใกล้ (Local Area Network: LAN) ระบบเครือข่ายระยะไกล (Wide Ares Network: WAN) ระบบอินทราเน็ต (Intranet) และระบบอินเทอร์เน็ต (Internet) โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บริหารของหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษร รวมทั้ง ต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

4. การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่

4.1 ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้นๆ ต้องกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้ง กำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติตามที่กำหนดไว้ในเอกสาร "การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน"

4.2 การเปลี่ยนแปลงและการยกเลิกรหัสผ่าน ผู้ดูแลระบบต้องปฏิบัติตามที่กำหนดไว้ในเอกสาร "การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน"

4.3 กรณีผู้ดูแลระบบมีความจำเป็นต้องให้สิทธิ์เพิ่มเป็นกรณีพิเศษแก่ผู้ใช้งานที่มีสิทธิ์พื้นฐาน ต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงานต้นสังกัด และต้องมีการควบคุมผู้ใช้งานที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอ โดยต้องดำเนินการอย่างน้อย ดังนี้

4.3.1 ควบคุมการใช้งานอย่างเข้มงวดและอนุญาตให้เข้าใช้งานเฉพาะกรณีที่จำเป็นเท่านั้น

4.3.2 กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

4.3.3 กรณีมีการใช้งานไม่ต่อเนื่อง ให้มีการเปลี่ยนรหัสผ่านทุกครั้ง ภายหลังจากเสร็จสิ้นการใช้งานในแต่ละครั้ง หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานให้มีการเปลี่ยนรหัสผ่านทุก 3 เดือน

4.4 กำหนดขั้นตอนในการลงทะเบียนผู้ใช้งาน (user registration) ดังนี้

4.4.1 มีการระบุชื่อบัญชีผู้ใช้งานแยกเป็นรายบุคคล

4.4.2 การกำหนดชื่อผู้ใช้ กำหนดจากชื่อภาษาอังกฤษไม่ต่ำกว่า 4 อักขระ

4.4.3 มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานต้นสังกัด

4.4.4 มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศ การตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดสัญญาจ้าง เป็นต้น

5. วิธีการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

5.1 ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ หากข้อมูลมีความลับ

5.2 เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

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

5.4 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ SSL หรือ VPN

5.5 มีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลตามที่ระบุไว้ในเอกสาร "การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน"

การกำหนดชั้นความลับข้อมูล

1. ชั้นที่ 1 ข้อมูลเปิดเผยได้

- ข้อมูลที่บุคคลทั่วไปสามารถทราบได้โดยไม่ต้องมีการปิดกั้น เป็นข้อมูลที่ไม่มีผลต่อการปฏิบัติงานของบริษัท สามารถนำเสนอต่อบุคคลทั่วไป สาธารณชน หรือเป็นข้อมูลที่กฎหมายระบุว่าต้องเปิดเผย
- การเปิดเผยข้อมูลทั้งหมดหรือบางส่วน จะไม่เกิดผลเสียหายต่อบริษัท เช่น ข้อมูลที่เผยแพร่บนเว็บไซต์ของบริษัท เป็นต้น

2. ชั้นที่ 2 ข้อมูลใช้ภายในบริษัท

- ข้อมูลที่เจ้าของข้อมูลพิจารณาแล้วว่า สามารถเปิดเผยให้ผู้ใช้งานภายในบริษัทรับทราบได้ แต่ไม่สมควรเปิดเผยต่อบุคคลภายนอก เพราะอาจจะสร้างความเสียหายให้กับบริษัทได้

- การเปิดเผยข้อมูล เจ้าของข้อมูลต้องใช้ดุลยพินิจในการอนุญาตหรือได้รับความเห็นชอบจากผู้บริหาร คณะทำงาน หรือหน่วยงาน

3. ชั้นที่ 3 ข้อมูลลับ

- ข้อมูลที่บริษัทพิจารณาแล้วว่าไม่สามารถเปิดเผยให้ผู้ใช้งานทุกคนทราบได้ กำหนดให้เฉพาะผู้ที่เกี่ยวข้อง และจำเป็นต้องใช้ในการปฏิบัติงานทราบเท่านั้น และเป็นการใช้งานตามสิทธิ ความจำเป็นที่ควรทราบ เพื่อให้เพียงพอต่อการปฏิบัติงาน ข้อมูลมีความสำคัญต่อการดำเนินการของบริษัท เป็นข้อมูลภายใน และไม่สามารถเปิดเผยต่อบุคคลภายนอกที่ไม่เกี่ยวข้องตามกฎหมายได้ เนื่องจากข้อมูลนี้จะสร้างความเสียหายให้กับบริษัทได้

- การเปิดเผยข้อมูลจะต้องได้รับความเห็นชอบจากเจ้าของข้อมูล หรือคณะทำงาน หรือกรรมการผู้จัดการ หรือคณะกรรมการ

4. ชั้นที่ 4 ข้อมูลลับมาก

- ข้อมูลที่ใช้ภายในบริษัท แต่เป็นข้อมูลลับ ใช้งานโดยผู้ใช้งานบางกลุ่มของบริษัท ซึ่งมีรหัสพิเศษในการเข้าใช้งาน และไม่สามารถเปิดเผยต่อบุคคลภายนอกได้ เนื่องจากข้อมูลมีความจำเป็นต่อการปฏิบัติงานของบริษัท จะทำให้เกิดผลเสียหายร้ายแรงต่อบริษัท

- การเปิดเผยข้อมูล จะต้องได้รับความเห็นชอบจากเจ้าของข้อมูล หรือคณะทำงาน หรือกรรมการผู้จัดการ หรือคณะกรรมการ

5. ชั้นที่ 5 ข้อมูลลับที่สุด

- ข้อมูลที่ใช้ภายในบริษัทแต่เป็นข้อมูลลับ ใช้งานโดยผู้บริหารระดับสูงของบริษัทเท่านั้น ซึ่งมีรหัสพิเศษในการเข้าใช้งาน และเป็นการใช้เพื่อการวินิจฉัย และตัดสินใจที่สำคัญของบริษัท ไม่สามารถเปิดเผยต่อบุคคลภายนอกได้ เนื่องจากข้อมูลมีความจำเป็นต่อการปฏิบัติงานของบริษัท ทำให้เกิดผลเสียหายร้ายแรงต่อบริษัท

- การเปิดเผยข้อมูล ไม่สามารถทำได้ เว้นแต่การบังคับตามกฎหมาย

6. การควบคุมการเข้าใช้งานระบบจากภายนอก

6.1 ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับบริษัทอย่างเพียงพอ เพื่อขอใช้สิทธิ์ในการเข้าถึงระบบจากระยะไกล และต้องได้รับอนุมัติจากบริษัท

6.2 เจ้าหน้าที่แผนกไอทีเป็นผู้ควบคุมการเข้าถึงระบบจากระยะไกล (Remote access)

6.3 ผู้ใช้งานที่มีความจำเป็นต้องเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกล ต้องได้รับอนุมัติจากผู้จัดการแผนกไอที และมีการควบคุมอย่างเข้มงวด โดยผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าถึงระบบและข้อมูลอย่างเคร่งครัด

6.4 ผู้ดูแลระบบต้องควบคุมพอร์ต (Port) ที่ระบบสารสนเทศเทศให้บริการ ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

6.5 การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ผู้ดูแลระบบต้องอนุญาตตามพื้นฐานของความจำเป็นเท่านั้น และให้ปิด Port และ Modem เมื่อผู้ใช้งานได้ใช้งานเสร็จสิ้นแล้วทันที

7. การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก

ผู้ใช้งานระบบทุกคน เมื่อจะเข้าใช้งานระบบของบริษัท ต้องผ่านการพิสูจน์ตัวตนจากระบบของบริษัท โดยมีแนวทางปฏิบัติดังนี้

7.1 การแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username)

7.2 การพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password)

7.3 การเข้าสู่ระบบสารสนเทศของบริษัทจากอินเทอร์เน็ตนั้น จะต้องมีการตรวจสอบผู้ใช้งาน

7.4 การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน โดยใช้รหัสผ่าน หรือวิธีการเข้ารหัส

การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน

การบริหารรหัสผ่าน

1. แผนกไอทีต้องกำหนด ชื่อผู้ใช้ (Username) ระบบคอมพิวเตอร์เฉพาะบุคคลไม่ซ้ำกัน และกำหนดชื่อผู้ใช้ในส่วนของ ชื่อผู้ใช้ของผู้ใช้งาน ชื่อผู้ใช้ของผู้ดูแลระบบ ชื่อผู้ใช้ของผู้ดูแลฐานข้อมูล ชื่อผู้ใช้ของผู้พัฒนาระบบ ชื่อผู้ใช้ของเจ้าหน้าที่ทางเทคนิค หรืออื่นๆ ให้มีความแตกต่างกัน

2. การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องใส่ซองปิดผนึก ส่งไปยังผู้ใช้งาน พร้อมแจ้งช่องทางการเข้าถึง "แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ" เพื่อสร้างความรู้ความเข้าใจ และให้ผู้ใช้งานปฏิบัติตามโดยเคร่งครัด

3. แผนกไอทีกับหน่วยงานต่างๆ ของบริษัทจะทบทวนสิทธิการเข้าถึงระบบสารสนเทศของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง

การใช้งานรหัสผ่าน

4. ผู้ใช้งานต้องเก็บรักษารหัสผ่าน (Password) ของตนเองและของกลุ่มไว้เป็นความลับ

5. ห้ามทำการบันทึกรหัสผ่าน (Password) ไว้ในไปรษณีย์อิเล็กทรอนิกส์ หรือแบบฟอร์มอิเล็กทรอนิกส์ต่าง ๆ

6. ไม่จดหรือบันทึกรหัสผ่าน (Password) ส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

7. ผู้ใช้งานทุกคนต้องเปลี่ยนรหัสผ่าน (Password) เริ่มต้นทันที หลังจากได้รับมอบรหัสผ่านเริ่มต้นจากผู้ดูแลระบบของศูนย์เทคโนโลยีสารสนเทศ

8. กำหนดให้รหัสผ่าน (Password) ต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยควรมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน และไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้พจนานุกรม

9. ไม่ใช้รหัสผ่าน (Password) ส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

10. ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่เจ้าหน้าที่ครอบครองอยู่

11. ในกรณีที่ลืมรหัสผ่าน หรือสงสัยว่ารหัสผ่าน (Password) ถูกผู้อื่นทราบ ให้รีบทำการเปลี่ยนแปลงรหัสผ่านทันที หรือแจ้งให้แผนกไอทีทราบ เพื่อทำการเปลี่ยนรหัสผ่าน (Password) ทั้งหมดที่เกี่ยวข้อง

12. หากมีการกระทำความผิดเกิดขึ้นจากชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของบุคคลใด บุคคลนั้นต้องเป็นผู้รับผิดชอบต่อการกระทำความผิดนั้น ตามกฎหมาย ระเบียบ ข้อบังคับ ที่เกี่ยวข้อง

13. กรณีผู้ใช้งานของหน่วยงานภายในบริษัทลาออก ให้แผนกไอทีทำการยกเลิกสิทธิของผู้ที่ลาออก ออกจากระบบทันที

14. กรณีผู้ใช้งานของหน่วยงานภายในบริษัท มีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิ์การใช้งาน ให้หน่วยงานต้นสังกัด แจ้งแผนกไอที เพื่อทำการเปลี่ยนแปลงสิทธิ์ในการใช้งาน

15. ผู้ใช้งานทุกคนของบริษัท มีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยต้องไม่ยินยอมให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากชื่อผู้ใช้ (Username) ระบบคอมพิวเตอร์ของตน

การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
(Physical and environmental security)
แนวปฏิบัติ

1. **การบริหารจัดการทางกายภาพ** (Physical security management)

1.1 กำหนดระดับความสำคัญของพื้นที่ในศูนย์เทคโนโลยีสารสนเทศ

1.2 มีระบบป้องกัน ให้ครอบคลุมพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน หรือบริเวณที่มีความสำคัญ

1.3 ผู้ดูแลระบบ ต้องปิดประตูและหน้าต่างห้องแม่ข่ายให้ล็อคอยู่เสมอ

2. **การควบคุมการเข้า-ออก** (Physical entry controls)

2.1 ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาเยือน (Visitors)

2.2 ดูแลผู้ที่มาเยือนในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของสินทรัพย์หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

2.3 มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และควรมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

2.4 สร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

2.5 มีการควบคุมการเข้าถึงพื้นที่ ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

2.6 มีการพิสูจน์ตัวตน โดยการอ่านบัตรหรือการใช้รหัสผ่าน เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ

2.7 จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

2.8 บริษัทผู้ได้รับการว่าจ้าง ต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

2.9 ผู้มาเยือนต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในศูนย์เทคโนโลยีสารสนเทศ

2.10 จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

3. การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public access, delivery, and loading areas)

3.1 จำกัดพื้นที่หรือบริเวณสำหรับการเข้าถึงเพื่อการส่งมอบหรือขนถ่ายผลิตภัณฑ์โดยบุคคลภายนอก

3.2 ดูแลบุคลากรซึ่งสามารถเข้าถึงพื้นที่บริเวณส่งมอบหรือขนถ่ายผลิตภัณฑ์

3.3 ลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอก

4. การจัดวางและการป้องกันอุปกรณ์ (Equipment sitting and protection)

4.1 จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของผู้ปฏิบัติงานในศูนย์เทคโนโลยีสารสนเทศให้น้อยที่สุด

4.2 อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่ง ที่มีความมั่นคงปลอดภัย

4.3 ไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน

4.4 ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณ

5. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)

5.1 มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของบริษัท ที่เพียงพอต่อความต้องการใช้งาน โดยให้มีระบบสำรองกระแสไฟฟ้า (UPS) และระบบปรับอากาศ

5.2 ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนตาม 5.1 อย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

6. การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling security)

6.1 ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

6.2 จัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

6.3 ตู้ Rack ที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

7. การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

7.1 กำหนดให้มีการบำรุงรักษาอุปกรณ์อย่างน้อยปีละ 1 ครั้ง

7.2 ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

7.3 จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

7.4 จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

7.5 ควบคุมและสอดส่องดูแลการปฏิบัติงานของบริษัทผู้รับจ้างเหมาบำรุงรักษาระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ภายในบริษัท

7.6 ควบคุมการส่งอุปกรณ์ออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหาย หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

7.7 จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

8. การนำสินทรัพย์ของบริษัท ออกไปภายนอกสถานที่ (Removal of property)

8.1 ผู้ใช้งานต้องขออนุญาตหัวหน้าหน่วยงานต้นสังกัดก่อนนำอุปกรณ์หรือสินทรัพย์ออกนอกบริษัท

8.2 ผู้ใช้งานต้องบันทึกข้อมูลการนำอุปกรณ์ของบริษัท ออกไปภายนอกสถานที่ เพื่อเก็บไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนาอุปกรณ์ส่งคืน

9. การป้องกันสินทรัพย์ที่ใช้งานภายนอกบริษัท (Security of equipment off-premises)

9.1 กำหนดมาตรการความปลอดภัยของสินทรัพย์ เพื่อป้องกันความเสี่ยงจากการนำสินทรัพย์ของบริษัทออกไปใช้งานภายนอก

9.2 ไม่ทิ้งสินทรัพย์ของบริษัทไว้ในที่สาธารณะโดยไม่มีผู้ดูแลรับผิดชอบ

9.3 ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบดูแลสินทรัพย์ของบริษัท เสมือนเป็นสินทรัพย์ของตนเอง

10. **การกำจัดสินทรัพย์หรือการนำสินทรัพย์กลับมาใช้งานอีกครั้ง** (Secure disposal or re-use of equipment)

10.1 ให้ทำลายข้อมูลสำคัญในสินทรัพย์ก่อนที่จะกำจัดสินทรัพย์ดังกล่าว

10.2 มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในสินทรัพย์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนาสินทรัพย์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

นโยบายการบริหารจัดการระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน

การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ
(Communications and operations management)

แนวปฏิบัติ

1. **ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร** (Documented operating procedures)

1.1 มีการจัดทำคู่มือการปฏิบัติงานระบบเทคโนโลยีสารสนเทศ โดยมีรายละเอียดอย่างน้อย ดังนี้

- การปฏิบัติงานในห้องแม่ข่าย
- การเปิดและปิดระบบงาน ได้แก่ การเปิด - ปิดเครื่องแม่ข่าย การเปิด - ปิดระบบงาน การเปิด - ปิดระบบให้บริการ
- การสำรองข้อมูล
- การบำรุงรักษาอุปกรณ์
- การจัดการกับสื่อบันทึกข้อมูล ได้แก่ การทำป้ายชื่อบ่งชี้ การลบ การป้องกันการนำสื่อบันทึกข้อมูลกลับมาใช้งานอีกครั้ง
- การส่งงานเข้าไปประมวลผลในเครื่องคอมพิวเตอร์ และการจัดการกับข้อผิดพลาดที่เกิดขึ้น
- การประมวลผลข้อมูล ได้แก่ ขั้นตอนในการนำข้อมูลเข้าระบบงาน ประมวลผล และแสดงผล
- การใช้งานโปรแกรมยูทิลิตี้
- 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 มีการกำหนดแบ่งแยกหน้าที่ความรับผิดชอบในการปฏิบัติงานของแต่ละบุคคลไว้อย่างชัดเจนโดยมิให้มีการกำหนดหน้าที่ที่สำคัญไว้ที่บุคคลเพียงคนเดียว

3.2 ให้ผู้บังคับบัญชามีการควบคุมดูแลอย่างใกล้ชิดสำหรับงานที่มีความเสี่ยงต่อการเกิดความเสียหาย

3.3 ให้มีการจัดเก็บหลักฐานการปฏิบัติงานที่สามารถใช้ตรวจสอบได้ในภายหลัง

4. **การแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน** (Separation of development, test, and operational facilities)

4.1 ให้กำหนดมาตรการแยกเครื่องคอมพิวเตอร์ของระบบงาน สำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกันตามความจำเป็น เพื่อป้องกันผลกระทบจากการทำงาน

4.2 กำหนดมาตรการควบคุมการถ่ายโอนระบบงานจากเครื่องที่ใช้สำหรับการพัฒนา ไปสู่เครื่องที่ใช้สำหรับการให้บริการ

4.3 กำหนดให้มีการแยกบัญชีผู้ใช้งานออกจากกัน สำหรับระบบงานที่ใช้ในการพัฒนาทดสอบ และใช้ระบบงานจริง

การป้องกันโปรแกรมที่ไม่ประสงค์ดี
(Controls against malicious code)
แนวปฏิบัติ

1. ห้ามการติดตั้งซอฟต์แวร์อื่นๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งการใช้ไฟล์อื่นที่บริษัทไม่อนุญาตให้ใช้งาน

2. ให้ติดตั้งซอฟต์แวร์ เพื่อป้องกันโปรแกรมไม่ประสงค์ดีให้กับระบบเทคโนโลยีสารสนเทศของบริษัท

3. ให้ผู้ดูแลระบบดำเนินการตรวจสอบโปรแกรมไม่ประสงค์ดีในเครื่องเซิร์ฟเวอร์ให้บริการ และอุปกรณ์เทคโนโลยีสารสนเทศอื่นๆ ณ จุดทางเข้า-ออกเครือข่ายอย่างสม่ำเสมอ เพื่อดักจับโปรแกรมไม่ประสงค์ดีที่เข้าสู่ระบบ

4. กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติสำหรับการจัดการกับโปรแกรมไม่ประสงค์ดี ได้แก่ การรายงานการเกิดขึ้นของโปรแกรมไม่ประสงค์ดี การวิเคราะห์ การจัดการ การกู้คืนระบบจากความเสียหายที่พบ เป็นต้น

5. มีการติดตามข้อมูลข่าวสารเกี่ยวกับโปรแกรมไม่ประสงค์ดีอย่างสม่ำเสมอ

6. ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้ และให้รับทราบขั้นตอนปฏิบัติ เมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

7. เครื่องคอมพิวเตอร์ทั้งหมด ได้แก่ เครื่องคอมพิวเตอร์แม่ข่าย (Server) เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และเครื่องคอมพิวเตอร์แบบพกพา (Note book) ต้องได้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัสรุ่นล่าสุดของบริษัทจากเจ้าหน้าที่แผนกไอที และจะต้องเปิดใช้งานโปรแกรมตรวจสอบและกำจัดไวรัสตลอดเวลา

8. เครื่องคอมพิวเตอร์ Server ที่ให้บริการการตรวจสอบและกำจัดไวรัส ต้องมีการปรับปรุงข้อมูลล่าสุดของไวรัสอยู่เสมอ และต้องเป็นผู้ให้บริการปรับปรุงข้อมูลไวรัสล่าสุดให้แก่ เครื่องคอมพิวเตอร์ Server เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และเครื่องคอมพิวเตอร์แบบพกพาทุกเครื่องโดยอัตโนมัติ

9. ต้องทำการตรวจสอบไวรัสกับแฟ้มข้อมูล (file) ต่างๆ ที่ download มา แฟ้มข้อมูลที่แนบมากับไปรษณีย์อิเล็กทรอนิกส์, แฟ้มข้อมูลที่ได้มาจากสื่อบันทึกข้อมูลภายนอก (CD, Thumb Drive, Diskette or share file)

การเข้าถึงระบบโปรแกรมประยุกต์และสารสนเทศ

(Information handling procedures)

แนวปฏิบัติ

1. การจัดการสารสนเทศ

1.1 มีการกำหนดข้อมูลตามระดับชั้นความลับ ได้แก่ ข้อมูลทั่วไป ข้อมูลส่วนบุคคล ข้อมูลใช้ภายในข้อมูลลับ

1.2 มีขั้นตอนปฏิบัติเพื่อจัดการกับข้อมูลตามระดับชั้นความลับ ควรประกอบด้วยวิธีการประมวลผลการควบคุมการเข้าถึง การจัดเก็บ ระยะเวลาที่สามารถเข้าถึง และช่องทางการเข้าถึง

1.3 มีการจำกัดการเข้าถึงข้อมูลตามระดับชั้นความลับ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

1.4 มีมาตรการเพื่อตรวจสอบว่าข้อมูลที่นำออกจากระบบงานมีความถูกต้องและสมบูรณ์ก่อนที่จะนำไปใช้งานต่อไป

1.5 มีการจัดทำบัญชีรายชื่อผู้มีสิทธิเข้าถึงข้อมูลและสื่อบันทึกข้อมูลสำคัญ และมีการทบทวนบัญชีรายชื่ออย่างสม่ำเสมอ

1.6 การเข้าถึงต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

1.7 ระบบไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน จะต้องดำเนินการ ดังนี้

(1) ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่นๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อหน่วยงาน

(2) มีการควบคุมสภาพแวดล้อม ได้แก่ มีห้องแม่ข่ายเฉพาะ มีระบบไฟสำหรับระบบเฉพาะ มีระบบป้องกันผู้มีสิทธิเข้าออกห้องแม่ข่าย

(3) มีการควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา และต้องกำหนดมาตรการป้องกันความเสี่ยงที่มีต่ออุปกรณ์

1.8 การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking) จะต้องดำเนินการ ดังนี้

(1) ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของผู้ใช้งานจากระยะไกลตามแนวปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอก รวมถึงการเตรียมการระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องเพื่อให้มีความมั่นคงปลอดภัย

(2) ผู้ดูแลระบบเตรียมการป้องกันทางกายภาพสำหรับสถานที่ที่จะอนุญาตการปฏิบัติงานของผู้ใช้งานจากระยะไกล ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล

(3) ผู้ดูแลระบบมีการรักษาความมั่นคงปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่างๆ ภายในบริษัทก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกลตามแนวปฏิบัติการควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ

(4) ผู้ปฏิบัติงานจากระยะไกลต้องรักษาความลับของหน่วยงาน ไม่อนุญาตให้ครอบครัวหรือบุคคลอื่นๆ ใด เข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท

(5) การขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน ต้องปฏิบัติตาม "การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน"

2. การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of connection time)

2.1 กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการจำกัดช่วงระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น ได้แก่ กำหนดให้ใช้งานได้ 2 ช.ม. ต่อการเชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานตามปกติเท่านั้น หรือช่วงนอกเวลาทำงาน เป็นต้น

2.2 กำหนดให้ระบบเทคโนโลยีสารสนเทศ ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกบริษัท) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

3. การควบคุมการเข้าถึงระบบปฏิบัติการ (operation system access control)

3.1 กำหนดขั้นตอนปฏิบัติเพื่อเข้าใช้งานที่มั่นคงปลอดภัย

(1) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบ ก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

(2) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

(3) จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

(4) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

3.2 ระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติ ดังนี้

(1) ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน

(2) สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม

3.3 กำหนดหลักเกณฑ์ยุติการเชื่อมต่อ เมื่อว่างเว้นจากการใช้งานเป็นเวลา 30 นาทีเป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

3.4 กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อ เพื่อให้ผู้ใช้สามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้งานได้ 3 ชม. ต่อการเชื่อมต่อหนึ่งครั้ง หรือกำหนดให้ใช้งานได้เฉพาะช่วงเวลาเท่านั้น

4. การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit logging)

จัดให้มีการบันทึกข้อมูลพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบเทคโนโลยีสารสนเทศ ที่แสดงให้ทราบว่าใครทำอะไร ที่ไหน เมื่อไร และอย่างไร

การบริหารจัดการการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

แนวปฏิบัติ

1. การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

1.1 กำหนดให้มีรหัสผู้ใช้/รหัสผ่าน (Username/Password) ในการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและระบบปฏิบัติการ

1.2 กำหนดจำนวนครั้งที่สามารถพิมพ์รหัสผิดได้ หากเกินกว่าที่กำหนดระบบต้องทำการ Lock ไม่ให้ใช้งานเป็นระยะเวลาหนึ่ง

1.3 ผู้ดูแลระบบควรกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่ระบุไว้ในเอกสาร "การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน"

1.4 ผู้ดูแลระบบควรตั้งระบบการล็อคหน้าจอเมื่อไม่มีการใช้งาน เมื่อต้องการใช้งาน ผู้ใช้ต้องใส่รหัสผ่าน

1.5 ผู้ดูแลระบบต้องทำการ Logout 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 แจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

3.2 พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบงาน รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในกรณีที่บริษัทต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

4. การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

4.1 จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

4.2 ให้กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

4.3 ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

5. การเฝ้าดูและตรวจสอบ

5.1 ต้องดำเนินการเก็บ Log และ Audit Trails ของเหตุการณ์ละเมิดความมั่นคงปลอดภัยดังต่อไปนี้

5.1.1 Log ทั้งหมดที่เกี่ยวข้องกับเหตุการณ์ละเมิดความมั่นคงปลอดภัยต้องเก็บไว้อย่างน้อยเป็นเวลา 90 วัน

5.1.2 ต้องมีระบบจัดเก็บ Log ที่มีอยู่เกินกว่า 90 วัน ให้มีความปลอดภัยและพร้อมให้เรียกใช้งานได้เมื่อพนักงานเจ้าหน้าที่ต้องการ ต้องสามารถนำออกมามอบให้กับพนักงานเจ้าหน้าที่ได้

5.2 ผู้ดูแลระบบ ต้องตรวจสอบ Log และเหตุการณ์ละเมิดความมั่นคงปลอดภัย และรายงานให้กับผู้บังคับบัญชาทราบ ดังนี้

5.2.1 การโจมตีในรูปแบบ Port-Scan

5.2.2 การเข้าสู่ระบบของผู้ใช้งานที่ไม่มีสิทธิในการใช้งานระบบนั้น

5.2.3 เหตุการณ์ผิดปกติของเครื่องคอมพิวเตอร์ Server ที่เกิดขึ้น

5.3 ต้องดำเนินการบำรุงรักษา (Maintenance) เป็นประจำ

5.4 ต้องมีการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง พร้อมจัดทำรายงานผลการประเมินความเสี่ยงเสนอผู้บังคับบัญชา

การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer)

แนวทางปฏิบัติ

1. การปฏิบัติทั่วไป

1.1 เครื่องคอมพิวเตอร์ที่บริษัทอนุญาตให้ผู้ใช้งาน ใช้งานเป็นสินทรัพย์ของบริษัท ดังนั้น ผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของบริษัท

1.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของบริษัท ต้องเป็นโปรแกรมที่บริษัทได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย

1.3 ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ ของบริษัท และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

1.4 ไม่อนุญาตให้ ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม โปรแกรมยูทิลิตี้ ในเครื่องคอมพิวเตอร์ส่วนบุคคลของบริษัท เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากเจ้าหน้าที่ของแผนกไอที

1.5 การส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อม จะต้องได้รับการพิจารณาจากแผนกไอที

1.6 ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

1.7 ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น

1.8 ผู้ใช้งาน ต้องใช้งานโปรแกรมรักษาจอภาพ (Screen saver) โดยตั้งเวลาประมาณ 15 นาทีเพื่อให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้น เมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์

1.9 ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของบริษัท ยกเว้นจะได้รับการพิจารณาอนุมัติจากผู้จัดการแผนกไอที ก่อนการใช้งาน

1.10 ระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ส่วนบุคคลต้องมีการ Update service pack และhot fix ที่เป็น version ล่าสุดเสมอ โดยเจ้าหน้าที่ของแผนกไอที หรือผู้ดูแลระบบ

1.11 การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคลจะต้องกำหนดโดยเจ้าหน้าที่ของแผนกไอทีเท่านั้น

1.12 การเคลื่อนย้ายเครื่องคอมพิวเตอร์จากจุดเชื่อมต่อเครือข่ายเดิมไปยังจุดเชื่อมต่อเครือข่ายใหม่ภายในบริษัท จะต้องแจ้งแผนกไอทีดำเนินการให้เท่านั้น

1.13 กรณีส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมโดยผู้รับจ้าง เมื่อตรวจซ่อมเสร็จแล้วต้องให้เจ้าหน้าที่แผนกไอที เป็นผู้ติดตั้งโปรแกรมที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศของบริษัท

1.14 ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์ส่วนบุคคลของบริษัททุกเครื่อง เว้นแต่ได้รับความเห็นชอบจากเจ้าหน้าที่ของแผนกไอที

1.15 เครื่องคอมพิวเตอร์ทุกเครื่องต้องได้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัส โดยโปรแกรมป้องกันไวรัสของบริษัท จากเจ้าหน้าที่แผนกไอที

1.16 ผู้ใช้งานไม่ควรสร้าง short-cut หรือปุ่มกดง่าย บน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของบริษัท

1.17 ผู้ใช้งานมีหน้าที่และความรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์โดยต้องปฏิบัติ ดังนี้

- ไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์
- ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ disk drive

1.18 ห้ามเจ้าหน้าที่ทุกคนทำการปรับแต่งการตั้งค่าเวลาของเครื่องคอมพิวเตอร์ส่วนบุคคลของบริษัททุกเครื่อง และต้องดูแลมิให้เครื่องที่ถือครอบครองถูกแก้ไขการตั้งค่าเวลา ในกรณีที่ค่าเวลาของเครื่องคอมพิวเตอร์ส่วนบุคคลถูกแก้ไข เจ้าของเครื่องจะปฏิเสธความรับผิดชอบไม่ได้ และเมื่อรู้ว่าเครื่องมีการแก้ไขการตั้งค่าเวลาต้องแจ้งให้แผนกไอทีทราบทันที

1.19 ต้องทำการล้างข้อมูลในเครื่องคอมพิวเตอร์ทุกครั้งที่มีการเปลี่ยนเครื่องคอมพิวเตอร์ให้กับเจ้าของเครื่องรายใหม่ พร้อมทั้งต้องทำการปลด Password สำหรับการเข้าใช้เครื่องคอมพิวเตอร์ (ระบบปฏิบัติการ) และต้องทำการแจ้งการเปลี่ยนแปลงแก่ผู้ดูแลการใช้งานเครื่องคอมพิวเตอร์ทุกครั้ง

2. แนวทางปฏิบัติในการเข้าใช้เครื่องคอมพิวเตอร์ (ระบบปฏิบัติการ) และ รหัสผ่าน

2.1 ผู้ใช้งาน ต้องกำหนดชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

2.2 ผู้ใช้งาน ต้องกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตาม "การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน"

2.3 ผู้ใช้งาน ไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) ของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

3. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

3.1 ผู้ใช้งาน ควรตรวจสอบหาไวรัสจากสื่อต่างๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

3.2 ผู้ใช้งานควรตรวจสอบ File ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือ File ที่ download มาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

3.3 ผู้ใช้งานควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

4. การสำรองข้อมูลและการกู้คืน

4.1 ผู้ใช้งานเครื่องคอมพิวเตอร์ทุกเครื่อง มีหน้าที่ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกข้อมูลภายนอก

4.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

การใช้งานเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ (mobile computing)

แนวปฏิบัติ

1. การใช้งานทั่วไป

1.1 เครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ที่บริษัท อนุญาตให้ผู้ใช้งานใช้งานเป็นสินทรัพย์ของบริษัท ดังนั้น ผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่อย่างมีประสิทธิภาพเพื่องานของบริษัท

1.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ของบริษัท ต้องเป็นโปรแกรมที่บริษัทได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

1.3 ผู้ใช้งานควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

1.4 การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) จะต้องกำหนดโดยเจ้าหน้าที่ของแผนกไอที เท่านั้น

1.5 กรณีส่งเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ตรวจซ่อมโดยผู้รับจ้าง เมื่อตรวจซ่อมเสร็จแล้วต้องให้เจ้าหน้าที่แผนกไอที เป็นผู้ติดตั้งโปรแกรมที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศของบริษัท

1.6 ระบบปฏิบัติการบนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ต้องมีการ Update service pack และ hot fix ที่เป็น version ล่าสุดเสมอ โดยเจ้าหน้าที่ของแผนกไอทีเท่านั้น

1.7 ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม โปรแกรมยูทิลิตี้ ในเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ของบริษัท เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากเจ้าหน้าที่ของแผนกไอที

1.8 ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ทุกเครื่อง เว้นแต่ได้รับความเห็นชอบจากเจ้าหน้าที่แผนกไอที และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ให้มีสภาพเดิม

1.9 เครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ทุกเครื่องต้องได้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัสโดยโปรแกรมป้องกันไวรัสของบริษัทจากเจ้าหน้าที่ของแผนกไอที

1.10 การนำเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ทุกเครื่องออกไปใช้งานนอกบริษัท เมื่อนำกลับมาที่บริษัทต้องทำการเชื่อมต่อระบบเครือข่ายภายในบริษัท เพื่อทำการอัพเดท (Update) ข้อมูลไวรัสล่าสุด และต้องมี

การป้องกันความเสี่ยงจากการเข้าถึงสารสนเทศโดยไม่ได้รับอนุญาต จากบุคคลภายนอกบริษัท ซึ่งรวมถึงครอบครัวและเพื่อน

1.11 ห้ามผู้ใช้งานทุกคนทำการปรับแต่งการตั้งค่าเวลาของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ของบริษัททุกเครื่อง และต้องดูแลมิให้เครื่องที่ถือครอบครองถูกแก้ไขการตั้งค่าเวลา ในกรณีที่ค่าเวลาของเครื่องคอมพิวเตอร์ถูกแก้ไข เจ้าของเครื่องจะปฏิเสธความรับผิดชอบไม่ได้ และเมื่อรู้ว่าเครื่องมีการแก้ไขการตั้งค่าเวลาต้องแจ้งให้แผนกไอทีทราบทันที

1.12 การเชื่อมต่อเพื่อใช้ระบบงานจากภายนอกให้ปฏิบัติตามนโยบายการควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ (Access Control)

1.13 ต้องทำการลบข้อมูลทุกครั้งที่มีการเปลี่ยนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ให้กับเจ้าของเครื่องรายใหม่ พร้อมทั้งต้องทำการปลด Password สำหรับการเข้าใช้เครื่องคอมพิวเตอร์ (ระบบปฏิบัติการ) และต้องทำการแจ้งการเปลี่ยนแปลงแก่ผู้ดูแลการใช้งานเครื่องคอมพิวเตอร์ทุกครั้ง

2. ความปลอดภัยทางด้านกายภาพ

2.1 ผู้ใช้งาน มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย โดยการล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

2.2 ผู้ใช้งาน ไม่ควรเก็บหรือใช้งานเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ในสถานที่ที่มีความร้อน/ ความชื้น/ ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

2.3 ไม่ควรใส่เครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้

2.4 ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ควรใส่กระเป๋าสำหรับเครื่องเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน

2.5 หลีกเลี่ยงการของแข็งกดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่แตกเสียหายได้

2.6 ไม่วางของทับบนหน้าจอและแป้นพิมพ์

2.7 การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าที่มีรอยขีดข่วนได้

2.8 การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดอยู่ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

2.9 ไม่เคลื่อนย้ายเครื่องในขณะที่ฮาร์ดดิสก์กำลังทำงาน

2.10 ไม่ใช้หรือวางเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ใกล้สิ่งที่เป็นของเหลว

2.11 ไม่ใช้หรือวางเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส

2.12 ไม่ควรวางเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้

2.13 ไม่ควรติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่ที่มีการสั่นสะเทือน

3. การเข้าใช้เครื่องคอมพิวเตอร์ (ระบบปฏิบัติการ) และ รหัสผ่าน

3.1 ผู้ใช้งาน ต้องกำหนดชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่

3.2 ผู้ใช้งาน ต้องกำหนดรหัสผ่านให้มีคุณภาพดีตามที่ระบุไว้ในเอกสาร "ข้อกำหนดการจัดการชื่อผู้ใช้และรหัสผ่านของระบบสารสนเทศของบริษัท"

3.3 ผู้ใช้งาน ต้องใช้งานโปรแกรมรักษาจอภาพ (Screen saver) โดยตั้งเวลาประมาณ 15 นาที ให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน

3.4 ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

3.5 ผู้ใช้งาน ต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) ของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

4. การสำรองข้อมูลและการกู้คืน

4.1 เจ้าหน้าที่แผนกไอที มีหน้าที่ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น ฮาร์ดดิสก์แบบติดตั้งภายนอก เป็นต้น

4.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

5. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

5.1 ผู้ใช้งานควรตรวจสอบหาไวรัสจากสื่อต่างๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

5.2 ผู้ใช้งานควรตรวจสอบ File ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือ File ที่ download มาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

5.3 ผู้ใช้งานควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

การใช้งานอินเทอร์เน็ต (Use of the Internet)

แนวทางปฏิบัติ

1. ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย ได้แก่ Firewall , Proxy และ IPS/IDS

2. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บบราวเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บบราวเซอร์ติดตั้งอยู่

3. ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของบริษัท เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม

4. ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของบริษัท โดยผ่านความเห็นชอบจากผู้บริหารของหน่วยงานต้นสังกัด

5. ผู้ใช้งานต้องไม่กระทำการเปิดเผยข้อมูลสำคัญเกี่ยวกับงานของบริษัท ที่ไม่เข้าหลักเกณฑ์การเปิดเผยประกาศอย่างเป็นทางการ ผ่านทางอินเทอร์เน็ตความลับ

6. ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

7. การใช้งานเว็บบอร์ด (Web Board) ของบริษัท ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของบริษัท

8. หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

9. ผู้ใช้งานต้องปฏิบัติตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และ พ.ศ. 2560 อย่างเคร่งครัด

การใช้งานจดหมายอิเล็กทรอนิกส์ (Use of Electronic Mail)

แนวทางปฏิบัติ

1. ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทเท่านั้น ในการติดต่อหรือรับ-ส่งข้อมูลกับหน่วยงานภายนอกทั้งราชการ และเอกชน ผ่านทางจดหมายอิเล็กทรอนิกส์

2. แผนกไอที เป็นผู้กำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของบริษัท ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของผู้ใช้งานรวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เมื่อมีการลาออก เป็นต้น

3. การรับ-ส่งข้อมูลของบริษัทที่เป็นความลับ ห้ามรับ-ส่งผ่านทางระบบจดหมายอิเล็กทรอนิกส์

4. ผู้ใช้งานรายใหม่จะต้องทำการเปลี่ยนรหัสผ่าน (Password) โดยทันที เมื่อได้รับรหัสผ่าน (default password) ในการผ่านเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรก โดยต้องกำหนดรหัสผ่านให้มีคุณภาพดีตามที่ระบุไว้ใน "การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน"

5. ห้ามผู้ใช้งานตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

6. ผู้ใช้งานควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด โดยเปลี่ยนรหัสผ่านทุก 3-6 เดือน

7. ผู้ใช้งาน ต้องไม่ใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อบริษัท หรือละเมิดสิทธิ์สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม หรือส่งต่อข้อความที่กล่าวร้าย ทำให้เสื่อมเสีย หรือข้อความที่หยาบคาย ลามก ข่มขู่ ก่อกวน หรือสร้างความเสียหายให้กับผู้อื่น รวมถึงไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของบริษัท

8. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ให้ทำการออกจากระบบ (Log out) ทุกครั้งเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

9. ระบบจดหมายอิเล็กทรอนิกส์ของบริษัท มีการตัดการใช้งานของผู้ใช้งาน (Log out หน้าจอ) เมื่อผู้ใช้งานไม่ได้ใช้งานระบบเป็นเวลา 30 นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง

10. ผู้ใช้งาน ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file

11. ผู้ใช้งาน ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก ในเครื่องที่อยู่ในระบบเครือข่ายของบริษัท

12. ผู้ใช้งาน ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

13. ผู้ใช้งาน ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

14. ผู้ใช้งานต้องไม่ส่งหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่มีข้อมูลคอมพิวเตอร์ โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ประเภทดังต่อไปนี้

14.1 ข้อมูลคอมพิวเตอร์อันเป็นเท็จ

14.2 ข้อมูลคอมพิวเตอร์อันเป็นเท็จ ที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

14.3 ข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

14.4 ข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกอนาจาร

15. ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่นเพื่ออ่าน รับส่ง ข้อความยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

16. ผู้ใช้งาน ต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของบริษัท ทำให้เกิดความแตกแยกระหว่างบริษัท ผ่านทางจดหมายอิเล็กทรอนิกส์

17. ข้อควรระวัง ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้น ไม่ควรจัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)
แนวทางปฏิบัติ

1. ห้ามใช้ระบบเครือข่ายไร้สายภายในอาคารของบริษัท ในระหว่างที่บริษัท ยังไม่มีการติดตั้งระบบบริหารจัดการและระบบรักษาความปลอดภัยสาหรับระบบเครือข่ายไร้สายโดยเฉพาะ
2. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายชั่วคราวของบริษัท จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับการพิจารณาอนุมัติจากผู้จัดการแผนกไอที ตามความจำเป็นในการใช้งาน
3. ผู้ดูแลระบบต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย
4. ผู้ดูแลระบบต้องต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (access point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้
5. ผู้ดูแลระบบต้องควรทำการเปลี่ยนค่า SSID (service set identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (access point) มาใช้งาน
6. ผู้ดูแลระบบต้องควรเปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบ สำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และควรจะเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย
7. ผู้ดูแลระบบต้องต้องกำหนดค่าใช้ Wep (wired equivalent privacy) หรือ WPA (Wi-Fi protected access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN client และอุปกรณ์กระจายสัญญาณ (access point) เพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากขึ้น
8. ผู้ดูแลระบบต้องควรเลือกใช้วิธีการควบคุม MAC Address (media access control address) และชื่อผู้ใช้ (username) รหัสผ่าน (password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้ (username) รหัสผ่าน (password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง
9. ผู้ดูแลระบบต้องควรจะมีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน
10. ผู้ดูแลระบบต้องต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่าย ไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

11. ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้บริหารให้ทราบโดยทันที

การสำรองและกู้คืนข้อมูล) และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and Recovery and IT Continuity Plan)

แนวทางปฏิบัติ

1. การสำรองข้อมูลและกู้คืนข้อมูลในสถานการณ์ปกติ เมื่อมีระบบงานใหม่หรือข้อมูลใหม่ หรือข้อมูลที่มีการเปลี่ยนแปลงใหม่ กำหนดให้ใช้แนวทางปฏิบัติในการจัดทำนโยบายการสำรอง และกู้คืนข้อมูล ดังต่อไปนี้

1.1 มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

1.2 กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

- กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง
- กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง
- บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ขนาดข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
- ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน ได้แก่ระบบปฏิบัติการ ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลในฐานข้อมูล
- จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน
- ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ
- จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้
- ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

1.3 กำหนดผู้รับผิดชอบในการสำรองข้อมูล

1.4 กำหนดชนิดของระบบงานนั้น ที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ อย่างน้อย ต้องประกอบด้วยข้อมูลในระบบ ข้อมูลของระบบงาน และข้อมูลสำหรับตัวระบบ ได้แก่ ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์อื่นๆ ที่เกี่ยวข้อง เป็นต้น

1.5 กำหนดความถี่ในการสำรองข้อมูล ขึ้นอยู่กับความสำคัญของข้อมูลและการยอมรับความเสี่ยงที่กำหนดโดยเจ้าของข้อมูล หรือระบบ

1.6 กำหนดขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง รวมทั้งซอฟต์แวร์

1.7 การเก็บสื่อบันทึกข้อมูลสำรองต้องถูกเก็บไว้บริเวณพื้นที่ภายนอกอาคารของบริษัท

1.8 ต้องจัดทำฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อสำรองข้อมูล เพื่อให้สามารถค้นหาได้โดยเร็ว

1.9 ข้อมูลที่สำรองไว้ต้องได้รับกระบวนการพิสูจน์ความสมบูรณ์ครบถ้วนของข้อมูลในการสำรองข้อมูลทุกครั้ง

1.10 ต้องทำการทดสอบกู้คืนข้อมูลที่สำรองไว้ อย่างน้อยปีละ 1 ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้ เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่างสมบูรณ์

1.11 จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้คืนระบบกลับคืนได้ภายในระยะที่กำหนด

1.12 การสำรองข้อมูล และการกู้ข้อมูลของทุกระบบ ต้องถูกบันทึกเป็นเอกสาร และมีการตรวจสอบความถูกต้องเป็นระยะๆ

1.13 ต้องมีการตรวจสอบรายงานบันทึกการเก็บสื่อข้อมูลที่สถานที่เก็บข้อมูลสำรองเป็นประจำทุกปี

1.14 สื่อบันทึกข้อมูลสำรองต้องมีการเปลี่ยนสื่อตามอายุการใช้งานของสื่อตามประเภทของสื่อแต่ละชนิด

1.15 การขอใช้งานสื่อบันทึกข้อมูลสำรองจะต้องได้รับอนุมัติจากผู้มีอำนาจหน้าที่ และจัดทำทะเบียนคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง โดยต้องมีรายละเอียดเกี่ยวกับผู้รับ ผู้ส่ง ผู้อนุมัติประเภทข้อมูล และเวลา

2. ต้องจัดทำ แผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทางต่อไปนี้

2.1 มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

(1) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(2) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น ได้แก่ ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว น้ำท่วม การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(3) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(4) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(5) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(6) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

2.2 มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง

3. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

4. พนักงานที่เกี่ยวข้องกับแผนสำรองฉุกเฉิน ต้องเข้ารับการอบรม หรือสร้างความตระหนักเพื่อให้รู้หรือทราบวิธีปฏิบัติในกรณีที่เกิดเหตุฉุกเฉินในกรณีต่างๆ

5. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

6. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ 1 ครั้ง

ความมั่นคงปลอดภัยของ Firewall

แนวปฏิบัติ

1. แผนกไอที มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ (Fire wall) ทั้งหมด

2. การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

3. ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

4. ผู้ใช้งานอินเทอร์เน็ตจากภายนอก จะต้องมีการ Login account ก่อนการใช้งานทุกครั้ง

5. ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

6. การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

7. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

8. การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่แผนกไอทีอนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับการพิจารณาอนุมัติจากผู้จัดการแผนกไอที

9. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

10. ต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

11. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

12. แผนกไอที มีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทางานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

13. การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และได้รับความเห็นชอบจากสำนักงานก่อน

14. ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ต

ความมั่นคงปลอดภัยของการตรวจจับการบุกรุก

แนวปฏิบัติ

1. ให้จัดทำ Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของสานักงาน และเครือข่ายข้อมูลทั้งหมดรวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

2. ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

3. IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

4. พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

5. มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต

6. สำนักงาน มีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

นโยบายการตรวจสอบและประเมินความเสี่ยง

การตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

แนวปฏิบัติ

1. สำนักงานต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศและเครือข่ายการสื่อสารข้อมูล อย่างน้อยปีละ 1 ครั้ง

2. สำนักงานต้องจัดให้มีการตรวจสอบและประเมินการรักษาความมั่นคงปลอดภัยระบบสารสนเทศทั้งจากผู้ตรวจสอบภายใน (Internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor)

3. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศของสำนักงานได้รับความเสียหาย หรืออันตรายใดๆ อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน ผู้กระทำการดังกล่าว ต้องรับผิดชอบและชดใช้ค่าเสียหายที่เกิดขึ้นทั้งหมด

4. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศของสำนักงานก่อให้เกิดความเสียหาย หรืออันตรายใดๆ แก่สำนักงานหรือ ผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้กระทำการดังกล่าวต้องรับผิดชอบและชดใช้ค่าเสียหายที่เกิดขึ้นทั้งหมด

5. กำหนดให้ผู้บริหารระดับสูง และคณะอนุกรรมการบริหารความเสี่ยง มีหน้าที่กำกับดูแลรับผิดชอบการดำเนินงานด้านสารสนเทศ เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายใดๆ ที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศของสำนักงาน

การใช้สิทธิในการเข้าถึงข้อมูลสารสนเทศในการตรวจสอบและประเมินความเสี่ยง

แนวปฏิบัติ

1. เจ้าหน้าที่แผนกไอที มีหน้าที่เก็บและตรวจสอบข้อมูลสารสนเทศที่มีอยู่ในระบบ รวมทั้ง มีหน้าที่เก็บบันทึกข้อมูลจราจรทางคอมพิวเตอร์ของผู้ใช้งานภายในบริษัท ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ โดยจะเก็บรักษาไว้ไม่น้อยกว่า 90 วัน

2. แผนกไอทีและหน่วยงานที่เกี่ยวข้อง มีหน้าที่กำหนดสิทธิการเข้าใช้ระบบงานสารสนเทศของบริษัททุกระบบ ให้แก่ผู้ใช้งานทั้งผู้ใช้งานภายในและผู้ใช้งานภายนอกทุกระดับ ได้แก่ ระดับผู้ใช้งานทั่วไป ระดับเจ้าของระบบงาน และระดับผู้ดูแลระบบ หรืออื่นใดตามการมอบหมายจากผู้บริหาร

3. เจ้าหน้าที่ของบริษัททุกคน เมื่อพบข้อบกพร่องด้านความมั่นคงปลอดภัยของบริษัท หรือเหตุการณ์ละเมิดความมั่นคงปลอดภัยต่างๆ หรือการละเมิดข้อกำหนดนี้ ให้แจ้งแผนกไอทีหรือหน่วยงานที่รับผิดชอบทันที

4. ห้ามเจ้าหน้าที่กระทำการใดๆ ที่มีผลให้เกิดอันตราย เป็นภัยคุกคาม หรือเป็นโทษกับผู้อื่น ได้แก่ การทำให้ลดประสิทธิภาพในการทำงานของเครือข่ายคอมพิวเตอร์ การกีดกัน ถอดถอนสิทธิในการใช้งานเครือข่ายคอมพิวเตอร์ของเจ้าหน้าที่ที่มีสิทธิในการใช้งาน การเพิ่มสิทธิในการใช้งานเกินกว่าสิทธิที่กำหนดไว้ หรือการใช้อุบายดักการตรวจสอบความมั่นคงปลอดภัยของคอมพิวเตอร์ของบริษัท

5. เจ้าหน้าที่ของบริษัททุกคน ต้องไม่พยายามที่จะเข้าถึงข้อมูลใดๆ หรือระบบงานใดๆ ที่มีอยู่ในระบบเครือข่ายคอมพิวเตอร์ของบริษัท ที่เจ้าหน้าที่นั้น ไม่มีสิทธิในข้อมูลหรือระบบงานนั้นๆ เว้นแต่จะได้รับอนุญาตจากผู้มีอำนาจอนุญาต

6. การเข้าใช้งานของระบบสารสนเทศ ต้องมีการกำหนดชื่อผู้ใช้งานและ รหัสผ่าน และสิทธิ์การเข้าใช้งาน

7. รหัสผู้ใช้งาน และรหัสผ่านหรือข้อมูลประเภทที่คล้ายกัน หรืออุปกรณ์ที่ใช้ในการยืนยันสิทธิในการใช้งานซึ่งยืนยันตัวบุคคลถือว่าเป็นข้อมูลลับ โดยห้ามทำการเผยแพร่ต่อบุคคลภายนอก ให้ทราบ และเจ้าของรหัสไม่สามารถปฏิเสธความรับผิดชอบได้ในกรณีที่เกิดความเสียหายของข้อมูลหรือระบบดังกล่าว

การให้การสนับสนุนต่อ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพ.ศ. 2560 และ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

แนวปฏิบัติ

ผู้ใช้งานเครือข่ายและสารสนเทศของสำนักงาน ต้องไม่กระทำการอันเป็นการกระทำความผิดตาม พ.ร.บ.ฯ คอมพิวเตอร์ และ พ.ร.บ. การรรักษาความมั่นคงปลอดภัยไซเบอร์ฯ ดังนี้

1. เข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะของผู้อื่นโดยมิชอบด้วยนโยบายด้านการเก็บรักษาข้อมูลการจราจรทางคอมพิวเตอร์

2. พยายามหรือ ทำให้ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะแล้วนำไปเปิดเผยโดยมิชอบ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

3. เข้าถึงโดย มิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการ นั้นมิได้มีไว้สำหรับตน

4. กระทำด้วยประการใดโดยมิชอบ ด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์

5. ทำให้เสียหาย, ทำลาย, แก้ไข, เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

6. กระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอขัดขวาง หรือรบกวนจนไม่สามารถทางานตามปกติได้

7. ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่น โดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข

8. กระทำความผิดตามข้อ 5 หรือ ข้อ 6 แล้ว

- ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือภายหลัง
- เป็นการกระทำที่เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในเศรษฐกิจของประเทศ และกระทำความผิดดังที่กล่าวมาแล้วเป็นเหตุให้ผู้อื่นถึงแก่ความตาย

9. จำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะ เพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามข้อ 1 ถึง ข้อ 7

10. นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ตามที่ระบุไว้ดังต่อไปนี้

10.1 ปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

10.2 ข้อมูลอันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

10.3 ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

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. ไม่ทำการใดๆ ที่เข้าข่ายลักษณะของภัยคุกคามทางไซเบอร์ ที่มีการแบ่งเป็น 3 ระดับ ดังต่อไปนี้

12.1 ภัยคุกคามทางไซเบอร์ในระดับเฝ้าระวัง หมายถึง ภัยคุกคามทางไซเบอร์ในระดับที่อาจก่อให้เกิดความเสียหาย แต่ยังไม่ก่อให้เกิดผลกระทบต่อบุคคล ทรัพย์สิน หรือข้อมูลที่เกี่ยวข้องที่สำคัญในระดับร้ายแรง

12.2 ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามในระดับร้ายแรงที่มีลักษณะดังต่อไปนี้

(ก) เป็นภัยคุกคามที่ก่อให้เกิดความเสี่ยงที่จะทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือการให้บริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

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

(ค) เป็นภัยคุกคามที่มีความารุนแรงที่ก่อหรืออาจก่อให้เกิดความเสี่ยงภัย หรือความเสียหายต่อบุคคล หรือต่อข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่สำคัญหรือมีจำนวนมาก

12.3 ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะดังต่อไปนี้

(ก) เป็นภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ฉุกเฉินเร่งด่วน ที่ใกล้จะเกิด และส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สาธารณูปโภคขั้นพื้นฐาน ความมั่นคงของรัฐ หรือชีวิตความเป็นอยู่ของประชาชน

(ข) เป็นภัยคุกคามทางไซเบอร์ที่ฉุกเฉิน เร่งด่วน ที่ใกล้จะเกิดอันอาจเป็นผลให้บุคคลจำนวนมากเสียชีวิต หรือระบบคอมพิวเตอรีจำนวนมากถูกทำลายในวงกว้างระดับประเทศ

(ค) เป็นภัยคุกคามทางไซเบอร์อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศ หรือส่วนหนึ่งส่วนใดของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วน เพื่อรักษาไว้ซึ่งการปกครองระบบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องปัด หรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

การแจกจ่ายเอกสารนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

1. แผนการเผยแพร่นโยบาย

1.1 เอกสารนโยบายและแนวปฏิบัติฉบับนี้ จะจัดทำให้ผู้ใช้งานทุกคนได้อ่าน และทำความเข้าใจ และประกาศบนเว็บไซต์ของบริษัท

2. แผนการฝึกอบรม

2.1 รวบรวมข้อมูล วิเคราะห์ว่าพนักงานหน่วยงานใดได้รับผลกระทบจากนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

2.2 พนักงานที่ได้รับผลกระทบดังกล่าว ต้องได้รับการฝึกอบรมเรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

2.3 ต้องสร้างความรู้ความเข้าใจกับผู้ใช้งานให้ทราบถึงความมั่นคงปลอดภัยสารสนเทศ เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ โดยฝึกอบรมการใช้งานระบบสารสนเทศของบริษัท หรือฝึกอบรมนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามความจำเป็น

บทลงโทษ

ผู้ใช้งานคนใดฝ่าฝืนนโยบายและแนวปฏิบัติฉบับนี้ บริษัทจะพิจารณาลงโทษทางวินัยตามระเบียบบริหารงานบุคคล รวมทั้งอาจมีความรับผิดทั้งทางแพ่ง และทางอาญา

การทบทวนนโยบาย

ผู้จัดการแผนกไอที ต้องดำเนินการทบทวนนโยบายฉบับนี้เป็นประจำ อย่างน้อยปีละ 1 ครั้ง และต้องเสนอให้คณะอนุกรรมการบริหารความเสี่ยง และคณะกรรมการบริหารอนุมัติ หากมีการเปลี่ยนแปลง

ประกาศใช้ ณ วันที่ 1 กันยายน พ.ศ.2562 เป็นต้นไป

ลงชื่อ.....

(นายประภากร วีระพงษ์)

กรรมการผู้จัดการ