ORIGINAL ISMS

นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

Information Security Management System Policy

(ISMS Policy)

เลขที่เอกสาร	ISMS-PC-01-MIS
วันที่มีผลบังคับใช้	22 เมษายน 2567
ระดับชั้นความลับ	ภายใน
เจ้าของเอกสาร	ฝ่ายเทคโนโลยีสารสนเทศ
บังคับใช้	บุคลากร
ผู้อนุมัติ	คณะกรรมการระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ

ประวัติการแก้ไขเอกสาร

เวอร์ชัน	รายละเอียดการแก้ไข	วันที่มีผลบังคับใช้
1.0	เอกสารตั้งต้น	28/03/2566
2.0	- ปรับแก้เนื้อหา - ยกเลิกเอกสารที่เกี่ยวข้อง ISMS-PD-08-MIS_ แนวปฏิบัติการขอเข้าพื้นที่ควบคุม - เพิ่มเอกสารที่เกี่ยวข้อง ISMS-PD-19-MIS_ แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม	22/04/2567

ORIGINAL ISMS

การอนุมัติเอกสาร

เจ้าของเอกสาร	
ชื่อ ว่าที่ ร.ต. ชลิต สุนทรสุนทร ตำแหน่ง Manager วันที่ 22 เมษายน 2567	ลงชื่อ ..... (ISMS Working Committee)
ผู้ตรวจทานเอกสาร	
ชื่อ นางสาวปรียา แสงโชติ ตำแหน่ง Lead Officer วันที่ 22 เมษายน 2567	ลงชื่อ ..... (Document Control Officer)
ผู้อนุมัติเอกสาร	
ชื่อ นาย HSIN-WANG YANG ตำแหน่ง Chief Financial Officer วันที่ 22 เมษายน 2567	ลงชื่อ ..... (ISMS Management Committee)

สารบัญ

หน้า

1. บทนำ

บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด (“บริษัท”) คำนึงถึงความสำคัญของการนำเทคโนโลยีสารสนเทศ เข้ามาช่วยเพิ่มศักยภาพการดำเนินงานของบริษัท เพื่อก่อให้เกิดกระบวนการบริหารจัดการที่เป็นระบบ มีระเบียบ เป็นขั้นตอน ลดความซ้ำซ้อน ตอบสนองความต้องการของผู้ใช้บริการ และช่วยให้การดำเนินธุรกิจมีความต่อเนื่อง

บริษัทจึงได้เล็งเห็นว่าในการนำเทคโนโลยีสารสนเทศเข้ามาใช้ในการดำเนินงาน จำเป็นต้องกำหนดนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศฉบับนี้ขึ้นมาใช้เป็นแนวทางการพัฒนาให้สอดคล้องกับกลยุทธ์ และวิสัยทัศน์ของบริษัทฯ รวมถึงกฎหมาย ข้อบังคับ มาตรฐานสากลต่างๆ ที่เกี่ยวข้อง และการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศในปัจจุบัน เพื่อให้การให้บริการทางด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ มีประสิทธิผล มีความมั่นคงปลอดภัย และมีกรอบในการบริหารจัดการเทคโนโลยีสารสนเทศที่ดี รวมถึงเพื่อให้ผู้ที่เกี่ยวข้องเกิดความเชื่อมั่นในการให้บริการระบบสารสนเทศของบริษัทฯ

2. องค์ประกอบของนโยบาย

ส่วนที่ 1 หน้าที่ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Responsibilities)

ส่วนที่ 2 หน้าที่ของผู้ดูแลระบบเทคโนโลยีสารสนเทศ (Administrator Responsibilities)

ส่วนที่ 3 การใช้อุปกรณ์สื่อสารประเภทพกพา (Mobile Device)

ส่วนที่ 4 การใช้คอมพิวเตอร์ทำงานจากระยะไกล (Teleworking)

ส่วนที่ 5 การกำหนดความปลอดภัยด้านทรัพยากรบุคคล (Human Resource Security)

ส่วนที่ 6 การใช้รหัสผ่าน (Password)

ส่วนที่ 7 การใช้คอมพิวเตอร์พีซี/โน้ตบุ๊ค (Personal Computer/Notebook)

ส่วนที่ 8 การใช้คอมพิวเตอร์ซอฟต์แวร์ (Software Computer)

ส่วนที่ 9 การใช้อินเทอร์เน็ต และบริการเครือข่าย (Internet and Network Service)

ส่วนที่ 10 การใช้บริการอีเมล (E-mail Service)

ส่วนที่ 11 การใช้เครือข่ายสังคมออนไลน์ (Online Social Networking)

ส่วนที่ 12 การเผยแพร่ข้อมูลในเว็บไซต์ (Publish Information on Website)

ส่วนที่ 13 การรักษาและป้องกันความลับของข้อมูล (Information Protection)

ส่วนที่14 กำหนดความปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environment Security)

ส่วนที่ 15 การเข้ารหัสข้อมูล (Cryptography)

ส่วนที่ 16 การป้องกันไวรัสคอมพิวเตอร์ (Malware Protection)

ส่วนที่ 17 การไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น (Intellectual Property)

ส่วนที่ 18 การแลกเปลี่ยนสารสนเทศ (Information Sharing)

ส่วนที่ 19 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Reporting)

ส่วนที่ 20 การบริหารความต่อเนื่องของธุรกิจ (Business Continuity Management)

ส่วนที่ 21 การรับมือเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Security Management)

ส่วนที่ 22 การใช้งาน Cloud Computing อย่างปลอดภัย (Cloud Computing Security)

ส่วนที่ 23 การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศในการบริหารจัดการโครงการ (Information Security Project Management)

ส่วนที่ 24 การควบคุมการเข้าถึง (Access Control)

ส่วนที่ 25 ความมั่นคงปลอดภัยสารสนเทศด้านการสื่อสาร(Communication Security)

ส่วนที่ 26 การบริหารจัดการความเสี่ยง (Risk Management)

ส่วนที่ 27 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)

ส่วนที่ 28 การนำเครื่องคอมพิวเตอร์ที่บริษัทจัดสรรให้ออกนอกพื้นที่ (Taking Computers allocated by the Company out of the Area)

3. บทบังคับใช้และบทลงโทษ

นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศฉบับนี้ ให้มีผลบังคับใช้นับจากวันที่ประกาศให้มีผลบังคับใช้ต่อผู้ใช้งานระบบสารสนเทศของบริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด ภายใต้ขอบเขตการขอรับรองทั้งหมดโดยไม่มีการยกเว้น ผู้ฝ่าฝืนจะมีความผิดและต้องได้รับการลงโทษทางวินัยตามระเบียบที่บริษัทฯ กำหนดไว้

4. นโยบาย

4.1 ส่วนที่ 1 หน้าที่ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Responsibilities)

(1) พนักงานมีหน้าที่ในการรักษาความปลอดภัยของระบบข้อมูล ให้เป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยฉบับนี้

(2) ผู้บังคับบัญชาทุกระดับชั้นมีหน้าที่และความรับผิดชอบในการกำกับดูแลผู้ใต้บังคับบัญชาให้ปฏิบัติตามข้อกำหนดฉบับนี้อย่างเคร่งครัด

(3) พนักงานที่มีการกระทำที่ละเมิดกฎหมาย เช่น พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 หรือ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายอื่นๆ หรือละเมิดความปลอดภัยด้านสารสนเทศของบริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด โดยข้อเท็จจริงของการกระทำที่ส่อเจตนาในทางที่ไม่เหมาะสมให้ถือเป็นความผิดทางวินัย

4.2 ส่วนที่ 2 หน้าที่ของผู้ดูแลระบบเทคโนโลยีสารสนเทศ (Administrator Responsibilities)

(1) ต้องใช้บัญชีผู้ใช้งานและรหัสผ่านของตนเองในการควบคุมดูแลระบบเทคโนโลยีสารสนเทศ หรือหากมีความจำเป็นหรือมีข้อจำกัดบางประการ ต้องมีการกำหนดการควบคุมการใช้งานและมีการมอบหมายอย่างเป็นลายลักษณ์อักษรไว้

(2) ดูแลรักษาและปรับปรุงระบบคอมพิวเตอร์เพื่อให้สามารถใช้งานได้ตามความชำนาญและสอดส่องดูแลการใช้งานเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ให้เป็นไปตามนโยบายฉบับนี้

(3) สำรองข้อมูลสำคัญทางธุรกิจที่อยู่ในระบบสารสนเทศ (Data) โปรแกรมระบบปฏิบัติการ (Operating System) โปรแกรมระบบงานสารสนเทศ (Application System) และชุดคำสั่ง (Source Code) ให้ครบถ้วนพร้อมใช้งานได้อย่างต่อเนื่อง รวมถึงมีการจัดเก็บสื่อบันทึกข้อมูลสำรองไว้นอกสถานที่ โดยระเบียบปฏิบัติเพิ่มเติมให้อ้างอิงจากเอกสาร *ISMS-PD-06-MIS_แนวปฏิบัติการสำรองและทดสอบกู้คืนข้อมูล*

(4) มีการกำหนดการเข้าถึงหรือควบคุมการใช้งานสารสนเทศตามสิทธิของผู้ใช้งานที่ได้รับผิดตามความเหมาะสม

(5) ต้องไม่เข้าถึงข้อมูลส่วนบุคคลของบุคคลใดๆ รวมถึงข้อมูลทางธุรกิจโดยมิชอบ และต้องไม่กระทำการที่เข้าข่ายลักษณะการกระทำความผิดตามกฎหมาย

(6) ปฏิบัติตามเอกสาร *ISMS-PD-04-MIS_แนวปฏิบัติการควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ* เมื่อมีความจำเป็นต้องเปลี่ยนแปลงอุปกรณ์ระบบคอมพิวเตอร์ อุปกรณ์ระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์หรืออุปกรณ์ระบบคอมพิวเตอร์

(7) ต้องควบคุม จัดเก็บ ป้องกัน ข้อมูลคอมพิวเตอร์หรือสารสนเทศให้เป็นไปตามเอกสาร *ISMS-PD-05-MIS_แนวปฏิบัติการจัดระดับชั้นความลับ การบ่งชี้และการจัดการกับสารสนเทศ*

(8) จัดให้ทำคู่มือ แนวปฏิบัติหรือสิ่งอื่นใดที่จำเป็นต่อการควบคุมหรือการปฏิบัติการเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรือสารสนเทศ โดยต้องจัดทำเป็นลายลักษณ์อักษรที่อาจอยู่ในรูปสื่อสิ่งพิมพ์หรืออิเล็กทรอนิกส์ ทั้งนี้ ประเภทหรือจำนวนคู่มือ ขั้นตอนปฏิบัติดังกล่าวให้เป็นไปตามเอกสาร *ISMS-PD-05-MIS_แนวปฏิบัติการจัดระดับชั้นความลับ การบ่งชี้และการจัดการกับสารสนเทศ*

(9) ตรวจสอบความถูกต้องของข้อมูล เอกสาร หรือรายงานต่างๆ รวมทั้งแก้ไขให้ถูกต้องตามความจำเป็น ก่อนที่จะบันทึกข้อมูลหรือนำออกจากระบบงานของ บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด

4.3 ส่วนที่ 3 การใช้อุปกรณ์สื่อสารประเภทพกพา (Mobile Device)

(1) อุปกรณ์พกพา ได้แก่ เครื่องคอมพิวเตอร์พกพา (Laptop Computer) สมาร์ทโฟน (Smartphone) แท็บเล็ต (Tablet) เป็นต้น

(2) สื่อบันทึกข้อมูล ได้แก่ สื่อบันทึกข้อมูลทั่วไป เช่น ซีดีรอม (CD- ROM) ดีวีดีรอม (DVD-ROM) และสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ (Removable Media) ได้แก่ ฮาร์ดดิสก์ภายนอก (External Hard Disk) ทัมไดรฟ์ (Thumb Drive) ซีดีรอม (CD- ROM) ดีวีดีรอม (DVD-ROM) เป็นต้น

(3) บุคลากรที่มีความจำเป็นต้องใช้งานอุปกรณ์พกพาหรือสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้โดยอุปกรณ์นั้นเป็นทรัพย์สินของบริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด จะต้องมีการ

ดำเนินการขออนุมัติเพื่อยืมอุปกรณ์และต้องได้รับการอนุมัติก่อนนำไปใช้งาน และต้องดำเนินการคืนอุปกรณ์เหล่านั้นแก่ บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด เมื่อเสร็จสิ้นการใช้งาน

(4) กรณีบุคลากรนำอุปกรณ์พกพาส่วนบุคคลซึ่งไม่ได้เป็นทรัพย์สินของบริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด มาใช้ภายในบริษัท แบ่งเป็น 2 กรณี ดังนี้

(ก) อุปกรณ์พกพาส่วนบุคคลที่ใช้ในการปฏิบัติงานประจำ และสามารถเข้าถึงระบบสารสนเทศของ บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด ได้ จะต้อง

- มีการลงทะเบียนเพื่อขอใช้บริการเครือข่ายและระบบสารสนเทศของ บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด และต้องผ่านการพิสูจน์ตัวตนทุกครั้งก่อนการเข้าใช้งาน
- ได้รับสิทธิการเข้าถึงระบบเฉพาะที่เกี่ยวข้องกับการปฏิบัติงานของตนเอง และต้องได้รับการอนุมัติจากผู้มีอำนาจ
- มีการควบคุมการตั้งรหัสผ่านตามที่ระบุในส่วนที่ 6 การใช้รหัสผ่านของนโยบายฉบับนี้

(ข) อุปกรณ์พกพาส่วนบุคคลที่นำมาใช้งานชั่วคราว จะต้อง

- มีการลงทะเบียนเพื่อขอใช้บริการเครือข่ายไร้สายของ บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด และต้องผ่านการพิสูจน์ตัวตนทุกครั้งก่อนการเข้าใช้งาน
- ไม่สามารถใช้ทรัพยากรต่างๆ ในระบบเทคโนโลยีสารสนเทศของ บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด ได้ โดยเจ้าหน้าที่งานสนับสนุนทางเทคนิคจะอนุญาตให้อุปกรณ์พกพาส่วนบุคคลใช้บริการได้เฉพาะระบบอินเทอร์เน็ตเท่านั้น
- ควรมีการตั้งรหัสผ่านลงบนอุปกรณ์พกพา

(5) จัดให้มีระบบเครือข่ายที่มีความปลอดภัยและระบบเฝ้าระวังในการเข้าใช้งาน

(6) การจัดเก็บข้อมูลเพื่อใช้ปฏิบัติงานของ บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด บนอุปกรณ์พกพาหรือสื่อบันทึกข้อมูล ทั้งที่เป็นทรัพย์สินของ บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด และทรัพย์สินส่วนบุคคลบุคลากรจะต้องเข้มงวดในการป้องกันและรักษา

ความปลอดภัยไม่ว่าจะอยู่ภายใน บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด หรือในที่สาธารณะใดๆ

(7) ต้องมีความระมัดระวัง และหลีกเลี่ยงการละทิ้งอุปกรณ์หรือสื่อบันทึกข้อมูล ในที่สาธารณะ หรือในที่สามารถพบเห็นและหยิบง่าย

(8) บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด มีสิทธิในการตรวจสอบอุปกรณ์พกพาหรือสื่อบันทึกข้อมูล ทั้งที่เป็นทรัพย์สินของบริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด และทรัพย์สินส่วนบุคคล

4.4 **ส่วนที่ 4 การใช้คอมพิวเตอร์ทำงานจากระยะไกล** (Teleworking)

(1) พนักงานต้องไม่นำชื่อบัญชีผู้ใช้งานให้บุคคลอื่นใช้งาน และต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

(2) พนักงานต้องลงทะเบียนการใช้งานตามเอกสาร *ISMS-PD-14-MIS_แนวปฏิบัติในการเข้าถึงจากระยะไกล* บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด สงวนสิทธิ์ที่จะระงับการใช้งานระบบ VPN หากมีเหตุสงสัยว่าคอมพิวเตอร์นั้นไม่ปลอดภัยต่อเครือข่าย

(3) การใช้งานระบบ VPN ต้องมีการเข้ารหัสที่มีความมั่นคงปลอดภัยหรือตามมาตรฐานสากล เช่น SSL เป็นต้น

4.5 **ส่วนที่ 5 การกำหนดความปลอดภัยด้านทรัพยากรบุคคล** (Human Resource Security)

(1) มีกระบวนการคัดเลือกบุคลากรอย่างเหมาะสม เช่น การตรวจสอบภูมิหลังของผู้สมัครงานต้องมีการดำเนินการโดยมีความสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ และจริยธรรมที่เกี่ยวข้อง และต้องดำเนินการในระดับที่เหมาะสมกับตำแหน่งหน้าที่

(2) มีการทำข้อตกลงการปฏิบัติงานตามที่บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด กำหนดไว้ตามสัญญาการจ้างงาน

(3) ให้มีการฝึกอบรม ให้ความรู้ และสร้างความตระหนัก ให้ความรู้ และฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ

(4) ให้มีกระบวนการในกรณียุติการว่าจ้างหรือเปลี่ยนแปลงหน้าที่งาน รวมทั้งการยกเลิกสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศ และระบบเครือข่ายของบริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด และการส่งคืนทรัพย์สิน เมื่อหมดภาระหน้าที่

4.6 **ส่วนที่ 6 การใช้รหัสผ่าน** (Password)

(1) พนักงานต้องใช้รหัสผ่านที่เป็นของตนเองในการแสดงตนเข้าใช้งานหรือปฏิบัติงานในระบบข้อมูลตามสิทธิ์ที่ได้รับเท่านั้น

(2) พนักงานที่ได้รับรหัสผ่านในครั้งแรก ต้องเปลี่ยนรหัสผ่านใหม่ทันที เพื่อให้เป็นความลับเฉพาะตัว ในกรณีที่รหัสผ่านถูกเปิดเผยแล้ว พนักงานจะต้องทำการเปลี่ยนรหัสผ่านใหม่ทันที

(3) หากผู้ใช้งานพบเหตุที่สงสัยว่าถูกผู้อื่นนำรหัสผ่านไปใช้ ให้ดำเนินการเปลี่ยนรหัสผ่านและแจ้ง “ผู้ดูแลระบบ” ในทันที

(4) รหัสผ่านควรมีความยาวไม่น้อยกว่า 8 ตัวอักขระ ประกอบด้วย ตัวอักษร ตัวเลข หรือสัญลักษณ์อื่นใดที่ยากต่อการคาดเดา หรือตามความสามารถสูงสุดของระบบที่รับได้

(5) ไม่กำหนดรหัสผ่านจากชื่อ หรือนามสกุลของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือคำศัพท์ที่ปรากฏในพจนานุกรม

(6) กำหนดให้มีการเปลี่ยนรหัสผ่านทุกๆ 6 เดือน สำหรับผู้ใช้งานทั่วไป ทุก ๆ 3 เดือนสำหรับผู้ปฏิบัติทางเทคนิคบนระบบต่าง ๆ ทั้งนี้ ให้พิจารณาจากผลกระทบและความรุนแรง ต่อข้อมูล และภาพพจน์ชื่อเสียงของ บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด

(7) ห้ามเปิดเผยรหัสผ่านให้บุคคลอื่นทราบโดยเด็ดขาด

(8) ห้ามจดรหัสผ่านไว้บนกระดาษ หรือ เขียนติดไว้ที่เครื่องคอมพิวเตอร์ หรือ บริเวณโต๊ะทำงาน

(9) ห้ามนำรหัสผ่านเก่ากลับมาใช้ใหม่ จำนวน 3 ครั้ง รวมปัจจุบันเป็น 4 ครั้ง

4.7 **ส่วนที่ 7 การใช้คอมพิวเตอร์พีซี/โน้ตบุ๊ค** (Personal Computer/Notebook)

(1) ดูแลเครื่องคอมพิวเตอร์พีซี/โน้ตบุ๊คที่ตนเองถือครองให้อยู่ในสภาพเรียบร้อยและใช้งานเครื่องในลักษณะปกติเท่านั้น ไม่อนุญาตให้ดัดแปลง เพิ่ม หรือ ลดอุปกรณ์ใดๆ ของเครื่องคอมพิวเตอร์นั้น

(2) ห้ามติดตั้งหรือถอดถอนโปรแกรมคอมพิวเตอร์ที่ได้ติดตั้งหรือกำหนดให้ใช้งาน โดยการติดตั้งซอฟต์แวร์ให้ปฏิบัติตามเอกสาร *ISMS-PD-15-MIS_แนวปฏิบัติในการติดตั้งซอฟต์แวร์บนระบบงาน*

(3) ห้ามติดตั้งและใช้งานโปรแกรมประเภท FTP (File Transfer Protocol) เพื่อการเคลื่อนย้ายข้อมูล

(4) หากเกิดการชำรุด เสียหาย หรือสูญหายของเครื่องคอมพิวเตอร์พีซี/โน้ตบุ๊คที่ใช้งาน เมื่อสอบสวนแล้วและพบว่าไม่ได้ใช้ความระมัดระวังและดูแลอย่างเพียงพอ ต้องรับผิดชอบในการชำรุด เสียหาย หรือสูญหายนั้น

(5) ไม่อนุญาตให้นำเครื่องคอมพิวเตอร์พีซี/โน้ตบุ๊คไปใช้งานเพื่อการอื่นใดที่ไม่เกี่ยวข้องกับงานตามภารกิจหรือหน้าที่ความรับผิดชอบ

(6) ลบหรือมีมาตรการป้องกันข้อมูลสำคัญ (เช่น ข้อมูลลับ ข้อมูลใช้ภายในเท่านั้น โดยการเข้ารหัสข้อมูล) ที่อยู่ในเครื่องคอมพิวเตอร์พีซี/โน้ตบุ๊คก่อนส่งซ่อม

(7) สำรองข้อมูลในเครื่องพีซี/โน้ตบุ๊คที่ใช้งานอย่างสม่ำเสมอเพื่อป้องกันจากการสูญหายของข้อมูลในกรณีต่างๆ เช่น ฮาร์ดดิสก์เสีย ไฟกระชากจนทำให้ฮาร์ดดิสก์พัง หรืออื่นๆ

(8) ต้องไม่ใช้เครื่องคอมพิวเตอร์พีซี/โน้ตบุ๊คในทางที่ก่อหรือจะก่อให้เกิดความเสียหายต่อผู้อื่น ต่อบริษัท ผิดกฎหมายหรือศีลธรรมอันดี เช่น

- การเข้าถึงข้อมูล เครือข่าย หรือระบบงานโดยมิชอบหรือโดยไม่ได้รับอนุญาต
- การรบกวน หรือก่อความรำคาญต่อเครือข่ายหรือระบบงาน
- การดักรับหรือดักจับข้อมูลของผู้อื่น
- การลักลอบถอดรหัสผ่าน
- การปลอมแปลงหรือเปลี่ยนแปลงข้อมูลโดยมิชอบหรือโดยไม่ได้รับอนุญาต
- การเผยแพร่รูปภาพ ข้อความ หรือเสียงที่ไม่เหมาะสม
- การกระทำสิ่งใดที่ผิดกฎหมายหรือส่อเจตนาไปในทางที่ผิดจากพฤติกรรมการใช้งานปกติ

(9) ระมัดระวังและรักษาเครื่องโน้ตบุ๊คเมื่อมีการนำไปใช้งานนอกสถานที่ เพื่อป้องกันการสูญหาย และห้ามปล่อยเครื่องโน้ตบุ๊คทิ้งไว้โดยไม่มีผู้ดูแล

(10) ห้ามให้ผู้อื่นใช้งานเครื่องโน้ตบุ๊คของบริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด

(11) ต้องมีการพิสูจน์ตัวตนก่อนการเข้าใช้งานเครื่องคอมพิวเตอร์พีซี/โน้ตบุ๊ค ทุกครั้ง

(12) ตรวจสอบให้มีการตั้งค่า Screen Saver เพื่อให้เครื่องโน้ตบุ๊คทำการล็อคหน้าจอโดยอัตโนมัติหลังจากที่ไม่ได้มีการใช้งานเกินกว่า 15 นาที

4.8 ส่วนที่ 8 การใช้คอมพิวเตอร์ซอฟต์แวร์ (Software Computer)

(1) พนักงานต้องใช้คอมพิวเตอร์ซอฟต์แวร์ตามมาตรฐานที่ บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัดกำหนดไว้

(2) ห้ามพนักงานนำคอมพิวเตอร์ซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ใช้สิทธิ์มาใช้งานกับเครื่องคอมพิวเตอร์ของ บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด และหากเกิดการฟ้องร้องจากผู้เสียหายแล้ว พนักงานผู้นั้นต้องรับผิดชอบความเสียหายที่เกิดขึ้นทั้งหมด

(3) ห้ามพนักงานใช้อุปกรณ์คอมพิวเตอร์ บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด เพื่อทำการผลิต ครอบครอง หรือจำหน่ายคอมพิวเตอร์ซอฟต์แวร์ที่ไม่เหมาะสม หรือผิดกฎหมาย

(4) บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด ขอสงวนสิทธิที่จะเข้าตรวจสอบข้อมูลที่คอมพิวเตอร์ที่พนักงาน หากมีเหตุต้องสงสัยว่าพนักงานกระทำการสิ่งใดที่อาจส่งผลกระทบในทางเสียหายต่อ บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด

4.9 ส่วนที่ 9 การใช้อินเทอร์เน็ตและบริการเครือข่าย (Internet and Network Service)

(1) ใช้เพื่อปฏิบัติงานตามภารกิจของหน่วยงานหรือหน้าที่ความรับผิดชอบของตนเอง

(2) ไม่ใช้อินเทอร์เน็ตและบริการเครือข่ายของ บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด เพื่อ

- การกระทำที่ขัดต่อ พ.ร.บ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- ลามกอนาจาร เว็บไซต์ที่มีเนื้อหาต่อต้านชาติ ศาสนา พระมหากษัตริย์ เว็บไซต์ที่เป็นภัยต่อสังคม เว็บไซต์ที่เป็นการบ่อนทำลายต่อความมั่นคงของชาติ เป็นต้น
- เล่นเกม ดูภาพยนตร์ หรือฟังเพลงในเวลาทำงาน
- เข้าไปสนทนาในห้องสนทนาบนเครือข่ายอินเทอร์เน็ตในเวลาทำงาน
- ทำการดาวน์โหลดข้อมูลหรือโปรแกรมที่เป็นการละเมิดสิทธิหรือทรัพย์สินทางปัญญาของผู้อื่น
- เป็นช่องทางในการบุกรุกระบบของผู้อื่น

4.10 ส่วนที่ 10 การใช้บริการอีเมล (E-mail Service)

(1) ใช้งานอีเมลเพื่อปฏิบัติงานตามภารกิจของหน่วยงานหรือหน้าที่ความรับผิดชอบของตนเองที่ได้รับมอบหมาย

(2) ใช้ความระมัดระวังและตรวจสอบอีเมลแอดเดรสของผู้รับให้ถูกต้อง เพื่อป้องกันการส่งข้อมูลสำคัญผิดตัวผู้รับและทำให้ข้อมูลเกิดการรั่วไหล

(3) ระบุชื่อของผู้ส่ง ตำแหน่ง และข้อมูลติดต่อกลับไว้ในอีเมลทุกฉบับที่ส่งไปเพื่อเป็นข้อมูลในการติดต่อกลับ

(4) ใช้คำที่สุภาพในการส่งอีเมล

(5) จำกัดการส่งหรือส่งต่อข้อมูลทางอีเมลไปยังผู้รับหรือกลุ่มผู้รับอีเมลเท่าที่มีความจำเป็นต้องรับทราบข้อมูลในอีเมลนั้นเท่านั้น

(6) สำรองข้อมูลอีเมลตามความจำเป็นอย่างสม่ำเสมอ

(7) ในการติดต่องานตามภารกิจหรือหน้าที่ความรับผิดชอบของตนกับหน่วยงานภายในและภายนอก ห้ามให้ใช้อีเมลแอดเดรสอื่นๆ นอกเหนือจากที่ บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด ได้กำหนดให้ใช้งาน

(8) ห้ามเข้าถึงข้อมูลอีเมลของผู้อื่นโดยไม่ได้รับอนุญาต

(9) ห้ามลงทะเบียนด้วยอีเมลแอดเดรสของ บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด ไว้ตามที่อยู่เว็บไซต์ต่างๆ ที่ไม่มีความเกี่ยวข้องกับภารกิจงานของตนเอง

(10) ห้ามส่งอีเมลที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

(11) ห้ามส่งอีเมลที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

(12) ห้ามส่งอีเมลที่มีลักษณะเป็นการละเมิดต่อกฎหมาย ทรัพย์สินทางปัญญา หรือสิทธิของบุคคลอื่น

(13) ห้ามส่งอีเมลที่มีโปรแกรมไม่ประสงค์ดีไปให้กับผู้อื่นโดยเจตนา

(14) ห้ามปลอมแปลงหรือสวมรอยใช้อีเมลของผู้อื่น

(15) ห้ามรับหรือส่งอีเมลแทนผู้อื่นโดยไม่ได้รับอนุญาต

4.11 **ส่วนที่ 11 การใช้เครือข่ายสังคมออนไลน์** (Online Social Networking)

(1) พนักงานต้องไม่ใช้เครือข่ายสังคมออนไลน์ที่ก่อให้เกิดความเสียหายต่อบริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด ละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่น ผิดกฎหมาย ละเมิดศีลธรรม แสวงหาผลประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาประโยชน์ในเชิงธุรกิจ

(2) พนักงานต้องไม่สนทนาหรือส่งข้อมูลที่เป็นความลับของบริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด ผ่านเครือข่ายสังคมออนไลน์

(3) พนักงานต้องไม่ใช้อีเมลของบริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด ในการลงทะเบียนใช้งานเครือข่ายสังคมออนไลน์

4.12 **ส่วนที่ 12 การเผยแพร่ข้อมูลในเว็บไซต์** (Publish Information on Website)

(1) ตรวจสอบความถูกต้องและความเหมาะสมของข้อมูลก่อนนำขึ้นเผยแพร่ในเว็บไซต์ของบริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด

(2) ผู้บังคับบัญชาของผู้ที่รับผิดชอบ ตรวจสอบซ้ำอีกครั้งเพื่อความถูกต้องและความเหมาะสมของเนื้อหานั้นก่อนนำข้อมูลขึ้นเผยแพร่ในเว็บไซต์

(3) หลังจากนำข้อมูลขึ้นเผยแพร่แล้ว ให้เฝ้าระวังหน้าเว็บไซต์ดังกล่าวอย่างสม่ำเสมอ เพื่อดูว่ามีการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาตเกิดขึ้นหรือไม่

4.13 **ส่วนที่ 13 การรักษาและป้องกันความลับของข้อมูล** (Information Protection)

(1) พนักงานต้องไม่ละเมิดข้อมูลส่วนบุคคลของผู้อื่น

(2) พนักงานต้องไม่เข้าถึงข้อมูลของผู้อื่นรวมถึงข้อมูลทางธุรกิจโดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล

(3) พนักงานต้องไม่ทำการพิมพ์หรือคัดลอกข้อมูล ที่เป็นความลับของ บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด และผู้อื่น เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

(4) พนักงานต้องจัดชั้นความลับของข้อมูลอิเล็กทรอนิกส์และปฏิบัติตามเอกสาร *ISMS-PD-05-MIS_แนวปฏิบัติการจัดระดับชั้นความลับ การบ่งชี้และการจัดการกับสารสนเทศ* และต้องไม่เปิดเผยข้อมูลความลับ ต่อบุคคลที่ไม่เกี่ยวข้อง

(5) พนักงานจะต้องจัดเก็บเอกสารหรือข้อมูลที่เกี่ยวข้องกับงานของ บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด ในตู้หรือสถานที่จัดเก็บที่จัดเตรียมให้ เมื่อไม่มีความจำเป็นต้องใช้งาน

และต้องป้องกันไม่ให้เอกสารหรือข้อมูลถูกเปิดเผยอันเนื่องมาจากความประมาทในการจัดเก็บ

(6) พนักงานต้องทำการตรวจสอบและทบทวนสิทธิการใช้ข้อมูลอิเล็กทรอนิกส์ที่ใช้งานร่วมกันภายในเครือข่ายคอมพิวเตอร์ของ บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด

4.14 **ส่วนที่ 14 ความปลอดภัยด้านกายภาพและสภาพแวดล้อม** (Physical and Environment Security)

(1) ให้มีการรักษาความมั่นคงปลอดภัยพื้นที่ที่มีการประมวลผลข้อมูล โดยให้มีการควบคุมการเข้าออกอย่างเหมาะสม กำหนดให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงพื้นที่ได้ โดยให้ปฏิบัติตาม *ISMS-PD-19-MIS_ แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม*

(2) ให้มีการควบคุมพื้นที่หรือบริเวณสำหรับรับส่งของและตรวจสอบอุปกรณ์ ทั้งนี้จุดหรือบริเวณดังกล่าวควรแยกออกมาจากบริเวณที่มีอุปกรณ์ประมวลผลสารสนเทศ เพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต

(3) ให้มีการป้องกันอุปกรณ์จากการล้มเหลวของกระแสไฟฟ้าและการหยุดชะงักอื่น ๆ ที่มีสาเหตุมาจากการล้มเหลวของระบบและอุปกรณ์สนับสนุนการทำงานต่าง ๆ

(4) ให้มีจัดเก็บสายสัญญาณให้เป็นระเบียบเรียบร้อย เพื่อป้องกันความเสียหาย และจัดทำหรือปรับปรุง ป้ายกำกับ (Label) ของอุปกรณ์ และสายสัญญาณต่าง ๆ ในศูนย์คอมพิวเตอร์ให้ครบถ้วนและถูกต้อง

(5) ให้มีการตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูล เพื่อให้มั่นใจว่าข้อมูลสำคัญและซอฟต์แวร์ที่มีใบอนุญาตถูกยกเลิก ลบทิ้ง หรือเขียนทับอย่างมั่นคงปลอดภัย ก่อนการกำจัดอุปกรณ์หรือก่อนการนำอุปกรณ์ไปใช้งานใหม่

(6) ให้มีการลบข้อมูลหรือวิธีการจัดการอื่น ๆ อย่างมั่นคงปลอดภัย สำหรับสื่อบันทึกข้อมูลที่จัดเก็บข้อมูลสำคัญที่ไม่มีความจำเป็นในการใช้งาน

4.15 **ส่วนที่ 15 การเข้ารหัสข้อมูล** (Cryptography)

(1) ข้อมูลที่สำคัญของบริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด ต้องกำหนดให้มีมาตรการการเข้ารหัสข้อมูลตามมาตรฐานสากล หรือให้สอดคล้องกับข้อตกลง ระเบียบข้อบังคับและกฎหมายที่เกี่ยวข้อง

(2) บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด ต้องกำหนดวิธีการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัสลับข้อมูล โดยให้ครอบคลุมวงจรการบริหารจัดการกุญแจ (key Management Life Cycle) โดยให้ปฏิบัติตาม ISMS-PD-12-MIS_แนวปฏิบัติในการบริหารจัดการการเข้ารหัสลับข้อมูล

4.16 **ส่วนที่ 16 การป้องกันไวรัสคอมพิวเตอร์** (Malware Protection)

(1) พนักงานต้องไม่ปรับแต่งหรือยกเลิกการทำงานของโปรแกรมป้องกันไวรัสที่ติดตั้งใช้งานในเครื่องคอมพิวเตอร์พีซี/โน้ตบุ๊ค

(2) พนักงานต้องไม่ดาวน์โหลดข้อมูลหรือซอฟต์แวร์จากเว็บไซต์ที่ไม่เหมาะสม

(3) พนักงานมีหน้าที่ต้องติดตามข่าวสารที่เกี่ยวกับการเตือนภัยไวรัสและความปลอดภัยข้อมูลจากประชาสัมพันธ์ของบริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด

(4) ตรวจสอบโปรแกรมป้องกันไวรัสในเครื่องคอมพิวเตอร์ที่ใช้งานให้มีการทำงานตามปกติและมีการปรับปรุงฐานข้อมูลรูปแบบไวรัสอย่างสม่ำเสมอ หากพบว่าทำงานผิดปกติ ให้รีบแจ้งหน่วยงานผู้รับผิดชอบเพื่อดำเนินการแก้ไขโดยทันที

(5) ตรวจสอบข้อมูลในเครื่องคอมพิวเตอร์ที่ใช้งานด้วยโปรแกรมป้องกันไวรัส (ที่ติดตั้งในเครื่องนั้น) เพื่อกำจัดไวรัสอย่างน้อยสัปดาห์ละ 1 ครั้ง

4.17 **ส่วนที่ 17 การไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น** (Intellectual Property)

(1) ปฏิบัติตามเงื่อนไขการใช้งานหรือที่กำหนดไว้ของซอฟต์แวร์หรือทรัพย์สินทางปัญญาอื่นๆ ที่ บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด หรือผู้ใช้งานมีใช้งานหรือครอบครอง

(2) ห้ามทำซ้ำ เปลี่ยนแปลง หรือแก้ไขทรัพย์สินทางปัญญาไปสู่รูปแบบอื่นที่เป็นการละเมิดเงื่อนไขหรือข้อตกลงการใช้งาน

(3) ห้ามสำเนาทั้งหมดหรือบางส่วนของหนังสือ บทความ รายงาน หรือเอกสารอื่น ๆ ที่เป็นการละเมิดเงื่อนไขของเจ้าของทรัพย์สินทางปัญญา

4.18 **ส่วนที่ 18 การแลกเปลี่ยนสารสนเทศ** (Information Sharing)

(1) การแลกเปลี่ยนสารสนเทศระหว่างบริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด กับหน่วยงานภายนอกต้องดำเนินการการแลกเปลี่ยนข้อมูลด้วยวิธีการที่มีความมั่นคงปลอดภัยและสอดคล้องกับการจัดการระดับชั้นข้อมูลสารสนเทศ โดยให้ปฏิบัติตาม *ISMS-PD-05-MIS_แนวปฏิบัติการจัดระดับชั้นความลับ การบ่งชี้และการจัดการกับสารสนเทศ*

4.19 **ส่วนที่ 19 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย** (Information Security Reporting)

(1) เมื่อพบเหตุการณ์ด้านความมั่นคงปลอดภัย ให้รีบรายงานเหตุการณ์นั้นไปยังผู้ดำเนินการให้ความช่วยเหลือ โดยเร็วที่สุด

(2) ให้ความร่วมมือและประสานงานกับผู้ดำเนินการให้ความช่วยเหลือ ในการดำเนินการจัดการกับเหตุการณ์นั้น

4.20 **ส่วนที่ 20 การบริหารความต่อเนื่องของธุรกิจ** (Business Continuity Management)

(1) พนักงานต้องให้ความร่วมมือในการซ้อมแผนการดำเนินธุรกิจอย่างต่อเนื่อง ตามที่ระบุในเอกสาร *ISMS-PD-11-MIS_แนวปฏิบัติการบริหารจัดการความต่อเนื่องทางธุรกิจ* หรือแผนการอื่นที่เกี่ยวข้องกับการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

(2) ดำเนินการซ้อมแผนการดำเนินธุรกิจอย่างต่อเนื่องอย่างน้อยปีละ 1 ครั้ง

4.21 **ส่วนที่ 21 การรับมือเหตุการณ์ผิดปกติทางไซเบอร์** (Cyber Security Management)

(1) ต้องมีมาตรการในการเตรียมความพร้อมสำหรับเหตุการณ์ด้านความปลอดภัยไซเบอร์ (Preparing for a Cyber Security Incident)

(2) ต้องมีมาตรการในการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ (Responding to Cyber Security Incident)

(3) ต้องมีการติดตามสถานการณ์ด้านความปลอดภัยทางไซเบอร์ (Following up the Cyber Security Incident)

4.22 **ส่วนที่ 22 การใช้บริการ Cloud Computing อย่างปลอดภัย (Cloud Computing Security)**

(1) ต้องกำหนดกลยุทธ์และนโยบายการใช้บริการ Cloud Computing สำหรับผู้ให้บริการภายนอก

(2) ต้องมีแนวทางในการบริหารความเสี่ยงที่เกี่ยวข้องกับการใช้บริการ Cloud Computing

(3) ต้องมีการบริหารจัดการผู้ให้บริการ Cloud Computing จากภายนอก

(4) ต้องมีการรักษาความปลอดภัยและความลับของระบบงานและข้อมูลของการใช้บริการ Cloud Computing

(5) ต้องมีการดำเนินการเพื่อให้มั่นใจว่าระบบงานและข้อมูลของการใช้ระบริการ Cloud Computing มีความถูกต้องเชื่อถือได้

(6) ต้องมีการดำเนินการเพื่อให้มั่นใจถึงความพร้อมใช้ของการใช้บริการ Cloud Computing

(7) ต้องมีการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่ครอบคลุมถึงผู้ใช้บริการของบริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด

4.23 **ส่วนที่ 23 การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศในการบริหารจัดการโครงการ (Information Security Project Management)**

(1) ผู้บริหารระดับฝ่ายต้องกำหนดให้มีการควบคุมความเสี่ยง การติดตามการดำเนินงานโครงการ รวมถึงการประเมินภาพรวมในการดำเนินงานโครงการ ทั้งโครงการที่เป็นโครงการภายในและโครงการที่จัดซื้อจัดจ้างจากหน่วยงานภายนอก

(2) เจ้าของโครงการควรกำหนดข้อตกลงและความต้องการด้านความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องกับนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงกฎระเบียบ หรือข้อบังคับต่างๆ ที่เกี่ยวข้องของบริษัทฯ ไว้ในข้อตกลงหรือสัญญาของโครงการ

(3) เจ้าของโครงการควรกำหนดบทลงโทษเมื่อผู้ดำเนินงานไม่ปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงกฎระเบียบ หรือข้อบังคับต่างๆ ที่เกี่ยวข้อง

4.24 **ส่วนที่ 24 การควบคุมการเข้าถึง** (Access Control)

(1) บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัดต้องกำหนดวิธีการบริหารจัดการการลงทะเบียนและถอดถอนสิทธิผู้ใช้งานอย่างเป็นลายลักษณ์อักษรและปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัทรับทราบและปฏิบัติตาม

(2) บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด และเจ้าของข้อมูล ต้องกำหนดให้มีการมอบหมายหรือกำหนดสิทธิ์การใช้งานให้แก่ผู้ใช้งานในการเข้าถึงข้อมูลหรือระบบสารสนเทศตามหน้าที่ความรับผิดชอบ

(3) บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด ต้องมีการบริหารจัดการรหัสผู้ใช้งานที่มีสิทธิ์ระดับสูง

(4) บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด ต้องกำหนดวิธีการบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้

4.25 **ส่วนที่ 25 ความมั่นคงปลอดภัยสารสนเทศด้านการสื่อสาร** (Communication Security)

(1) ผู้ดูแลระบบ ต้องควบคุม กำกับให้มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์เพื่อป้องกันภัยคุกคาม และมีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและแอพพลิเคชั่นที่ทำงานบนเครือข่ายคอมพิวเตอร์ รวมทั้งข้อมูลสารสนเทศที่มีการแลกเปลี่ยนบนเครือข่าย

(2) ผู้ดูแลระบบ ต้องควบคุมให้มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับของการให้บริการ และความต้องการด้านการบริหารจัดการของการให้บริการเครือข่ายทั้งหมด ลงในข้อตกลงหรือสัญญาการให้บริการด้านเครือข่ายต่างๆ ทั้งที่เป็นการให้บริการจากภายในหรือภายนอก

(3) บริษัท เอเพ็กซ์ เซอร์คิต (ไทยแลนด์) จำกัด ต้องจัดให้มีการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยต้องพิจารณาถึงความต้องการของผู้ใช้งานในการเข้าถึงระบบเครือข่าย ผลกระทบทางด้านความมั่นคงปลอดภัยสารสนเทศ และระดับความสำคัญของข้อมูลที่อยู่บนเครือข่ายนั้น

4.26 **ส่วนที่ 26 การบริหารจัดการความเสี่ยง** (Risk Management)

(1) บริษัทดำเนินการบริหารจัดการและแสวงหาโอกาส ภายใต้ระดับความเสี่ยงที่ยอมรับได้ เพื่อให้บรรลุวัตถุประสงค์ในการดำเนินงานและวัตถุประสงค์ของบริษัท

(2) กำหนดกลยุทธ์ของบริษัทให้สอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ซึ่งกำหนดโดยผู้บริหารระดับสูง

(3) กำหนดให้มีการติดตามการบริหารจัดการความเสี่ยง เพื่อให้มั่นใจว่าความเสี่ยงของบริษัทมีการจัดการที่เหมาะสมอย่างต่อเนื่อง โดยกรอบการบริหารจัดการความเสี่ยงให้อ้างอิงเอกสาร ISMS-PD-03-MIS_แนวปฏิบัติการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

4.27 **ส่วนที่ 27 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ** (System Acquisition, Development and Maintenance)

(1) ผู้ดูแลระบบและผู้พัฒนาระบบ ต้องจัดทำขั้นตอนการปฏิบัติงานสำหรับการควบคุมการบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ หรือระบบงาน ทั้งนี้ ขั้นตอนการปฏิบัติงานควรประกอบด้วย

- การประเมินผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง
- เงื่อนไขการขออนุมัติขอแก้ไขหรือพัฒนาระบบสารสนเทศ หรือระบบงาน
- ขั้นตอนปฏิบัติงานในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบกรณีฉุกเฉิน และบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจอนุมัติของแผนกงานทุกครั้ง
- การจัดทำแผนการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ หรือระบบงาน
- การจัดเก็บโปรแกรม Version ก่อนการเปลี่ยนแปลงไว้ใช้งาน หรือมีกระบวนการถอยกลับสู่สภาพเดิม (Fall-Back) ของระบบงาน ในกรณีระบบงานผิดพลาดหรือไม่สามารถใช้งานได้
- การทดสอบการเปลี่ยนแปลงระบบสารสนเทศ หรือระบบงาน
- การสื่อสารให้กับบุคคลที่เกี่ยวข้องได้รับทราบและสามารถปฏิบัติงานได้อย่างถูกต้อง

(2) ผู้ดูและระบบ ต้องตรวจติดตามการใช้งานระบบสารสนเทศที่มีการใช้งานภายหลังการเปลี่ยนแปลง เพื่อตรวจสอบว่าการเปลี่ยนแปลงไม่มีผลกระทบต่อการทำงานของระบบและไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยระบบสารสนเทศ

(3) ผู้ดูแลระบบ ต้องควบคุมการติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการจริง โดยให้ดำเนินการตามขั้นตอนการปฏิบัติงานสำหรับการควบคุมการบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศที่กำหนดไว้

(4) ผู้ดูแลระบบและผู้พัฒนาระบบ ต้องให้มีการจำกัดการเปลี่ยนแปลงใดๆ ต่อซอฟต์แวร์ที่ใช้งาน (Software Package) โดยให้เปลี่ยนแปลงเฉพาะเท่าที่จำเป็น และควบคุมทุกๆ การเปลี่ยนแปลงอย่างเข้มงวด

(5) ผู้ดูแลระบบและผู้พัฒนาระบบ ต้องควบคุมให้มีการจัดทำข้อกำหนดขั้นต่ำของการพัฒนาระบบสารสนเทศ และข้อกำหนดการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศของระบบสารสนเทศใหม่ หรือการปรับปรุงระบบสารสนเทศเดิม ลงในข้อตกลงหรือสัญญา ทั้งโครงการที่เป็นโครงการภายในและโครงการที่จัดซื้อจัดจ้างหน่วยงานภายนอกเป็นผู้ดำเนินการ

(6) ผู้ดูแลระบบและผู้พัฒนาระบบ ต้องควบคุมให้มีการตรวจสอบข้อมูลใดๆ ที่จะรับเข้าสู่แอพพลิเคชั่นก่อนเสมอ เพื่อให้มั่นใจได้ว่าข้อมูลมีความถูกต้องและมีรูปแบบเหมาะสม

(7) ผู้ดูแลระบบและผู้พัฒนาระบบ ต้องควบคุมให้มีการตรวจสอบการทำงานของแอพพลิเคชั่นเพื่อตรวจหาข้อผิดพลาดของข้อมูลที่อาจเกิดจากการทำงานหรือการประมวลผลที่ผิดพลาด

(8) ผู้ดูแลระบบและผู้พัฒนาระบบ ต้องควบคุมให้มีข้อกำหนดขั้นต่ำสำหรับการรักษาความน่าเชื่อถือ (Authenticity) และความถูกต้องครบถ้วน (Integrity) ของข้อมูลในแอพพลิเคชั่น รวมทั้งมีการระบุและปฏิบัติตามวิธีการป้องกันที่เหมาะสม

(9) ผู้ดูแลระบบและผู้พัฒนาระบบ ต้องควบคุมให้มีการตรวจสอบข้อมูลใดๆ อันเป็นผลจากการประมวลผลของแอพพลิเคชั่น เพื่อให้มั่นใจได้ว่า ข้อมูลที่ได้จากการประมวลผลถูกต้องและเหมาะสม

(10) ผู้ดูแลระบบและผู้พัฒนาระบบ ต้องกำหนดให้มีการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับ ดังนี้

- จัดประเภทของข้อมูลและการสื่อสารที่จะต้องได้รับการเข้ารหัสลับ เช่น รหัสผ่าน เป็นต้น
- ผู้ดูแลระบบ ต้องกำหนดให้มีการใช้โปรแกรมที่มีความสามารถในการเข้ารหัสข้อมูล เพื่อให้บุคลากรใช้เป็นมาตรฐานเดียวกัน โดยโปรแกรมจะต้องทำหน้าที่ในการเข้ารหัสลับข้อมูลอย่างเหมาะสม เมื่อมีการเชื่อมต่อผ่านระบบเครือข่ายภายในบริษัทไปยังเครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์เครือข่ายต่างๆ ของบริษัท
- ผู้ดูแลระบบ ต้องกำหนดให้มีการใช้โปรแกรมที่มีความสามารถในการเข้ารหัสข้อมูล เพื่อให้บุคลากรใช้เป็นมาตรฐานเดียวกัน โดยโปรแกรมจะต้องทำหน้าที่ในการเข้ารหัสข้อมูลอย่างเหมาะสม เมื่อมีการเชื่อมต่อจากเครือข่ายภายนอกบริษัทเข้ามายังเครือข่ายภายในบริษัท

(11) ผู้ดูแลระบบ ต้องกำหนดให้มีแนวทางการบริหารจัดการกุญแจที่ใช้เข้ารหัสข้อมูล เพื่อรองรับการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับ โดยให้มีการควบคุม กำกับ ติดตาม ให้ครอบคลุมตลอดทั้งวงจรในการนำกุญแจรหัสลับไปใช้งาน

(12) ผู้ดูแลระบบและผู้พัฒนาระบบ ต้องจำกัดการเข้าถึงซอร์สโค้ด (Source Code) ของระบบงาน

(13) ผู้ดูแลระบบและผู้พัฒนาระบบ ต้องควบคุมให้มีการตรวจสอบทบทวนการทำงานของโปรแกรมที่มีความสำคัญในกรณีที่มีการเปลี่ยนแปลงใดๆ เกิดขึ้นในระบบปฏิบัติการคอมพิวเตอร์ และต้องควบคุมให้มีการทดสอบการใช้งานเพื่อให้มั่นใจว่าผลของการเปลี่ยนแปลงดังกล่าว จะไม่ส่งผลกระทบใดๆ ต่อความมั่นคงปลอดภัยของระบบสารสนเทศและการให้บริการระบบสารสนเทศ

(14) ผู้ดูแลระบบต้องตรวจสอบข้อมูลที่เกี่ยวข้องกับช่องโหว่ด้านเทคนิคอย่างสม่ำเสมอ เพื่อให้ทราบถึงภัยคุกคามและความเสี่ยง รวมถึงหาวิธีป้องกันและแก้ไขที่เหมาะสมกับช่องโหว่นั้น

(15) ผู้ดูแลระบบและผู้พัฒนาระบบ ต้องยึดหลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure System Engineering Principles) เข้ามาประยุกต์ใช้ในการพัฒนาระบบ

(16) ผู้ดูแลระบบและผู้พัฒนาระบบ ต้องมีการควบคุมสภาพแวดล้อมของการพัฒนาและบูรณาการระบบให้มีความมั่นคงปลอดภัย โดยต้องป้องกันข้อมูลของระบบที่เกิดขึ้นในระหว่างการพัฒนา การรับส่งข้อมูล การสำรองข้อมูล และการควบคุมการเข้าถึงระบบ

(17) ผู้ดูแลระบบและผู้พัฒนาระบบ ต้องมีการทดสอบฟังก์ชันการทำงานด้านความมั่นคงปลอดภัยสารสนเทศในระบบที่ได้รับการพัฒนาขึ้นใหม่ หรือทุกครั้งที่มีการเปลี่ยนแปลง โดยการทดสอบควรประกอบไปด้วย

- การทดสอบย่อย (Unit Testing)
- การทดสอบการทำงานร่วมกับระบบอื่น (Integration Testing)
- การทดสอบการเชื่อมต่อหรือติดต่อสื่อสารกันระหว่างซอฟต์แวร์ หรือระบบอื่น ๆ (System Testing)
- การทดสอบเพื่อรับรองความถูกต้องโดยผู้ใช้ (User Acceptance Test: UAT)

(18) กรณีที่มีการจ้างหน่วยงานภายนอกเข้ามาพัฒนาระบบ ผู้ดูแลระบบและผู้พัฒนาระบบต้องควบคุมโครงการพัฒนาซอฟต์แวร์ที่พัฒนาโดยหน่วยงานภายนอกดังนี้

- กำกับดูแล ควบคุม ติดตามตรวจสอบการทำงานของหน่วยงานภายนอก รวมถึงการจ้างช่วงพัฒนาระบบให้ดำเนินงานตามกฎระเบียบของบริษัทอย่างสม่ำเสมอ
- กำหนดความเป็นเจ้าของทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดที่ใช้ในการพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอกไว้ในสัญญาจ้าง
- กำหนดให้มีการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่มีการพัฒนาโดยหน่วยงานภายนอกไว้ในสัญญาจ้าง
- กำหนดให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดีในระบบงาน หรือซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

(19) หลังจากที่หน่วยงานภายนอกส่งมอบการพัฒนาซอฟต์แวร์เรียบร้อยแล้ว ผู้ดูแลระบบและผู้พัฒนาระบบต้องดำเนินการเปลี่ยนรหัสผ่านตั้งต้นทั้งหมดที่ได้รับมอบทันที

4.28 **การนำเครื่องคอมพิวเตอร์ที่บริษัทจัดสรรให้ออกนอกพื้นที่** (Taking Computers allocated by the Company out of the Area)

กรณีที่พนักงานนำเครื่องคอมพิวเตอร์ที่บริษัทจัดสรรให้ และนำกลับไปใช้งานที่บ้าน ต้องปฏิบัติตามคำแนะนำ ดังนี้

(1) พนักงานต้องดูแลรักษาเครื่องคอมพิวเตอร์ที่บริษัทจัดสรรให้เสมือนเป็นทรัพย์สินของตนเอง

(2) พนักงานต้องไม่จัดวางเครื่องคอมพิวเตอร์ที่บริษัทจัดสรรให้ไว้ในพื้นที่ที่ไม่ปลอดภัย เช่น ในรถที่สามารถมองเห็นทรัพย์สินได้

(3) พนักงานต้องไม่นำเครื่องคอมพิวเตอร์ของบริษัทไปให้ผู้อื่นใช้งาน

5. เอกสารที่เกี่ยวข้อง

- ISMS-PD-03-MIS_แนวปฏิบัติการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
- ISMS-PD-04-MIS_แนวปฏิบัติการควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ
- ISMS-PD-05-MIS_แนวปฏิบัติการจัดระดับชั้นความลับ การบ่งชี้และการจัดการกับสารสนเทศ
- ISMS-PD-06-MIS_แนวปฏิบัติการสำรองและทดสอบกู้คืนข้อมูล
- ISMS-PD-11-MIS_แนวปฏิบัติการบริหารจัดการความต่อเนื่องทางธุรกิจ
- ISMS-PD-12-MIS_แนวปฏิบัติในการบริหารจัดการการเข้ารหัสลับข้อมูล
- ISMS-PD-14-MIS_แนวปฏิบัติในการเข้าถึงจากระยะไกล
- ISMS-PD-15-MIS _แนวปฏิบัติในการติดตั้งซอฟต์แวร์บนระบบงาน
- ISMS-PD-19-MIS_ แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

6. เอกสารสำหรับบันทึก

-