นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

บริษัท ไอร่า แฟคตอริ่ง จำกัด (มหาชน)

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ได้รับการอนุมัติทบทวนจากที่ประชุมคณะกรรมการบริหาร ครั้งที่ 9/2567 เมื่อวันที่ 26 กันยายน 2567

AIRA FACTORING PUBLIC COMPANY LIMITED
AIRA Factoring Public Company Limited
บริษัท ไอร่า แฟคตอริ่ง จำกัด (มหาชน)
เลขที่บมจ. 0107547000141
188 Spring Tower Building, Floor 12A, Unit 6-10 Phaya Thai Road, Thung Phaya Thai subdistrict Ratchathewi District Bangkok 10400
188 อาคารสปริงทาวเวอร์ ชั้น 12A ยูนิตที่ 6-10 ถนนพญาไท แขวงทุ่งพญาไท
เขตราชเทวี กรุงเทพมหานคร 10400 Tel. 0-2657-6222, Fax: 0-2657-6244, 0-2657-6245

คำนำ

เพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัท ไอร่า แฟคตอริ่ง จำกัด (มหาชน) หรือต่อไปนี้เรียกว่า "บริษัท" เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ บริษัทจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ(Guideline) ขั้นตอนปฏิบัติ(Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

1.1 การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือเครือข่ายคอมพิวเตอร์ของบริษัท ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

1.2 กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร อ้างอิงตามมาตรฐาน ISO/IEC 27001 และมีการปรับปรุงอย่างต่อเนื่อง

1.3 นโยบายนี้จะต้องทำการเผยแพร่ให้พนักงานทุกระดับในบริษัทได้รับทราบและพนักงานทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

1.4 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร พนักงาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัท ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

1.5 นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลาปีละ 1 ครั้ง

AIRA FACTORING PUBLIC COMPANY LIMITED
AIRA Factoring Public Company Limited
บริษัท ไอร่า แฟคตอริ่ง จำกัด (มหาชน)
เลขที่บมจ. 0107547000141
188 Spring Tower Building, Floor 12A, Unit 6-10 Phaya Thai Road, Thung Phaya Thai subdistrict Ratchathewi District Bangkok 10400
188 อาคารสปริงทาวเวอร์ ชั้น 12A ยูนิตที่ 6-10 ถนนพญาไท แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพมหานคร 10400 Tel. 0-2657-6222, Fax: 0-2657-6244, 0-2657-6245

สารบัญ

เรื่อง หน้า

สารบัญ

สารบัญ

เรื่อง หน้า

AIRA FACTORING PUBLIC COMPANY LIMITED
AIRA Factoring Public Company Limited
บริษัท ไอร่า แฟคตอริ่ง จำกัด (มหาชน)
เลขที่บมจ. 0107547000141
188 Spring Tower Building, Floor 12A, Unit 6-10 Phaya Thai Road, Thung Phaya Thai subdistrict Ratchathewi District Bangkok 10400
188 อาคารสปริงทาวเวอร์ ชั้น 12A ยูนิตที่ 6-10 ถนนพญาไท แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพมหานคร 10400 Tel. 0-2657-6222, Fax: 0-2657-6244, 0-2657-6245

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ฝ่ายสารสนเทศ สายงานปฏิบัติการและสารสนเทศ บริษัท ไอร่า แฟคตอริ่ง จำกัด (มหาชน)

1. วัตถุประสงค์

1.1. เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศของบริษัทดำเนินงานเป็นไปได้อย่างมีประสิทธิภาพและประสิทธิผล

1.2. เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้มีการปรับปรุงอย่างต่อเนื่อง

1.3. เพื่อเผยแพร่นโยบายและแนวปฏิบัตินี้ให้กับพนักงานทุกระดับได้รับทราบ และถือปฏิบัติตามอย่างเคร่งครัด

1.4. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ หรือ การจัดการทางด้านเทคโนโลยีสารสนเทศและการสื่อสาร และให้ผู้ที่เกี่ยวข้อง ทั้งผู้บริหาร พนักงาน ผู้ดูแลระบบ และบุคคลภายนอกที่เข้ามาปฏิบัติงานตระหนักและถือปฏิบัติตามอย่างเคร่งครัด

1.5. เพื่อให้มีการดำเนินการตรวจสอบและประเมินความเสี่ยง ในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศและการสื่อสาร อย่างสม่ำเสมอ

1.6. เพื่อส่งเสริมให้พนักงานมีความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทนี้จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท ซึ่งพนักงานและหน่วยงานภายนอกจะ **ต้องถือปฏิบัติตามอย่างเคร่งครัด**

2. องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

หมวดที่ 1 นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร
หมวดที่ 2 โครงสร้างด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร
หมวดที่ 3 การบริหารจัดการทรัพย์สินของบริษัท
หมวดที่ 4 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร
หมวดที่ 5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
หมวดที่ 6 การเข้ารหัสข้อมูล
หมวดที่ 7 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของบริษัท
หมวดที่ 8 การควบคุมการเข้าถึง
หมวดที่ 9 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ
หมวดที่ 10 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท
หมวดที่ 11 การบริหารความต่อเนื่องในการดำเนินงานของบริษัท
หมวดที่ 12 การปฏิบัติตามข้อกำหนด

3. ความหมายและคำจำกัดความ

- "**สินทรัพย์คอมพิวเตอร์**" หมายความว่า สินทรัพย์ทุกอย่างที่เกี่ยวข้องกับการใช้ระบบคอมพิวเตอร์ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล เป็นต้น
- "**ระบบเครือข่าย**" หมายความว่า ระบบเครือข่ายคอมพิวเตอร์ของบริษัท
- "**คอมพิวเตอร์แม่ข่าย**" หมายความว่า เครื่องคอมพิวเตอร์ในระบบเครือข่ายที่ทำหน้าที่เป็น ศูนย์กลางของการทำงาน อาทิ จัดเก็บข้อมูลหรือซอฟต์แวร์สำหรับให้บริการแก่เครื่องคอมพิวเตอร์ อื่น ๆ หรือควบคุมการทำงานในเครือข่าย
- "**การเข้าถึงเครือข่ายจากระยะไกล**" หมายความว่า การที่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายเชื่อมต่อเข้ากับเครื่องคอมพิวเตอร์หรือเครือข่ายอื่นผ่านอุปกรณ์สื่อสารหรือสื่อสัญญาณอื่น ๆ อาทิ VPN
- "**การควบคุมการเข้าถึง**" หมายความว่า การควบคุมการเข้าถึงหรือใช้งานสินทรัพย์คอมพิวเตอร์ให้เป็นไปตามสิทธิที่กำหนดไว้เท่านั้น
- "**เครื่องคอมพิวเตอร์**" หมายความว่า อุปกรณ์ที่ใช้ในการประมวลผลข้อมูลที่ทำงาน ด้วยระบบอิเล็กทรอนิกส์ โดยทำงานตามคำสั่งผ่านทางซอฟต์แวร์ให้ได้ผลตามที่ต้องการ อาทิ คอมพิวเตอร์แม่ข่าย (Server) คอมพิวเตอร์ส่วนบุคคล (Personal Computer) และคอมพิวเตอร์แบบพกพาได้ (Notebook Computer)
- "**อุปกรณ์คอมพิวเตอร์**" หมายความว่า อุปกรณ์อิเล็กทรอนิกส์ที่ใช้งานร่วมกับเครื่องคอมพิวเตอร์เพื่อสนับสนุนให้เครื่องคอมพิวเตอร์ปฏิบัติงานได้ตามต้องการ และให้รวมถึงเครื่องคอมพิวเตอร์
- "**สื่อสัญญาณ**" หมายความว่า สื่อกลางใด ๆ ที่ใช้เชื่อมต่อระหว่างอุปกรณ์คอมพิวเตอร์ อาทิสายทองแดง สายใยแก้วนำแสง เครือข่ายไร้สาย

- "**ฮาร์ดแวร์**" หมายความว่า อุปกรณ์คอมพิวเตอร์
- "**ซอฟต์แวร์**" หมายความว่า ชุดคำสั่งที่สั่งให้คอมพิวเตอร์ทำงานตามต้องการ
- "**ซอฟต์แวร์ระบบ**" หมายความว่า ซอฟต์แวร์ที่ควบคุมการทำงานของอุปกรณ์คอมพิวเตอร์ เช่น ระบบปฏิบัติการ เป็นต้น
- "**ซอฟต์แวร์ประยุกต์**" หมายความว่า ซอฟต์แวร์ที่พัฒนาขึ้นเพื่อใช้กับงานเฉพาะด้านตามความต้องการ อาทิ ซอฟต์แวร์สำหรับพิมพ์เอกสาร ซอฟต์แวร์สำหรับการคำนวณทางบัญชี
- "**ระบบเทคโนโลยีสารสนเทศ**" หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ อาทิ อุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ระบบงาน และสารสนเทศ
- "**สารสนเทศ**" หมายความว่า ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ ได้
- "**ระบบงาน**" หมายความว่า การนำระบบเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการทำงานเพื่อให้งานสำเร็จตามวัตถุประสงค์ที่ตั้งไว้ อาทิ ระบบจัดเก็บเอกสาร ระบบจองยานพาหนะ
- "**ระบบปฏิบัติการ**" (Operating System) หมายความว่า ซอฟต์แวร์ควบคุมการทำงานของเครื่องคอมพิวเตอร์ และจัดสรรการใช้ทรัพยากรระบบ ซึ่งได้แก่ การจัดการหน่วยความจำ การควบคุม การทำงานของอุปกรณ์ป้อนข้อมูล (แป้นพิมพ์ เมาส์) และอุปกรณ์แสดงผล (จอภาพ เครื่องพิมพ์)
- "**ระบบป้องกันการบุกรุก**" (Firewall) หมายความว่า ระบบรักษาความปลอดภัยที่ประกอบด้วยกลุ่มอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ ซึ่งทำหน้าที่ป้องกันผู้ไม่ได้รับอนุญาตจากเครือข่ายภายนอกเข้าใช้ระบบ และจำกัดการใช้งานของผู้ใช้งานภายในให้เป็นไปตามนโยบายที่บริษัทกำหนด
- "**ข้อมูลสารสนเทศ**" หมายความว่า ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลได้ด้วยวิธีการทางอิเล็กทรอนิกส์บนอุปกรณ์คอมพิวเตอร์ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์
- "**ข้อมูลสำคัญ**" หรือ "**ข้อมูลที่เป็นความลับ** (Sensitive Information)" หมายถึง ข้อมูลสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจของบริษัท หรือที่บริษัท มีพันธะผูกพันตามข้อกำหนดของกฎหมาย จรรยาบรรณในการประกอบธุรกิจ หรือสัญญาซึ่งบริษัท ไม่อาจนำ ไปเปิดเผยต่อบุคคลอื่น หรือนำไปใช้ประโยชน์อย่างอื่น นอกเหนือจากวัตถุประสงค์ในการดำเนินธุรกิจของบริษัท การรั่วไหลของข้อมูลสำคัญ หรือข้อมูลที่เป็นความลับดังกล่าวอาจเป็นเหตุให้การดำเนินธุรกิจของบริษัท ต้องหยุดชะงัก ขาดประสิทธิภาพ หรือบริษัทเสื่อมเสียชื่อเสียง
- "**ไฟล์**" (File) หมายความว่า ข้อมูลที่ถูกรวบรวมลงสื่อบันทึกและระบุเป็นหนึ่งหน่วยโดยมี ชื่อเฉพาะ เช่น ซอฟต์แวร์ใช้งาน และไฟล์เอกสารต่าง ๆ ที่สร้างขึ้นและใส่ชื่อให้แก่ไฟล์นั้นแล้วเก็บบันทึกลง สื่อบันทึก เป็นต้น
- "**บริษัท**" หมายความว่า บริษัท ไอร่า แฟคตอริ่ง จำกัด (มหาชน)

- "**ผู้บังคับบัญชา**" หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของบริษัท
- "**ผู้อำนวยการฝ่ายสารสนเทศ**" หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท ซึ่งบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐาน การควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- "**ผู้ใช้งาน**" (User) หมายความว่า เจ้าหน้าที่ของกลุ่มบริษัทในเครือ บริษัท ไอร่า แฟคตอริ่ง จำกัด (มหาชน) หรือบุคคลภายนอกที่มีสิทธิใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท
- "**ผู้บริหารเครือข่าย**" (Network Administrator) หมายความว่า บุคคลที่ทำหน้าที่รับผิดชอบในการดูแลและบำรุงรักษาเครือข่าย
- "**ผู้บริหารคอมพิวเตอร์แม่ข่าย**" (Host/Server Administrator) หมายความว่า บุคคลที่ ทำหน้าที่รับผิดชอบในการดูแลและบำรุงรักษาคอมพิวเตอร์แม่ข่าย
- "**ผู้บริหารระบบป้องกันการบุกรุก**" (Firewall Administrator) หมายความว่า บุคคลที่ ทำหน้าที่รับผิดชอบในการดูแลและบำรุงรักษาระบบป้องกันการบุกรุก
- "**บัญชีผู้ใช้งาน**" (User Account) หมายความว่า บัญชีที่ผู้ใช้งานใช้ในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นไปตามข้อตกลงระหว่างผู้ใช้งานกับผู้ให้บริการระบบเทคโนโลยีสารสนเทศ
- "**บัญชีผู้บริหารคอมพิวเตอร์แม่ข่าย**" (Administrator Account) หมายความว่า บัญชีที่ผู้บริหารคอมพิวเตอร์แม่ข่ายใช้ในการบริหารระบบคอมพิวเตอร์แม่ข่าย
- "**เอกสารโครงแบบ**" (Configuration Document) หมายความว่า เอกสารที่แสดงรายละเอียดการกำหนดค่าต่าง ๆ ในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศใช้งานได้ตามความต้องการ
- "**ความเสี่ยง**" หมายความว่า โอกาสของสินทรัพย์คอมพิวเตอร์ในการถูกละเมิดการรักษาความปลอดภัย
- "**เหตุการณ์ผิดปกติ**" (Incident) หมายความว่า เหตุการณ์ใด ๆ ที่มีผลกระทบต่อการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ
- "**เจ้าหน้าที่**" หมายความว่า พนักงานประจำ พนักงานตามสัญญาจ้าง พนักงานชั่วคราว และให้หมายความรวมถึง เจ้าหน้าที่ของบริษัทที่ให้บริการภายนอกด้านเทคโนโลยีให้กับบริษัท
- "**ส่วนงาน**" หมายความ ฝ่าย/ส่วนงาน ที่เป็นไปตามโครงสร้างบริษัทของบริษัท
- "**ส่วนงานเจ้าของข้อมูล**" หมายความว่า เจ้าหน้าที่ในส่วนงานตั้งแต่ 1 คนขึ้นไปที่ได้รับมอบหมายจากส่วนงานให้เป็นผู้รับผิดชอบข้อมูล
- "**โปรแกรมประสงค์ร้าย**" หมายความว่า ฮาร์ดแวร์หรือซอฟต์แวร์ที่มีการตั้งใจใส่เข้าไปในระบบโดยไม่ได้รับอนุญาต เพื่อให้ทำงานตามความประสงค์ของผู้ประสงค์ร้าย ซึ่งมีผลให้คอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศ หรือชุดคำสั่งอื่นได้รับความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
- "**พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร**" (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

- พื้นที่ทำงานทั่วไป (General Working Area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน
- พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area)
- พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area)
- พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area)
- พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless Lan Coverage Area)

- "**จดหมายอิเล็กทรอนิกส์**"หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP3 และ IMAP เป็นต้น
- "**รหัสผ่าน**"หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
- "**ชุดคำสั่งไม่พึงประสงค์**" หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
- "**บุคคลภายนอก**" หมายถึง บุคลากรหรือหน่วยงานภายนอกที่ดำเนินธุรกิจหรือให้บริการที่อาจได้รับสิทธิเข้าถึงสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศของบริษัทฯ เช่น
  - บริษัทคู่ค้า (Business Partner)
  - ผู้รับจ้างปฏิบัติงานให้กับบริษัทฯ (Outsource)
  - ผู้รับจ้างพัฒนาระบบหรือจัดหาวัสดุอุปกรณ์ต่าง ๆ (Supplier)
  - ผู้ให้บริการต่าง ๆ (Service Provider)
  - ที่ปรึกษา (Consultant)

หมวด 1

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Security Policy)

จุดประสงค์เพื่อการจัดให้มีนโยบายรักษาความปลอดภัยด้านสารสนเทศ เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางกฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง เมื่อประกาศฉบับนี้มีผลบังคับใช้ โดยมีวัตถุประสงค์เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่และความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่าง ๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำนโยบาย รายละเอียดของนโยบาย และการปฏิบัติตามนโยบาย

- ให้ฝ่ายสารสนเทศ เป็นผู้ทำหน้าที่ในการออกระเบียบปฏิบัติ ข้อกำหนด ข้อบังคับต่าง ๆ ที่จำเป็นเพื่อให้การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ของบริษัท และนำเสนอขอความเห็นชอบจากผู้บริหารระดับสูงของบริษัท
- ผู้บริหารระดับสูงของบริษัท จะต้องให้การสนับสนุนในเรื่องนโยบาย งบประมาณ ทรัพยากรและอื่น ๆ ที่จำเป็นเพื่อให้การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์มีการพัฒนาและปรับปรุงอย่างต่อเนื่อง
- ต้องจัดให้มีการเผยแพร่นโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ให้กับพนักงาน เจ้าหน้าที่ ผู้ให้บริการภายนอก และผู้ที่เกี่ยวข้องรับทราบและนำไปปฏิบัติ
- ต้องมีการดำเนินการทบทวน และประเมินนโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์อย่างน้อย 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญซึ่งมีผลต่อการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของบริษัท

หมวด 2

โครงสร้างด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร
(Organization of Information Security)

2.1 **โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศภายในบริษัท** (Internal Organization)

จุดประสงค์เพื่อบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ของบริษัท

- ผู้บริหารระดับสูงของบริษัทเป็นผู้กำหนดให้มีตัวแทนหรือคณะทำงานจากหน่วยงานต่าง ๆ ภายในบริษัท เพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของบริษัท
- ตัวแทนหรือคณะทำงานเหล่านั้นจะต้องมีการกำหนดหน้าที่ความรับผิดชอบในการดำเนินงานทางด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของบริษัทอย่างชัดเจน

- ตัวแทนหรือคณะทำงานซึ่งถูกแต่งตั้งโดยผู้บริหารระดับสูงของบริษัทเป็นผู้รับผิดชอบในการบริหารจัดการและควบคุมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ของบริษัท ตลอดจนทบทวนนโยบายระบบบริหารการรักษาความมั่นคงปลอดภัยสารสนเทศ
- ตัวแทนหรือคณะทำงานต้องจัดทำขั้นตอน และแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ต่าง ๆ และเอกสารที่เกี่ยวข้องในการจัดทำการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์
- พนักงานของบริษัทต้องไม่เปิดเผยความลับของบริษัท เว้นแต่จะได้รับการอนุญาตให้เปิดเผยจากบริษัท
- ต้องกำหนดรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่น ๆ เช่น ตลาดหลักทรัพย์ เป็นต้น ต้องจัดให้มีการทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระ(Independent Review of Information Security)
- ต้องกำหนดรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่น
- ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการการดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์โดยผู้ตรวจสอบอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญมากต่อบริษัท

2.2 โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External Parties)

จุดประสงค์เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของบริษัทที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก

- ต้องกำหนดให้มีการประเมินความเสี่ยงอันเกิดจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้สามารถเข้าถึงได้
- ต้องระบุและบังคับใช้ข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของบริษัท เมื่อมีความจำเป็นต้องให้บุคคลภายนอก หรือผู้ใช้บริการเข้าถึงสารสนเทศหรือทรัพย์สินสารสนเทศของบริษัท ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้
- ต้องระบุและจัดทำข้อกำหนดหรือข้อตกลงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศระหว่างบริษัทและหน่วยงานภายนอก เมื่อมีความจำเป็นต้องให้หน่วยงานนั้นเข้าถึงสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศของบริษัทก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

หมวด 3

การบริหารจัดการทรัพย์สินของบริษัท (Asset Management)

3.1 ความรับผิดชอบต่อสินทรัพย์ (Responsibility for Assets)

จุดประสงค์เพื่อให้มีการระบุทรัพย์สินของบริษัทและกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินอย่างเหมาะสม

- ต้องมีการจัดทำ และปรับปรุง บัญชีทรัพย์สิน (Inventory of Assets) ให้ทันสมัย
- ทรัพย์สินในบัญชีทรัพย์สินต้องระบุผู้ที่ถือครองทรัพย์สิน (Ownership of Assets)
- ต้องจัดทำกฎ ระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศอย่างเหมาะสม (Acceptable use of Assets)
- ต้องมีการเก็บรักษาทรัพย์สินที่มีความสำคัญต่อบริษัทอย่างเป็นระเบียบในสถานที่ที่ปลอดภัยให้เหมาะสม
- พนักงานและเจ้าหน้าที่ของหน่วยงานภายนอก ต้องคืนทรัพย์สินของบริษัททั้งหมดที่ตนเองถือครองเมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการว่าจ้างทันที (Return of Assets)
- พนักงานและเจ้าหน้าที่ของหน่วยงานภายนอก โดยการว่าจ้างจากบริษัท จะต้องมีความรับผิดชอบต่ออุปกรณ์คอมพิวเตอร์ที่ได้มอบไว้ให้ใช้งาน รวมทั้งสอดส่องดูแลทรัพยากรเหล่านี้ให้มีความปลอดภัย และคงความถูกต้อง โดยหมายความรวมถึงข้อมูล และระบบสารสนเทศของบริษัท
- ผู้ใช้งานต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ของบริษัทอย่างระมัดระวัง และให้การปกป้องเสมือนเป็นสินทรัพย์ของตน
- เครื่องคอมพิวเตอร์ลูกข่าย เครื่องคอมพิวเตอร์พกพา และเครื่องคอมพิวเตอร์แม่ข่าย ทั้งหมดของบริษัท ต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้งเมื่อต้องการเข้าใช้งาน และต้องได้รับการปกป้องอัตโนมัติโดยรหัสผ่านของ Screen Saver หรือทำการ Log Off อุปกรณ์ทุกครั้งเมื่อไม่ได้ใช้งานอุปกรณ์เป็นระยะเวลาหนึ่ง
- กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบอุปกรณ์คอมพิวเตอร์ของบริษัทที่ได้รับมอบหมาย
- ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ส่วนตัวของตนเข้าระบบเครือข่ายของบริษัทรวมถึงต้องไม่ติดตั้งซอฟต์แวร์ใด ๆ ลงในเครื่องคอมพิวเตอร์ของบริษัท ก่อนได้รับอนุญาตจากฝ่ายสารสนเทศ
- เครื่องคอมพิวเตอร์พกพาที่มีการเก็บข้อมูลลับไว้ ต้องได้รับการปกป้องเทียบเท่ากับเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ภายในบริษัท อาทิ การติดตั้งซอฟต์แวร์ป้องกันไวรัส ซอฟต์แวร์ป้องกันสปายแวร์ และมีการปรับปรุง Security Patch อยู่เสมอ ฯลฯ ในกรณีที่มีความประสงค์จะนำเครื่องคอมพิวเตอร์พกพาไปใช้ปฏิบัติงานนอกสถานที่ ต้องมีการจัดทำบันทึกเพื่อขออนุมัติในแต่ละครั้งจากผู้บริหารของหน่วยงานและแจ้งต่อฝ่ายงาน/ส่วนงานเทคโนโลยี

- อุปกรณ์คอมพิวเตอร์ของบริษัท ต้องไม่ถูกดัดแปลง หรือติดตั้งอุปกรณ์เพิ่มเติมใด ๆ ก่อนได้รับอนุญาตจากผู้บริหารของส่วนงานนั้น ๆ และเจ้าหน้าที่ ต้องไม่อนุญาตให้ผู้ไม่มีหน้าที่เกี่ยวข้องทำการติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ บนเครื่องคอมพิวเตอร์ของบริษัทอย่างเด็ดขาด
- การอนุญาตให้ใช้งานสินทรัพย์ด้านซอฟต์แวร์มีดังนี้
  - ห้ามเจ้าหน้าที่ทำการติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ของบริษัท
  - ซอฟต์แวร์ที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลลับหรือข้อมูลสำคัญของบริษัท ทั้งที่ได้มาจากการพัฒนาขึ้นโดยผู้ใช้งาน หรือที่ได้รับการจัดซื้อมา ต้องได้รับการตรวจสอบ ควบคุม และอนุมัติอย่างเหมาะสมโดยหน่วยงานเจ้าของระบบหรือข้อมูล ก่อนนำมาติดตั้งใช้งานบนระบบเทคโนโลยีสารสนเทศของบริษัทระบบสารสนเทศทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไป ต้องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอ เพื่อให้ผู้ใช้งานทั่วไปของบริษัท มีความเข้าใจและสามารถใช้งาน ระบบสารสนเทศได้
  - รายชื่อซอฟต์แวร์ หรือระบบสารสนเทศ ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งานต้องได้รับการจัดทำเป็นเอกสาร และได้รับการอนุมัติโดยผู้บริหารเทคโนโลยีสารสนเทศ
  - ซอฟต์แวร์ที่ใช้ต้องมีลิขสิทธิ์ถูกต้องครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ในการทำงานของบริษัทเท่านั้น
- การอนุญาตให้ใช้งานอินเทอร์เน็ตมีดังนี้
  - ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้บริษัทและบุคคลผู้ที่เกี่ยวข้องกับบริษัท เสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้ การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย
  - การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่านช่องทาง (Gateway) ที่ได้รับอนุญาต หรือผ่านเครื่องคอมพิวเตอร์ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเฉพาะกิจเท่านั้น ทั้งนี้ บริษัทขอสงวนสิทธิ์ในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งานในลักษณะที่ไม่เหมาะสม
  - ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบป๊อบอัพ หรือเข้าสู่เว็บไซต์ใด ๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต
  - ห้ามผู้ใช้งานเข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือผิดกฎหมาย
  - บริษัทห้ามการแสดงความคิดเห็นส่วนตัวในรูปแบบอิเล็กทรอนิกส์ (อาทิ โซเชียล มีเดีย, หรือ สื่อสังคมออนไลน์) ของพนักงาน ทั้งนี้ ความเสียหายใด ๆ ที่อาจเกิดขึ้นจากการแสดงความคิดเห็นดังกล่าว ถือเป็นความรับผิดชอบของพนักงานผู้นั้น
- การอนุญาตให้ใช้งานอีเมล์มีดังนี้
  - ผู้ใช้งานอีเมล์ทั้งหมดของบริษัท ต้องมี e-mail Account เป็นของตนเอง e-mail Account ต้องได้รับการปกป้องด้วยรหัสผ่าน เพื่อป้องกันการถูกล่วงละเมิดและการนำอีเมล์ไปใช้ในทางที่ผิด

- e-mail Account ที่มีวัตถุประสงค์พิเศษ อาทิ การสร้างขึ้นเพื่อเป็น e-mail Account กลางของส่วนงาน และ/หรือ เพื่อใช้งานร่วมกันโดยผู้ใช้งานมากกว่าหนึ่งคนขึ้นไป โดยต้องมีผู้ใช้งานหนึ่งคนที่ได้รับการแต่งตั้งให้ทำหน้าที่เป็นเจ้าของ e-mail Account นั้น
- e-mail Account ทั้งหมด และอีเมล์ทุกฉบับที่ถูกสร้าง และเก็บรักษาอยู่บนระบบคอมพิวเตอร์ หรือระบบเครือข่ายของบริษัท ถือเป็นสินทรัพย์ของบริษัท
- ผู้ใช้งานต้องใช้งานที่ได้รับอนุญาตเท่านั้นในการเข้าถึง และ/หรือ ติดต่อสื่อสารกับระบบอีเมล์ของบริษัท
- พื้นที่เก็บอีเมล์บนเครื่องคอมพิวเตอร์แม่ข่ายส่วนกลาง (Mailbox Size) ของผู้ใช้งานมีขนาดที่จำกัด ทั้งนี้เมื่อปริมาณของอีเมล์มากจนใกล้เคียงกับขนาดพื้นที่ที่ตั้งค่าไว้ ผู้ใช้งานจะได้รับข้อความแจ้งเตือนจากระบบ และถ้าหากปริมาณของอีเมล์มากเกินกว่าพื้นที่จัดเก็บแล้ว ผู้ใช้งานจะไม่สามารถรับ-ส่งอีเมล์ได้ตามปกติอีกต่อไป
- ขนาดของอีเมล์และไฟล์แนบได้รับการจำกัดไว้ โดยหากอีเมล์และไฟล์แนบมีขนาดใหญ่เกินกว่าที่กำหนด ผู้ใช้งานจะได้รับจดหมายตีกลับแจ้งว่าไม่สามารถส่งอีเมล์ดังกล่าวได้
- ผู้ใช้งานต้องลบอีเมล์ที่ไม่จำเป็นออกจาก Mailbox ของตนอยู่เสมอ เพื่อเป็นการรักษาพื้นที่เก็บอีเมล์ให้เป็นไปตามขนาดที่บริษัทกำหนด ทั้งนี้ผู้ใช้งานต้องเก็บรักษาอีเมล์ที่เกี่ยวข้องกับการทำงาน และอีเมล์ตามที่กฎหมายกำหนดไว้เท่านั้น
- ห้ามใช้ E-Mail Account ส่วนตัวมาใช้ในกิจกรรมของบริษัท ยกเว้นจะได้รับการอนุญาตเป็นรายบุคคลจากผู้บริหาร
- ห้ามใช้ E-Mail Account ของบริษัทเพื่อกระทำการใด ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย ตัวอย่าง อาทิ เพื่อการโฆษณายาสูบ สิ่งมึนเมา สินค้าหนีภาษี การเผยแพร่ซอฟต์แวร์ละเมิดลิขสิทธิ์
- ห้ามใช้ e-mail Account ของบริษัทในการประกาศข้อมูลใด ๆ ในชุมชนอิเล็กทรอนิกส์ อาทิ เว็บบอร์ด บล็อก กระดานข่าว เว้นแต่การประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนหนึ่งของการทำงานให้กับบริษัท
- ไฟล์เอกสารที่แนบมาพร้อมกับอีเมล์ จะต้องอยู่ในรูปแบบมาตรฐานซึ่งผู้รับสามารถเปิดอ่านได้ด้วยซอฟต์แวร์พื้นฐานบนทุกระบบปฏิบัติการ อาทิ PDF, DOC, TXT, CSV, XLS, JPG, GIF, PPT และ HTML
- อีเมล์ส่งออกนอกบริษัททุกฉบับต้องมีข้อความแสดงเจตจำนง/ข้อยกเว้นความรับผิดชอบของบริษัทแนบท้ายเสมอ
- ห้ามผู้ใช้งานทำสำเนาข้อความหรือทำสำเนาไฟล์แนบที่เป็นข้อมูลลับจากอีเมล์ของบุคคลอื่นก่อนได้รับอนุญาตจากเจ้าของข้อมูล
- ผู้ใช้งานต้องร่างเนื้อหาของอีเมล์ด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าตนเองเป็นผู้ส่งออกอีเมล์นั้นในนามตัวแทนของบริษัท
- ห้ามผู้ใช้งาน ใช้ข้อมูลภายในของบริษัทใด ๆ ของบริษัทส่งต่อให้บุคคลภายนอก ผ่านช่องทาง e-mail หรือผ่านสื่อ electronic ใด ๆ

- ห้ามผู้ใช้งานทำการปลอมแปลงข้อความในอีเมล์ หัวจดหมายอีเมล์ ลายเซ็นต์ในอีเมล์ หรือ e-mail Account ของบุคคลอื่นโดยเด็ดขาด
- ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งอีเมล์โดยใช้ e-mail Account ของตนโดยเด็ดขาด ไม่ว่าบุคคลนั้นจะเป็นผู้บังคับบัญชา เลขานุการ ผู้ช่วย หรือบุคคลอื่นใด ก็ตาม
- ห้ามผู้ใช้งานส่งอีเมล์ที่ผู้รับไม่ได้ต้องการ ตัวอย่าง อีเมล์ขยะ (Junk Mail) หรือโฆษณาสินค้าต่าง ๆ (Spam Mail)
- ห้ามผู้ใช้งานสร้างหรือมีส่วนร่วมใด ๆ กับการส่ง อีเมล์หลอกลวง หรือการส่งอีเมล์ในลักษณะลูกโซ่โดยเด็ดขาด
- ห้ามผู้ใช้งานส่งหรือส่งต่ออีเมล์ที่มีเนื้อหาหรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามกอนาจาร การยั่วยุทางเพศ หรืออีเมล์ที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรม หรือศาสนา และอีเมล์ที่กระทบต่อความมั่นคงของชาติ หรือสถาบันพระมหากษัตริย์โดยเด็ดขาด
- ห้ามผู้ใช้งานส่งอีเมล์ที่มีไฟล์แนบเกี่ยวกับการพนัน ภาพลามกอนาจาร หรือไฟล์อื่นใดที่ไม่เกี่ยวข้องกับการทำงานและส่งผลเสียต่อบริษัท
- ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจาก ผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัส อีเมล์บอมบ์ หรือโปรแกรมแฝง (ม้าโทรจัน)
- เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่า เครื่องคอมพิวเตอร์ของตนมีไวรัส ผู้ใช้งานต้องระงับการส่งอีเมล์โดยทันที และแจ้งให้ฝ่าย/ส่วนงานเทคโนโลยีเพื่อดำเนินการแก้ไข และต้องระงับการใช้งานจนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่สภาพปกติ

3.2 **การจัดชั้นความลับของสารสนเทศ** (Information Classification)

จุดประสงค์เพื่อให้สารสนเทศได้รับระดับการป้องกันที่เหมาะสมโดยสอดคล้องกับความสำคัญของสารสนเทศนั้นที่มีต่อบริษัท

- ชั้นความลับของสารสนเทศ (Classification of Information) ต้องมีการจัดชั้นความลับโดยพิจารณาจากความต้องการด้านกฎหมาย คุณค่าระดับความสำคัญ และระดับความอ่อนไหวหากถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
- ต้องมีการจัดทำขั้นตอนปฏิบัติสำหรับการบ่งชี้สารสนเทศ และปฏิบัติตาม ที่สอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่บริษัทกำหนดไว้
- ต้องมีการจัดทำขั้นตอนปฏิบัติสำหรับการจัดการทรัพย์สิน และปฏิบัติตามที่สอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่บริษัทกำหนดไว้

3.3 **การจัดการกับสื่อบันทึกข้อมูล** (Handling of Assets)

จุดประสงค์เพื่อป้องการการเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูล

- จัดทำขั้นตอนการปฏิบัติสำหรับการบริหารสื่อบันทึกข้อมูลที่ถอดแยกได้ และปฏิบัติตามที่สอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่บริษัทกำหนดไว้ (Management of Removable Media)
- สื่อบันทึกข้อมูลต้องมีการกำจัดหรือทำลายทิ้งอย่างมั่นคงปลอดภัย เมื่อหมดความต้องการในการใช้งาน โดยปฏิบัติตามขั้นตอนปฏิบัติสำหรับการทำลายซึ่งกำหนดไว้อย่างเป็นทางการ (Disposal of Media)
- การขนย้ายสื่อบันทึกข้อมูล ต้องมีการป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การนำไปใช้ผิดวัตถุประสงค์ หรือความเสียหายในระหว่างที่นำส่งหรือขนย้ายสื่อบันทึกข้อมูลนั้น (Physical Media Transfer)
- ห้ามการใช้งาน Share Drive ที่ทางฝ่ายสารสนเทศไม่ได้ทำการจัดเตรียมไว้ให้ เช่น google drive, Dropbox, One drive ส่วนตัว
- ห้ามนำสื่อบันทึกข้อมูล หรือสื่อบันทึกข้อมูลส่วนตัวที่ไม่ได้ทำการตรวจสอบมาใช้งานภายในบริษัท เมื่อมีความจำเป็นต้องใช้งานให้ทำการขออนุมัติจาก ผู้ช่วยกรรมการผู้จัดการสายงานปฏิบัติการและสารสนเทศ หรือผู้มีอำนาจอนุมัติสูงกว่าขึ้นไป

หมวด 4

ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resources Security)

4.1 การสร้างความความมั่นคงปลอดภัยในกระบวนการสรรหาบุคลากรก่อนการทำงาน (Prior to Employment)

จุดประสงค์เพื่อกำหนดและคัดสรรบุคคลก่อนที่จะเข้ามาทำงาน เพื่อลดความเสี่ยงจากความผิดพลาด การขโมย การปลอมแปลง และการนำไปใช้ในทางที่ไม่เหมาะสมของเจ้าหน้าที่อันเกิดจากการปฏิบัติงานกับระบบสารสนเทศ และทรัพยากรสารสนเทศอื่น ๆ ของบริษัท

- หน่วยงานภายนอกที่ได้รับการว่าจ้างตามสัญญาการจ้างงานต้องปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ ตามนโยบายและขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยของบริษัทอย่างเคร่งครัด
- ต้องทำการตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนที่จะบรรจุเป็นผู้บริหาร พนักงานชั่วคราวหรือนักศึกษาฝึกงาน โดยต้องไม่มีประวัติในการบุกรุก แก้ไข ทำลาย หรือโจรกรรมข้อมูลในระบบเทคโนโลยีสารสนเทศของหน่วยงานใดมาก่อน

4.2 การสร้างความความมั่นคงปลอดภัยขณะเป็นพนักงาน (During Employment)

จุดประสงค์เพื่อให้เจ้าหน้าที่ได้ตระหนักถึงภัยที่เกี่ยวข้องกับการปฏิบัติงานสารสนเทศ รวมถึงให้ความรู้แก่พนักงานเพื่อให้สามารถป้องกันภัยดังกล่าวได้

- เจ้าหน้าที่หรือผู้ใช้งานมีหน้าที่ศึกษาทำความเข้าใจวิธีปฏิบัติเกี่ยวกับการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศที่บริษัทกำหนด เพื่อนำไปปฏิบัติในการรักษาความปลอดภัยสินทรัพย์คอมพิวเตอร์ในส่วนที่ตนใช้งานหรือดูแลรับผิดชอบ
- ต้องจัดอบรมให้ความรู้แก่ พนักงาน เจ้าหน้าที่ เกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศ ซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัยฯ และการเปลี่ยนแปลงที่เกิดขึ้นด้านเทคโนโลยีสารสนเทศของบริษัทด้วย
- พนักงานทุกคน ต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและระเบียบปฏิบัติที่เกี่ยวข้องกับหน่วยงานก่อนหรืออย่างน้อยภายใน 30 วันนับจากเข้าทำงานในหน่วยงาน โดยควรเป็นส่วนหนึ่งของการปฐมนิเทศ และต้องมีการลงนามและเก็บรวบรวมไว้ในแฟ้มประวัติของบุคลากรด้วย
- ต้องกำหนดบทลงโทษทางวินัยสำหรับผู้ที่ฝ่าฝืนนโยบาย กฎ และ/หรือระเบียบปฏิบัติของบริษัท แต่หากเป็นการละเมิดข้อกฎหมาย บทลงโทษจะเป็นไปตามฐานความผิดที่ได้กระทำตามที่ระบุในแต่ละข้อกฎหมายนั้น ๆ

4.3 การยกเลิกการจ้างงาน (Termination of Change of Employment)

จุดประสงค์เพื่อให้มีการยกเลิกสิทธิ์กับเจ้าหน้าที่ที่ถูกยกเลิกการจ้างงานหรือหมดสัญญาฯ เพื่อความมั่นคงปลอดภัยของระบบสารสนเทศ เพื่อให้การบริหารจัดการ Login หรือ User ID เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด

- หน่วยงานด้านทรัพยากรบุคคล ต้องแจ้งให้ ฝ่ายสารสนเทศ ทราบทันทีเมื่อมีเหตุดังนี้
  - การว่าจ้างงาน
  - การเปลี่ยนแปลงสภาพการว่าจ้างงาน
  - การลาออกจากงาน หรือการสิ้นสุดการเป็นผู้บริหาร เจ้าหน้าที่ หรือการถึงแก่กรรม
  - การโยกย้ายหน่วยงาน
  - การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่
- พนักงานซึ่งพ้นสภาพจากการจ้างงานต้องคืนทรัพย์สินทั้งหมดซึ่งเกี่ยวข้องกับระบบงานคอมพิวเตอร์ รวมทั้งกุญแจ บัตรประจำตัวเจ้าหน้าที่ บัตรผ่านเข้า-ออก คอมพิวเตอร์และอุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่าง ๆ โดยจัดทำเอกสารส่ง
  มอบคืนทรัพย์สินของบริษัทที่ถือครองพร้อมส่งมอบทรัพย์สินของบริษัทให้กับเจ้าหน้าที่ฝ่ายทรัพยากรบุคคลลงนามก่อนวันสุดท้ายของการว่าจ้างงาน

หมวด 5

การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

5.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas)

จุดประสงค์เพื่อเป็นมาตรฐานในการรักษาความมั่นคงปลอดภัยทางกายภาพที่เกี่ยวกับสถานที่ซึ่งเป็นที่ตั้งและพื้นที่ใช้งานของระบบเทคโนโลยีสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูลและสารสนเทศซึ่งเป็นทรัพย์สินของบริษัท

5.1.1 ขอบเขต หรือ บริเวณโดยรอบทางกายภาพ (Physical Security Perimeter)

- การจัดทำบริเวณล้อมรอบต้องมีการจัดเป็นพื้นที่ควบคุม โดยสามารถแบ่งออกได้เป็น
  - พื้นที่ทำงานทั่วไป (General Working Area)
  - พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area)
  - พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือ ระบบเครือข่ายคอมพิวเตอร์ (IT Equipment Area)
  - พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area)
  - พื้นที่ใช้งานระบบเครือข่ายคอมพิวเตอร์ไร้สาย (Wireless LAN Coverage Area) เป็นต้น
- มีการจัดสภาพแวดล้อมทางกายภาพเพื่อป้องกันบุคคลภายนอกบุกรุกเข้าสู่พื้นที่ภายในสำนักงาน
- ประตู หรือ ทางเข้าสำนักงาน หรือ อาคารออกแบบเพื่อป้องกันการบุกรุกทางกายภาพ
- ประตู หรือ ทางเข้า-ออก ของห้องควบคุมระบบเครือข่ายคอมพิวเตอร์และเครื่องคอมพิวเตอร์แม่ข่ายต้องมีระบบที่สามารถล็อคได้ เพื่อป้องกันการบุกรุกทางกายภาพ

5.1.2 การควบคุมการเข้า-ออกทางกายภาพ (Physical Entry Controls) มีข้อปฏิบัติดังนี้

- มีการกำหนดสิทธิ์ หรือ ทะเบียนผู้ใช้งานที่มีสิทธิ์ผ่านเข้า-ออก เพื่อปฏิบัติหน้าที่ตามสิทธิ์และหน้าที่ที่ได้รับมอบหมายและช่วงเวลาที่สามารถผ่านเข้า-ออก บริเวณที่ต้องมีการรักษาความปลอดภัย และพื้นที่ที่มีข้อมูลสำคัญจัดเก็บ หรือ ประมวลผลอยู่
- อนุญาตให้ผ่านเข้า-ออกเฉพาะผู้ที่มีหน้าที่ปฏิบัติงานภายในพื้นที่ หรือ ผู้ที่ได้รับอนุญาตตามความจำเป็นเท่านั้น
- ต้องให้มีการพิสูจน์ตัวตนเพื่อควบคุมการเข้า-ออกพื้นที่ หรือ บริเวณที่มีความสำคัญ เช่น การใช้บัตรผ่านเข้า-ออก การใช้รหัสผ่าน การบันทึกการเข้า-ออกพื้นที่ในแบบฟอร์มบันทึกการเข้า-ออกพื้นที่ เป็นต้น
- ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่ หรือ บริเวณที่มีความสำคัญ เว้นแต่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้อำนวยการฝ่ายสารสนเทศ หรือ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่
- การขออนุญาตเข้าพื้นที่ หรือ บริเวณที่มีความสำคัญของบุคคลภายนอก โดยต้องมีเหตุผลที่เพียงพอในการขออนุญาต
- ให้บันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitor) และจะต้องมีเจ้าหน้าที่ของฝ่ายสารสนเทศอยู่กับบุคคลที่มาติดต่อตลอดเวลา

5.1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่น ๆ (Securing Offices Rooms and Facilities) มีข้อปฏิบัติดังนี้

- เจ้าหน้าที่ทุกคนมีหน้าที่ในการป้องกันทรัพย์สินของฝ่ายสารสนเทศ ที่ได้รับการจัดสรรหรือให้อยู่ในความรับผิดชอบ
- เจ้าหน้าที่ต้องออกจากระบบ เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล หรือ เมื่อไม่มีการใช้งานชั่วคราว
- ต้องล็อค ปิดห้องทำงานทุกครั้ง เมื่อไม่มีเจ้าหน้าที่อยู่ปฏิบัติงาน
- ต้องมีการจัดเก็บข้อมูล หรือ เก็บอุปกรณ์ที่สำคัญในสถานที่ที่มีความปลอดภัย เช่น ในตู้เอกสารที่มีกุญแจล็อค และไม่ทิ้ง เอกสารที่สำคัญไว้บนโต๊ะ เพื่อความปลอดภัยของข้อมูล
- ต้องไม่ให้ผู้อื่นใช้อุปกรณ์คอมพิวเตอร์ต่าง ๆ โดยไม่ได้รับอนุญาต เช่น เครื่องคอมพิวเตอร์ เครื่องพิมพ์เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น
- ต้องนำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

5.1.4 การป้องกันภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting Against External End Environmental Threats)

บริเวณที่ต้องมีการรักษาความปลอดภัยที่ระดับความสำคัญสูงสุด คือ ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือ ระบบเครือข่ายคอมพิวเตอร์ ห้องคอมพิวเตอร์ ต้องปฏิบัติตามในทุกข้อ และบริเวณที่ต้องมีการรักษาความปลอดภัยอื่น ๆ ควรปฏิบัติตามความจำเป็น ดังนี้

- จัดให้มีผนังที่แข็งแรง ติดตั้งจากพื้นห้องถึงเพดานด้านบน เพื่อป้องกันการบุกรุก
- จัดให้มีระบบป้องกันอัคคีภัย และระบบดับเพลิง
- จัดให้มีระบบควบคุมน้ำรั่ว ภายในห้องคอมพิวเตอร์
- จัดให้มีระบบควบคุมอุณหภูมิ และความชื้น เครื่องปรับอากาศที่สามารถตั้งอุณหภูมิ และควบคุมความชื้นภายในห้องให้มีสภาพแวดล้อมที่เหมาะสม
- จัดให้มีการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

5.1.5 การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in Secure Areas) มีข้อปฏิบัติดังนี้

- ต้องปฏิบัติงานตามคู่มือปฏิบัติงาน และคู่มือการจัดการอุปกรณ์ต่าง ๆ อย่างเคร่งครัด
- ห้ามนำสิ่งของต่อไปนี้เข้าพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัยโดยเด็ดขาด
  - อาหาร หรือ เครื่องดื่ม
  - วัตถุไวไฟ หรือ เชื้อเพลิง
- การปฏิบัติงานภายนอกเหนือจากเวลางานปกติ ต้องได้รับการอนุมัติจากผู้บังคับบัญชาต้นสังกัด
- ผู้ใช้งานภายนอกที่จะนำคอมพิวเตอร์ หรือ อุปกรณ์ใด ๆ มาเชื่อมต่อกับระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ของบริษัท ต้องได้รับอนุญาตจากผู้อานวยการฝ่ายสารสนเทศ หรือ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่แทน โดยผู้ใช้งานภายนอกต้องลงทะเบียนเพื่อขอรับ User, Password ในการเข้าใช้งานระบบเครือข่ายคอมพิวเตอร์เท่านั้น

- ห้ามผู้ใดเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือ กระทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์หลัก เป็นต้น หากมีความจำเป็นต้องเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือ กระทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ต้องได้รับอนุญาตจากผู้อำนวยการฝ่ายสารสนเทศ

5.1.6 พื้นที่สำหรับรับส่งสิ่งของ (Delivery and Loading Areas) มีข้อปฏิบัติดังนี้

- จำกัดการเข้าถึงพื้นที่ หรือ บริเวณที่มีการส่งมอบ หรือ ขนถ่ายผลิตภัณฑ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่ หรือ บริเวณส่งมอบนั้น
- ควรจัดพื้นที่ หรือ บริเวณส่งมอบไว้ในบริเวณต่างหากเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่น ๆ ภายในบริษัท
- ต้องตรวจสอบวัสดุ หรือ ปัจจัยการผลิตที่เป็นอันตรายก่อนที่จะโอนย้ายวัสดุนั้น ไปยังพื้นที่ที่มีการใช้งาน
- กำหนดให้มีการลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขาย หรือ ผู้ให้บริการภายนอกโดยให้สอดคล้องกับการบริหารจัดการทรัพย์สินของฝ่ายสารสนเทศ

5.2 **ความมั่นคงปลอดภัยของอุปกรณ์** (Equipment Security)

จุดประสงค์เพื่อป้องกันการใช้อุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต และเพื่อให้มั่นใจได้ว่าอุปกรณ์คอมพิวเตอร์ได้มีการป้องกันอย่างเพียงพอจากภัยธรรมชาติ การโจรกรรม และความเสียหายอื่น ๆ เจ้าหน้าที่หรือผู้ใช้งานต้องจัดวางและป้องกันอุปกรณ์ของบริษัทเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่าง ๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

5.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment Setting and Protection) มีข้อปฏิบัติดังนี้

- ต้องจัดวางอุปกรณ์ในพื้นที่ และบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของผู้ปฏิบัติงานในหน่วยงานให้น้อยที่สุด
- ต้องจัดวางระบบเทคโนโลยีสารสนเทศและการสื่อสารในตำแหน่งที่เหมาะสม เพื่อหลีกเลี่ยงการมองเห็นข้อมูลสำคัญจาก บุคคลภายนอก โดยการหันหน้าจอเข้ามาภายในโดยไม่ให้บุคคลผู้ซึ่งไม่มีสิทธิสามารถมองเห็นหน้าจอนั้นได้
- ต้องแยกอุปกรณ์ที่มีความสำคัญไว้ต่างหากอีกพื้นที่หนึ่ง เพื่อดูแลความมั่นคงปลอดภัย
- ห้ามไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณ หรือ พื้นที่ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบเครื่องคอมพิวเตอร์แม่ข่าย
- ดำเนินการตรวจสอบระดับอุณหภูมิ และดูแลสภาพแวดล้อมภายในบริเวณห้องควบคุมระบบเครือข่ายคอมพิวเตอร์/ระบบคอมพิวเตอร์/ระบบเครื่องคอมพิวเตอร์แม่ข่าย เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว

5.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities) มีข้อปฏิบัติดังนี้

- ต้องมีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เพียงพอต่อความต้องการ ดังต่อไปนี้
- จัดให้มีระบบสำรองกระแสไฟฟ้า (UPS) และปรับแรงดันไฟฟ้าอัตโนมัติที่สามารถทำงานเมื่อเกิดปัญหาขัดข้องทางไฟฟ้าโดยไม่ทำความเสียหายให้แก่อุปกรณ์ และระบบงานระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- จัดให้มีระบบเฝ้าระวังและรายงานเมื่อพบข้อผิดพลาด
- จัดให้มีการตรวจสอบ หรือ ทดสอบ ระบบและอุปกรณ์สนับสนุนเหล่านั้นอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าระบบงานทำงานได้ตามปกติ
- ติดตั้งระบบแจ้งเตือน ในกรณีที่ระบบสนับสนุนการทำงานภายในห้องระบบคอมพิวเตอร์ทำงานผิดปกติหรือหยุดการทำงาน

5.2.3 ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling Security) มีข้อปฏิบัติดังนี้

- หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้
- ให้มีการป้องกันสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือ การตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย
- ให้เดินสายสัญญาณสื่อสาร และสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณ ซึ่งกันและกัน
- ทำป้ายชื่อสำหรับสายสัญญาณ และบนอุปกรณ์เพื่อป้องกันการตัดสัญญาณผิดเส้น
- จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนถูกต้อง
- ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

5.2.4 การบำรุงรักษาอุปกรณ์ (Equipment Maintenance) มีข้อปฏิบัติดังนี้

- ให้มีการกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลา หรือ ที่แนะนำโดยผู้ผลิต
- ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ
- จัดเก็บบันทึกกิจกรรมการบำรุงอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบ หรือประเมินภายหลัง
- จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว
- ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอก ที่มาทำการบำรุงรักษาอุปกรณ์
- จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอกที่มาทำการบารุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

5.2.5 การนำทรัพย์สินออกนอกบริษัท (Removal of Assets) มีข้อปฏิบัติดังนี้

- ให้มีการขออนุญาตก่อนนำอุปกรณ์ หรือ ทรัพย์สินนั้นออกไปใช้งานนอกบริษัท
- กำหนดผู้มีอำนาจ/ผู้รับผิดชอบในการเคลื่อนย้าย หรือ นำอุปกรณ์ออกนอกบริษัท
- กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้นอกบริษัท

- เมื่อมีการนำอุปกรณ์ส่งคืนให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย
- บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้นอกบริษัทเพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

5.2.6 ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกบริษัทมีข้อปฏิบัติดังนี้

- กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์ หรือ ทรัพย์สินของบริษัทออกไปใช้งาน
- ไม่ทิ้งอุปกรณ์ หรือ ทรัพย์สินของบริษัทไว้โดยลำพังในที่สาธารณะ
- เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์ หรือ ทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

5.2.7 ความมั่นคงปลอดภัยสำหรับการกำจัด หรือ ทำลายอุปกรณ์ หรือ นำอุปกรณ์ไปใช้งานอย่างอื่น หรือ นำอุปกรณ์ไปใช้ซ้ำ มีข้อปฏิบัติดังนี้

- ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว
- มีมาตรการ หรือ เทคนิคในการลบ หรือ เขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์ สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

5.2.8 การป้องกันอุปกรณ์ที่ปล่อยทิ้งไว้โดยไม่มีผู้ดูแล หรือ ในขณะที่ว่างเว้นจากการใช้งาน หรือ ไม่ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์ (Unattended User Equipment) มีข้อปฏิบัติดังนี้

- ผู้ดูแลระบบ หรือ ผู้ใช้งาน ต้องลงชื่อออกจากระบบเทคโนโลยีสารสนเทศและการสื่อสาร ระบบงานคอมพิวเตอร์ที่ใช้งาน หรือ เครื่องคอมพิวเตอร์แบบพกพา โดยทันทีเมื่อเสร็จสิ้นการปฏิบัติงาน หรือเมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- ผู้ดูแลระบบ หรือ ผู้ใช้งาน ต้องล็อค ปิด หรือ เก็บอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งาน หรือ ปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว
- ผู้ดูแลระบบ ต้องกำหนดให้พนักงานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์ หรือ ระบบเทคโนโลยีสารสนเทศของตน โดยใส่รหัสผ่านได้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์ และให้มีการตั้งล็อคหน้าจอเครื่องคอมพิวเตอร์หลังจากไม่ได้ใช้งานเป็นเวลาไม่เกิน 15 นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

5.2.9 นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและนโยบายการป้องกันหน้าจอคอมพิวเตอร์ในขณะที่ไม่ได้ใช้งาน (Clear Desk and Clear Screen Policy) มีข้อปฏิบัติดังนี้

- ต้องกำหนดการควบคุมเอกสาร ข้อมูล หรือ สื่อบันทึกข้อมูลต่าง เช่น Thumb Drive และExternal Hard Disk ที่มีข้อมูลสารสนเทศที่สำคัญที่จัดเก็บ หรือ บันทึกอยู่ ไม่ให้วางทิ้งไว้บนโต๊ะทางาน หรือ สถานที่ไม่ปลอดภัยในขณะที่ไม่ได้ใช้งาน (Clear Desk)
- ต้องมีการควบคุมหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏในขณะที่ไม่ได้ใช้งาน (Clear Screen) เช่น การตัดออกจากระบบ (Session Time Out) และการล็อคหน้าจอ (Lock Screen) อัตโนมัติ เป็นต้น

หมวดที่ 6

การเข้ารหัสข้อมูล (Encryption)

6.1 มาตรการควบคุมการเข้ารหัสข้อมูล (Cryptographic Controls)

จุดประสงค์เพื่อให้การใช้งานระบบการเข้ารหัสข้อมูลมีความเหมาะสม มีประสิทธิภาพ และสามารถป้องกันการเข้าถึง หรือเปลี่ยนแปลง แก้ไขข้อมูลที่เป็นความลับ หรือ มีความสำคัญ

6.1.1 นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the Use of Cryptographic Controls)

ต้องจัดให้มีนโยบายควบคุมการใช้งานระบบการเข้ารหัสข้อมูลที่คำนึงถึงชนิด และวิธีการเข้ารหัสข้อมูล ที่สอดคล้องเหมาะสมกับระดับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลที่เป็นความลับ หรือ มีความสำคัญ รวมทั้ง กำหนดผู้รับผิดชอบในการดำเนินนโยบาย และการบริหารจัดการกุญแจเพื่อการเข้ารหัสข้อมูล (Key Management) โดยผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ ต้องแสดงข้อปฏิบัติสำหรับการเข้าถึงข้อมูลลับ หรือข้อมูลที่สำคัญเช่น

- ผู้ดูแลระบบต้องกำหนดรูปแบบ Wireless Security ให้เป็น WPA/WPA2 (WIFI Protected Access) ในการเข้ารหัสข้อมูลระหว่างเครื่องลูกข่าย (Wireless LAN Client) และอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point)
- การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted Backup) ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีรหัสก่อนเข้าถึงข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย
- การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (E-Mail) เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูลที่ฝ่ายสารสนเทศกำหนดไว้ และให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail) ของผู้รับให้ถูกต้อง เพื่อป้องกันการส่งผิด
- การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายคอมพิวเตอร์สาธารณะ ควรได้รับการเข้ารหัสลับ (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML encryption เป็นต้น
- การนำเทคนิคการเข้ารหัสข้อมูลมาใช้ในการรับส่งข้อมูลสารสนเทศ ผ่านช่องทางการสื่อสารบางประเภทที่ต้องการการรักษาความมั่นคงปลอดภัย เช่น การใช้งานระบบ Cloud Computing

6.1.2 การบริหารจัดการกุญแจ (Key Management)

ต้องจัดให้มีนโยบายการบริหารกุญแจเพื่อการเข้ารหัสข้อมูลตลอดช่วงเวลาการใช้งาน (Key Management Whole Life Cycle) โดยกำหนดแนวปฏิบัติเพื่อการคัดเลือกวิธีการเข้ารหัสการกำหนดความยาวของรหัสการใช้งานและการยกเลิกการใช้งานกุญแจเพื่อการเข้ารหัส กระบวนการบริหารจัดการกุญแจเพื่อการเข้ารหัส รวมทั้ง ติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบาย และแนวทางปฏิบัติดังกล่าวอย่างสม่ำเสมอ เช่น มาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรือ อื่น ๆ ที่มีความสำคัญเช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

หมวด 7

การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของบริษัท (Communication and Operations Management)

7.1 การกำหนดหน้าที่ความรับผิดชอบและวิธีการปฏิบัติงาน (Operational Procedures and Responsibilities)

จุดประสงค์เพื่อให้การใช้ปฏิบัติงานและการบริหารจัดการโครงสร้างพื้นฐานด้านสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย

7.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented Operating Procedures)

- ต้องจัดให้มีวิธีการปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของฝ่ายสารสนเทศที่สำคัญเป็นลายลักษณ์อักษร เพื่อให้พนักงาน สามารถปฏิบัติงานได้อย่างถูกต้อง และเป็นไปตามนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร
- ต้องทบทวนวิธีการปฏิบัติดังกล่าวให้เป็นปัจจุบันอยู่เสมอ รวมทั้ง จัดให้วิธีปฏิบัติงานดังกล่าวอยู่ในสภาพที่พร้อมใช้งานและเข้าถึงได้

7.1.2 การบริหารจัดการการเปลี่ยนแปลง (Change Management)

- ต้องจัดให้มีการควบคุมการปฏิบัติงานอย่างเคร่งครัด โดยเฉพาะในกรณีที่มีการเปลี่ยนแปลงโครงสร้างฝ่ายสารสนเทศ กระบวนการปฏิบัติงาน ขั้นตอนการปฏิบัติงาน การปรับตั้งค่าการทำงานของอุปกรณ์ประมวลผลข้อมูล หรือ การทำงานของระบบงานต่าง ๆ ที่มีผลกระทบต่อความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสาร เช่น
  - กำหนดขั้นตอน หรือ วิธีปฏิบัติที่เป็นลายลักษณ์อักษร ในกรณีการเปลี่ยนแปลงที่มีนัยสำคัญ
  - มีแผนรองรับ และดำเนินการทดสอบภายหลังการเปลี่ยนแปลง
  - มีการประเมินผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง
  - มีขั้นตอนการขออนุมัติจากผู้มีอานาจ
  - มีขั้นตอนการตรวจสอบเพื่อให้มั่นใจว่ากระบวนการเปลี่ยนแปลงดังกล่าวเป็นไปตามนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศ
  - มีการสื่อสารให้บุคคลที่เกี่ยวข้องได้รับทราบเพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง
  - มีกระบวนการถอยกลับสู่สภาพเดิม (Fall Back) ของระบบงาน หากเกิดข้อผิดพลาดระหว่างการเปลี่ยนแปลง
- ต้องทำการบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญและแจ้งให้หน่วยงานอื่น ๆ ที่เกี่ยวข้องทราบกรณีที่มีการเปลี่ยนแปลงแก้ไข

7.1.3 การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

ต้องติดตาม/เฝ้าระวังการทำงานของระบบงานและทรัพย์สินระบบเทคโนโลยีสารสนเทศและการสื่อสารประเภทอุปกรณ์ที่สำคัญ ให้ทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ เพื่อใช้เป็นข้อมูลในการประเมิน

สมรรถนะและความเพียงพอ (Capacity) ของระบบงานและทรัพย์สินสารสนเทศประเภทอุปกรณ์ระบบเทคโนโลยีสารสนเทศและการสื่อสารของฝ่ายสารสนเทศ

- มีการวางแผนการตรวจสอบประเมินขีดความสามารถของระบบและกำหนดค่าสูงสุดที่ยอมรับได้ของขีดความสามารถของระบบทั้งทางด้านอุปกรณ์ระบบคอมพิวเตอร์และระบบเครือข่าย อย่างน้อยการประเมินค่า CPU, RAM, Storage, Network Utilization
- ดำเนินการตรวจสอบประเมินขีดความสามารถของระบบดังระบุข้างต้น
- ดำเนินการวิเคราะห์ ประมวลผล ขีดสมรรถนะของระบบเพื่อค้นหาสาเหตุและปัญหา แนวทางการแก้ไขอย่างเป็นระบบ รวมทั้ง ติดตาม ปรับปรุง และคาดการณ์ความต้องการเพิ่มเติมในอนาคตเพื่อให้ระบบมีประสิทธิภาพ
- สรุปผลการบริหารจัดการขีดสมรรถนะของระบบ รวมถึงบุคลากร เพื่อให้สามารถรองรับแผนการปฏิบัติงานในอนาคตได้อย่างมีประสิทธิภาพ

7.1.4 การแยกสภาพแวดล้อมสาหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน

- ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) และใช้งานจริง (Production Environment) ออกจากกัน
- การแบ่งแยกส่วนดังกล่าว อาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือ แบ่งโดยการจัดเนื้อที่แยกไว้ต่างหากภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้
- มีการสำรองข้อมูลก่อนการปรับปรุงแก้ไข เพื่อการพัฒนาการทดสอบและการควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น เพื่อลดความเสี่ยงของการเข้าถึงหรือการเปลี่ยนแปลงสำหรับการให้บริการโดยไม่ได้รับอนุญาต

7.2 การจัดการผู้ให้บริการภายนอก (Third Party Service Delivery Management)

จุดประสงค์เพื่อให้มีและคงไว้ซึ่งระดับการรักษาความปลอดภัยสารสนเทศ และระดับการให้บริการที่เหมาะสมและสอดคล้องกับข้อตกลงการบริการกับหน่วยงานภายนอก

- ต้องมีการจัดทำข้อตกลงเพื่อควบคุมการให้บริการด้านเทคโนโลยีสารสนเทศของหน่วยงานภายนอกโดยต้องประกอบไปด้วยรายละเอียด ดังนี้
  - การยอมรับนโยบายและการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศของบริษัท
  - ขอบเขต รายละเอียด และระดับการให้บริการ (Service Level Agreement)
  - เอกสารต่าง ๆ เกี่ยวกับมาตรการการควบคุมที่ใช้ทั้งด้านกายภาพและด้าน Logical
  - เพื่อให้มั่นใจได้ว่าระบบงานของผู้ให้บริการจากภายนอกสามารถรักษาความมั่นคงปลอดภัยสารสนเทศได้ทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)
  - ข้อตกลงการเชื่อมโยงระบบเครือข่ายของหน่วยงานภายนอก

- ข้อมูลที่หน่วยงานภายนอกสามารถเข้าถึงได้และขั้นตอนและวิธีการร้องขอข้อมูลของบริษัท กรณีต้องการข้อมูลเพิ่มเติม
- สัญญาในการไม่เปิดเผยข้อมูลของบริษัท
- การยืมหรือการร้องขอใช้อุปกรณ์ของบริษัท
- ข้อกำหนดทางด้านกฎหมาย เช่น ความลับส่วนบุคคล (Privacy) และการป้องกันข้อมูล

- ให้ฝ่ายสารสนเทศ ทบทวนและตรวจสอบบริการจาก ผู้ให้บริการ ภายนอกตามข้อตกลงที่กำหนด
- ให้ฝ่ายสารสนเทศ เป็นผู้รับผิดชอบในการบริหารจัดการ การเปลี่ยนแปลงในการให้บริการจากผู้ให้บริการภายนอก
- หน่วยงานภายนอกที่ทำงานให้กับบริษัท ไม่ว่าจะทำงานอยู่ภายในบริษัทหรือนอกสถานที่ จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของบริษัท โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ
- ต้องพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของหน่วยงานภายนอก ทั้งนี้ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เข้าไปปฏิบัติงาน
- เจ้าของโครงการ ซึ่งรับปิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล
- บริษัทมีสิทธิ์ในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้มั่นใจว่าสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น
- ต้องดำเนินการให้ผู้ให้บริการหน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

7.3 การวางแผนและการยอมรับระบบสารสนเทศ (System Planning and Acceptance)

จุดประสงค์เพื่อลดความเสี่ยงต่อการเกิดความล้มเหลวของระบบลงให้เหลือน้อยที่สุด

- ฝ่ายสารสนเทศ ต้องมีการติดตามสภาพการใช้งาน และวิเคราะห์ขีดความสามารถทรัพยากรปัจจุบันอย่างสม่ำเสมอ ตามความเหมาะสมของทรัพยากรชนิด ต่าง ๆ โดยปฏิบัติตามเอกสารคู่มือการจัดการขีดความสามารถ
- ฝ่ายสารสนเทศ ต้องมีการวางแผนจัดการขีดความสามารถของระบบ อย่างน้อยปีละ 1 ครั้งโดยพิจารณาจากความต้องการใช้งานทรัพยากรสารสนเทศในอนาคต (อาทิ ความต้องการใน 1 ปีที่จะถึง อาทิ CPU ที่ความเร็วสูงขึ้น ฮาร์ดดิสก์ที่ความจุมากขึ้น สภาพการใช้งานทรัพยากรในปัจจุบัน การเปลี่ยนแปลงของเทคโนโลยี
- ฝ่ายสารสนเทศ ต้องจัดให้มีเกณฑ์ในการยอมรับระบบใหม่ ระบบที่จัดซื้อเข้ามาใช้งาน หรือทรัพยากรสารสนเทศอื่น ๆ ก่อนการใช้งาน รวมทั้งต้องทำการทดสอบก่อนที่จะตรวจรับระบบนั้นด้วย โดยปฏิบัติตามเอกสารคู่มือการจัดการการยอมรับระบบ

7.4 การควบคุมและป้องกันการใช้งานระบบและอุปกรณ์เคลื่อนที่ผิดวัตุประสงค์ (Protection against Malicious and Mobile Code)

จุดประสงค์เพื่อเป็นแนวทางการป้องกัน ควบคุมและคุ้มครองผู้ใช้งาน จากการใช้งานระบบซอฟแวร์ ข้อมูลและอุปกรณ์สื่อสารอิเล็กทรอนิกส์แบบไร้สายสารสนเทศ อาทิ โทรศัพท์มือถือ Smart Phone Tablets เครื่องคอมพิวเตอร์แบบพกพา ผิดจากวัตถุประสงค์การใช้งานที่กำหนดหรือกิจกรรมที่ไม่ประสงค์

- เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารอิเล็กทรอนิกส์แบบไร้สายสารสนเทศที่ต้องการใช้งานผ่านระบบเครือข่ายของบริษัท จะต้องได้รับการลงทะเบียนและกำหนดสิทธิ์การใช้งานตามนโยบายความปลอดภัย ก่อนได้รับการอนุมัติเพื่อใช้งานในระบบ โดยการลงทะเบียนของอุปกรณ์ที่เคลื่อนที่ได้ต้องประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้
  - วันที่รับเรื่อง และวันที่ขอลงทะเบียน
  - ชนิดและประเภทของอุปกรณ์
  - หมายเลขอุปกรณ์ อาทิ MAC Address
  - เจ้าของข้อมูล ผู้ดูแลระบบและผู้อนุมัติให้ดำเนินการ
  - ความจำเป็นที่จะต้องใช้งานอุปกรณ์นั้น ๆ
  - ระบุสิทธิ์การใช้งานของอุปกรณ์
- เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์แบบพกพา ต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัส รุ่นล่าสุดที่ได้รับการอนุมัติจากฝ่ายสารสนเทศ และต้องเปิดใช้งานตลอดเวลาที่ใช้งานเครื่อง โดยปฏิบัติตามเอกสารคู่มือการจัดการควบคุมซอฟต์แวร์ไม่ประสงค์ดี
- เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันไวรัส ต้องมีการปรับปรุงข้อมูลล่าสุด (Update Latest Pattern) อยู่เสมอ เครื่องให้บริการ เครื่องตั้งโต๊ะ และโน้ตบุ๊คทุกเครื่องต้องได้รับการปรับปรุงข้อมูลล่าสุดจากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันไวรัส โดยมีการรายงานผลดำเนินการปรับปรุงต่อผู้บริหารของฝ่าย/ส่วนงานเทคโนโลยีเป็นประจำทุกเดือน
- เอกสารการติดตั้งค่าของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการป้องกันไวรัส ต้องได้รับการตรวจสอบทุก 6 เดือน
- ห้ามเจ้าหน้าที่ทำการดาวน์โหลด Share Ware หรือ Free Ware โดยตรงจากอินเทอร์เน็ต โดยปราศจากการอนุมัติจากฝ่ายสารสนเทศ หลังจากการอนุมัติแล้วเจ้าหน้าที่ต้องทำการสแกนซอฟต์แวร์ด้วยโปรแกรมตรวจหาไวรัส ก่อนการใช้งาน
- ไฟล์ทุกไฟล์ที่ดาวน์โหลดในหน่วยงานเป็นไฟล์แนบของอีเมล์ สำเนาจากแผ่นดิสก์ หรือไฟล์แชร์ต่าง ๆ ต้องได้รับการสแกนหาไวรัส
- ห้ามผู้ใช้งานสร้าง เก็บ หรือเผยแพร่โปรแกรมมุ่งร้ายใด ๆ ตัวอย่าง ไวรัส หนอนอินเทอร์เน็ต โปรแกรมแฝง (ม้าโทรจัน) อีเมล์บอมบ์ เข้าสู่ระบบคอมพิวเตอร์ของบริษัท

- ห้ามผู้ใช้งานขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส ไฟล์ที่เกี่ยวข้องกับการทำงานเท่านั้นที่ได้รับอนุญาตให้สามารถรับ-ส่งผ่านระบบเครือข่ายของบริษัทได้ ทั้งนี้ ผู้ใช้งานควรรับไฟล์เฉพาะจากบุคคลที่ตนรู้จักและจากช่องทางการติดต่อสื่อสารที่น่าจะเป็นไปได้เท่านั้น นอกจากนี้ ผู้ใช้งานต้องทำการสแกนไวรัสในไฟล์ที่ได้รับด้วยซอฟต์แวร์ป้องกันไวรัสของบริษัท ก่อนเปิดใช้งานเสมอ
- เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องให้ปิดฟังก์ชันการทำงานเชื่อมต่อกับอินเทอร์เน็ตยกเว้นในกรณีที่จำเป็นต้องใช้เท่านั้น เพื่อเป็นการป้องกันไม่ให้โปรแกรมไม่ประสงค์ดีมีผลกระทบกับข้อมูลที่สำคัญบนเครื่องคอมพิวเตอร์แม่ข่ายเหล่านี้
- ห้ามผู้ใช้งานติดตั้งโปรแกรมชนิดเคลื่อนที่ได้ อาทิ Active Code ต่าง ๆ (เช่น Java, Active X) จากแหล่งที่ไม่น่าเชื่อถือในอินเทอร์เน็ต ต้องจัดให้มีการสัมมนา อบรมพิเศษภายในบริษัทให้กับพนักงาน เกี่ยวกับ การใช้เครื่องคอมพิวเตอร์ การใช้ระบบงาน และแนวทางการรักษาความปลอดภัยของระบบงานอย่างน้อยปีละ 1 ครั้ง

7.5 นโยบายการสำรองข้อมูล (Information Back-Up)

จุดประสงค์เพื่อเป็นแนวทางในกำหนดการสำรองข้อมูล เพื่อใช้ในการกู้ระบบในกรณีที่เกิดเหตุต่าง ๆ อาทิ ภัยธรรมชาติ ระบบเสียหาย

- ข้อมูลสำคัญที่เกี่ยวข้องกับการดำเนินงานทั้งหมด ทั้งที่มีการเก็บรักษาอยู่ในเครื่องคอมพิวเตอร์แม่ข่ายที่ดูแลต้องได้รับการสำรองข้อมูลอย่าง สม่ำเสมอ เพื่อประโยชน์ในการกู้คืนข้อมูลเมื่อมีปัญหาใด ๆ เกิดขึ้น เช่น การติดไวรัส ภัยธรรมชาติ ระบบเสียหาย เป็นต้น
- ให้ผู้ดูแลระบบกำหนดชนิดสื่อบันทึก ความถี่และช่วงเวลาการสำรองข้อมูลตามความเหมาะสม ให้เป็นปัจจุบันอย่างสม่ำเสมอ พร้อมทั้งกำหนดสื่อ ที่ใช้เก็บข้อมูล ขึ้นอยู่กับความสำคัญของข้อมูลและการยอมรับความเสี่ยงที่กำหนดโดยเจ้าของข้อมูล หรือ ระบบ โดยรูปแบบการสำรองข้อมูลมี 2 ชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Back Up) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)
- ให้ผู้ดูแลระบบตรวจสอบข้อมูลทั้งหมดว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลคอนฟิกกูเรชั่น (Configuration) ข้อมูลในฐานข้อมูล
- สื่อที่ใช้เก็บข้อมูลต้องมีป้ายบอกรายละเอียด ซึ่งประกอบด้วยข้อมูลอย่างน้อย ดังนี้
  - ชื่อระบบ
  - วันสร้าง
  - ระดับความสำคัญของข้อมูล
  - รายละเอียดติดต่อผู้ดูแลข้อมูล

  ทั้งนี้ให้ขึ้นอยู่กับรูปแบบการจัดเก็บข้อมูล
- ผู้ดูแลระบบและผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

- ต้องจัดให้มีการดูแลอุปกรณ์ หรือ ระบบสำรองข้อมูลให้มีประสิทธิภาพ สามารถใช้งานได้ตลอดเวลา
- ข้อมูลสำรองต้องได้รับการทดสอบเป็นระยะ ๆ เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่างสมบูรณ์
- ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุ ไม่สามารถดำเนินการอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหา และสรุปผลการแก้ไขปัญหา และรายงานต่อ ผู้ช่วยกรรมการผู้จัดการสายงานปฏิบัติการและสารสนเทศ ผู้อำนวยการฝ่ายสารสนเทศ

7.6 การจัดการระบบรักษาความปลอดภัยระบบเครือข่าย (Network Security Management)

จุดประสงค์เพื่อป้องกันข้อมูลในระบบเครือข่าย และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายของบริษัท

- ฝ่ายสารสนเทศ ต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติหรือการละเมิดความปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด
- ฝ่ายสารสนเทศ ต้องบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญและแจ้งให้หน่วยงานอื่น ๆ ที่เกี่ยวข้องทราบ กรณีที่มีการเปลี่ยนแปลงแก้ไขระบบเครือข่าย
- บริหารจัดการกิจกรรมที่เกี่ยวข้องให้เหมาะสมและต้องมั่นใจว่าสอดคล้องกับการควบคุมข้อมูลสารสนเทศที่ส่งผ่านเครือข่ายตลอดจนโครงสร้างพื้นฐานของบริษัทด้วย
- ระบบเครือข่ายทั้งหมดของบริษัทที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ Firewall หรือ ฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัสด้วย
- ฝ่ายสารสนเทศ ต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายของบริษัท และต้องกำหนดให้การเชื่อมต่อเข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะและติดต่อกับระบบงานที่กำหนดไว้เฉพาะเท่านั้น และควรกำหนดให้เครื่องคอมพิวเตอร์และระบบงานดังกล่าวแยกออกจากระบบเครือข่ายที่เป็นส่วนที่ใช้งานจริงของบริษัท ทั้งทางด้านกายภาพและทางด้าน Logical และต้องไม่อนุญาตให้หน่วยงานภายนอกมีสิทธิ์เข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่ายของบริษัทได้
- ห้ามผู้ใช้งานติดตั้งโมเด็มเข้ากับเครื่องคอมพิวเตอร์ของตน หรือต่อกับจุดใดก็ตามบนระบบเครือข่ายของบริษัท โดยไม่ได้รับอนุญาตจากฝ่ายสารสนเทศ
- ห้ามบุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใด ๆ จากภายนอกเข้ากับระบบคอมพิวเตอร์และระบบเครือข่ายของบริษัท โดยเด็ดขาด หากมีความจำเป็นต้องใช้งานต้องดำเนินการขออนุมัติตามระบบควบคุมสายงานของบริษัทก่อนทุกครั้ง
- ห้ามผู้ใช้งานติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย ตัวอย่าง Router, Switch, Hub และ Wireless Access Point โดยไม่ได้รับอนุญาตเด็ดขาด
- ห้ามผู้ใช้งานที่อยู่บนระบบเครือข่ายของบริษัททำการเชื่อมต่อออกไปยังเครือข่ายภายนอก ผ่านทางโมเด็มหรืออุปกรณ์เชื่อมต่ออื่นในขณะที่ยังเชื่อมต่ออยู่กับระบบเครือข่ายภายในบริษัทโดยเด็ดขาด

7.7 การจัดการสื่อที่ใช้ในการบันทึกข้อมูลให้มีความมั่นคงปลอดภัย (Media Handing)

จุดประสงค์ป้องกันความเสียหายที่อาจเกิดขึ้นกับสื่อที่ใช้ในการบันทึกข้อมูลของบริษัท

- ต้องกำหนดวิธีปฏิบัติและสิทธิ์สำหรับการบริหารและจัดการสื่อบันทึกข้อมูลที่สามารถถอดแยกได้ (Management of Removable Computer Media)
- การทำลายเอกสารและสื่อที่ใช้ในการบันทึกข้อมูล จะต้องได้รับการอนุมัติจากเจ้าของข้อมูล รวมทั้งบันทึกรายละเอียดอย่างเหมาะสม

- ให้ฝ่ายสารสนเทศ ทำการยกเลิกการใช้งาน USB Port เพื่อป้องกันความเสี่ยงที่อาจเกิดจากการนำสื่อบันทึกข้อมูลมาใช้งานภายในองค์โดยไม่ได้รับอนุญาต เมื่อมีความจำเป็นต้องใช้งานให้ทำการขออนุญาตการใช้งานเป็นรายกรณี
- ฝ่ายสารสนเทศ ต้องจัดเก็บเอกสารที่เกี่ยวกับระบบสารสนเทศ ของบริษัทอย่างปลอดภัย (Security of System Documentation)

7.8 การแลกเปลี่ยนข้อมูลสารสนเทศ (Exchange of Information)

จุดประสงค์เพื่อป้องกันการสูญหายของสารสนเทศและซอฟต์แวร์ รวมทั้งเพื่อป้องกันการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต หรือการนำสารสนเทศไปใช้ในทางที่ไม่เหมาะสม

- ให้ฝ่ายสารสนเทศ กำหนดวิธีการจัดส่งสื่อบันทึกข้อมูล (สารสนเทศหรือซอฟต์แวร์) ให้มีความมั่นคงปลอดภัย
- ให้ฝ่ายสารสนเทศ กำหนดวิธีการป้องกันการเข้าถึงข้อมูลอิเล็กทรอนิกส์รวมถึงการจัดส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบเครือข่าย
- ให้ฝ่ายสารสนเทศ กำหนดนโยบายและขั้นตอนการป้องกันการแลกเปลี่ยนข้อมูลระหว่างบริษัท

7.9 การบันทึกข้อมูลเหตุการณ์และการเฝ้าระวัง (Logging and Monitoring)

จุดประสงค์เพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

- การบันทึกข้อมูลแสดงเหตุการณ์ (Event Logging) ต้องจัดให้มีการบันทึกไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ โดยให้กำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าวและจัดเก็บหลักฐาน (Logs) ของระบบงานที่มีความสำคัญประเภทต่าง ๆ ดังต่อไปนี้

หลักฐานที่ต้องจัดเก็บ	รายละเอียดขั้นต่ำ	ระยะเวลาจัดเก็บขั้นต่ำ
หลักฐานการเข้าถึงพื้นที่หวงห้าม (physical access log)	บุคคลที่เข้าถึง	ไม่น้อยกว่า 90 วัน
	วันเวลาที่ผ่านเข้าออก	
	ความพยายามในการเข้าถึง (ถ้ามี)	
หลักฐานการเข้าถึงระบบปฏิบัติการ ฐานข้อมูลและระบบเครือข่ายคอมพิวเตอร์(authentication log)	บัญชีผู้ใช้งาน	ไม่น้อยกว่า 90 วัน
	วันเวลาที่เข้าใช้งาน	
	ความพยายามในการเข้าใช้งาน	
หลักฐานการเข้าถึงและใช้งานระบบสารสนเทศ (application log)	บัญชีผู้ใช้งาน	ไม่น้อยกว่า 90 วัน
	หมายเลขประจำเครื่องที่ใช้งาน (IP address, Mac address)	
	วันเวลาที่มีการใช้งาน	
หลักฐานการใช้งานอินเทอร์เน็ตผ่านระบบเครือข่ายคอมพิวเตอร์ภายใน (internet access log)	บัญชีผู้ใช้งาน	ไม่น้อยกว่า 90 วัน
	หมายเลขประจำเครื่องที่ใช้งาน (IP address, Mac	
	หมายเลขอินเทอร์เน็ต (organization IP address)	
	วันเวลาที่มีการใช้งาน	
	ที่อยู่ของเว็บไซต์ปลายทาง (full URL)	

หลักฐานการบริหาร (event log) ระบบปฏิบัติการและnetwork firewall	วันและเวลาที่เกิดเหตุการณ์	ไม่น้อยกว่า 90 วัน
	เหตุการณ์ที่เกิดขึ้นกับ OS (event services) เช่น สถานะการให้บริการของ service	
	เหตุการณ์ที่เกิดขึ้นกับ network firewall เช่นการ	
หลักฐานบันทึกข้อมูลจราจรคอมพิวเตอร์ของ network firewall (network firewall log)	วันและเวลา	ไม่น้อยกว่า 90 วัน
	IP address ต้นทาง (source) และปลายทาง	
	firewall action	
	port ที่ใช้ติดต่อ	
หลักฐานการจัดการบริหารข้อมูล (database log)	บัญชีผู้ใช้งาน	ไม่น้อยกว่า 90 วัน
	วันเวลาที่ข้าใช้งาน	

- การป้องกันข้อมูลล็อก (Protection of Log Information)
  - จำกัดสิทธิการเข้าถึงบันทึกเหล่านั้น อนุญาตให้เฉพาะเจ้าหน้าที่ที่ได้รับมอบหมายเท่านั้น เพื่อป้องกันข้อมูลระบบการบันทึกและจัดเก็บหลักฐานการใช้งานเกี่ยวกับระบบเทคโนโลยีสารสนเทศและการสื่อสารถูกเปลี่ยนแปลงแก้ไขทำความเสียหาย
  - ห้ามผู้ดูแลระบบแก้ไขข้อมูลจราจรคอมพิวเตอร์ (Log) ที่เก็บรักษาไว้
- ข้อมูลล็อกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and Operator Logs) กิจกรรมของผู้ดูแลระบบ และเจ้าหน้าที่ปฏิบัติการต้องมีการบันทึกไว้เป็นข้อมูลล็อกและมีการตรวจสอบอย่างสม่ำเสมอ และ ต้องเก็บบันทึกไว้อย่างน้อย 90 วัน นับตั้งแต่การใช้งานสิ้นสุดลง
- การตั้งนาฬิกาให้ถูกต้อง (Clock Synchronization) ต้องกำหนดระบบเวลาของอุปกรณ์ และระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีความสำคัญให้ตรงกับเวลาอ้างอิงสากล

7.10 การประชุมผ่านสื่ออิเล็กทรอนิกส์

จุดประสงค์เพื่อเป็นมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบควบคุมการประชุมผ่านสื่ออิเล็กทรอนิกส์

- การจัดประชุมผ่านสื่ออิเล็กทรอนิกส์ อย่างน้อยต้องมีกระบวนการดังนี้
  - การแสดงตนของผู้ร่วมประชุมผ่านสื่ออิเล็กทรอนิกส์ก่อนการประชุมให้ดำเนินการตามวิธีการที่ผู้มีหน้าที่จัดการประชุมกำหนด โดยอาจใช้เทคโนโลยีช่วยในการพิสูจน์และยืนยันตัวตนของผู้ร่วมประชุม
  - การสื่อสารหรือมีปฏิสัมพันธ์กันได้ด้วยเสียงหรือทั้งเสียงและภาพ ให้ดำเนินการด้วยช่องสัญญาณที่เพียงพอ รองรับการถ่ายทอดเสียง หรือทั้งเสียงและภาพได้อย่างชัดเจนและต่อเนื่อง รวมทั้งมีวิธีการในการจัดการสิทธิของผู้ร่วมประชุม
  - การเข้าถึงเอกสารประกอบการประชุมของผู้ร่วมประชุม ต้องแจ้งวิธีการที่ทำให้ผู้ร่วมประชุมสามารถเข้าถึงเอกสารประกอบการประชุม หรือข้อมูลที่เกี่ยวข้องกับการประชุมได้

- การลงคะแนนของผู้ร่วมประชุม หากเป็นการลงคะแนนทั่วไปให้มีวิธีการที่สามารถระบุตัวผู้ลงคะแนนและเจตนาของผู้ลงคะแนนได้ ส่วนการลงคะแนนลับ ให้มีวิธีการที่ทราบจำนวนของผู้ลงคะแนนและผลรวมของคะแนน โดยไม่สามารถระบุเจตนาของผู้ลงคะแนนแต่ละคนเป็นการทั่วไปได้
- กำหนดให้มีการจัดเก็บข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการประชุมผ่านสื่ออิเล็กทรอนิกส์ที่จำเป็น เช่น วิธีการแสดงตนหรือการลงคะแนน การแจ้งเหตุขัดข้องในการประชุม รวมทั้งข้อมูลจราจรอิเล็กทรอนิกส์ พร้อมกำหนดมาตรการเก็บรักษาด้วยวิธีการที่มีความมั่นคงปลอดภัยและด้วยวิธีการที่เชื่อถือได้
- การแจ้งเหตุขัดข้องในระหว่างการประชุม ให้ผู้มีหน้าที่จัดการประชุมจัดเตรียมช่องทางการแจ้งเหตุขัดข้องเพื่อรองรับการแก้ไขเหตุขัดข้องแก่ผู้ร่วมประชุม

ทั้งนี้ ในกรณีที่หน่วยงานใดมีการปฏิบัติงานที่เกี่ยวข้องกับการประชุมตามกฎหมายแตกต่างเป็นการเฉพาะแล้ว อาจเพิ่มเติมรายละเอียดที่แตกต่างนั้นได้

- การประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องลับ
  - ผู้มีหน้าที่จัดการประชุมต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยเพื่อป้องกันมิให้บุคคลที่ไม่มีสิทธิร่วมประชุมรู้หรือล่วงรู้ถึงข้อมูลการประชุมในเรื่องลับดังกล่าว
  - ผู้ร่วมประชุมผ่านสื่ออิเล็กทรอนิกส์ต้องรับรองต่อที่ประชุมว่าไม่มีบุคคลที่ไม่มีสิทธิร่วมประชุมสามารถรู้หรือล่วงรู้ถึงข้อมูลการประชุมในเรื่องลับ
  - การประชุมผ่านสื่ออิเล็กทรอนิกส์ในเรื่องที่มีชั้นความลับ ให้ใช้ระบบควบคุมการประชุมที่มีความมั่นคงปลอดภัยตามมาตรฐานที่กำหนดตามข้อ 24 โดยกรณีการประชุมในเรื่องที่มีชั้นความลับของหน่วยงานของรัฐ กำหนดเพิ่มเติมให้ต้องใช้ระบบควบคุมการประชุมที่ติดตั้งและให้บริการในราชอาณาจักร นอกจากนี้ ห้ามมิให้มีการบันทึกเสียงหรือทั้งเสียงและภาพของผู้ร่วมประชุมทุกคนตลอดระยะเวลาที่มีการประชุมในเรื่องลับ
- การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
  - มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการประชุมโดยทั่วไป
    - การธำรงไว้ซึ่งความลับ (confidentiality)
    - การธำรงไว้ซึ่งความถูกต้องครบถ้วน (integrity)
    - การธำรงไว้ซึ่งสภาพพร้อมใช้งาน (availability)
    - การคุ้มครองข้อมูลส่วนบุคคล ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability) ของข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้องหรือเกิดจากการประชุม ซึ่งเป็นไปตาม พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์

หมวด 8

การควบคุมการเข้าถึง (Access Control)

8.1 การควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirement for Access Control)

จุดประสงค์เพื่อควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศให้มีความมั่นคงปลอดภัย

- ฝ่ายสารสนเทศ ต้องจัดทำนโยบายและความต้องการในการ ใช้งานข้อมูลและระบบสารสนเทศ เพื่อควบคุมการเข้าถึงให้ทำได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- ฝ่ายสารสนเทศ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการเข้าใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน
- ผู้ดูแลระบบเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศได้
- ฝ่ายสารสนเทศ ต้องมีการบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท และเฝ้าระวังการละเมิดความปลอดภัย ที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ

8.2 นโยบายควบคุมการเข้าถึง (Access Control Policy) มีข้อปฏิบัติดังนี้

- บุคคล หรือ หน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าถึงข้อมูล และระบบเทคโนโลยีสารสนเทศและการสื่อสาร จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการฝ่ายสารสนเทศ หรือ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่แทน เป็นการล่วงหน้าอย่างน้อย 3 วันทำการ และจะกระทำได้ก็ต่อเมื่อได้รับการอนุมัติ โดยผู้อำนวยการฝ่ายสารสนเทศหรือ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่แทน
- ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่ต้องการใช้งานได้ ก็ต่อเมื่อได้รับอนุญาตจากเจ้าของข้อมูลตามความจำเป็นต่อการใช้งานเท่านั้น
- ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูล และระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้ง มีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ
- ผู้ดูแลระบบ หรือ ผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลได้
- ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึก และติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ
- ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาต และไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

- นโยบายควบคุมการเข้าถึงนี้ จะได้รับการทบทวนและปรับปรุง โดยฝ่ายสารสนเทศ ตามระยะเวลาอันสมควร หรือ ตามความจำเป็น

8.3 การจัดการการเข้าถึงระบบของผู้ใช้งาน (User Access Management)

จุดประสงค์เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์ใช้งานสามารถเข้าถึงระบบสารสนเทศได้

- การลงทะเบียนผู้ใช้งานใหม่ ต้องกำหนดให้มีระเบียบปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนผู้ใช้งานใหม่เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งระเบียบปฏิบัติสาหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในบริษัท เป็นต้น โดยปฏิบัติตามคู่มือการเข้าถึงระบบสารสนเทศของบริษัท โดยผู้ใช้งานต้องได้รับการทบทวน และพิจารณาอนุมัติตามขั้นตอนของบริษัทอย่างเคร่งครัด
- ต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบด้วย
- ผู้ดูแลระบบต้องกำหนดให้มีหลักเกณฑ์ในการยกเลิก การถอดถอนสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร และการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อผู้ใช้งานนั้นทำการลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง ฯลฯ หลังจากที่ได้รับแจ้งจากหน่วยงาน
- ผู้ใช้งานต้องได้รับการตรวจพิสูจน์ตัวตนทุกครั้งเมื่อทำการ Log-on เข้าสู่ระบบสารสนเทศ
- ฝ่ายสารสนเทศ ต้องบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัยอยู่เสมอ
- ฝ่ายสารสนเทศ ต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ปีละ 1 ครั้ง
- ให้มีการจัดเก็บบันทึกข้อมูลการเข้าถึงและการใช้งานระบบสารสนเทศแต่ละระบบ (Log Files) เป็นระยะเวลาอย่างน้อย 5 ปี

8.4 การรับผิดชอบหน้าที่ของผู้ใช้งาน (User Responsibilities)

จุดประสงค์เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์ สามารถเข้าถึงระบบสารสนเทศได้

- ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติ ตามที่กำหนดไว้ในเอกสาร 'การควบคุมการเข้าถึงสารสนเทศของบริษัท และการจัดการควบคุมการใช้รหัสผ่าน'
- เจ้าหน้าที่ต้องปฏิบัติตามการควบคุมการเข้าถึงสารสนเทศบริษัท การกำหนด การเปลี่ยนแปลงและการยกเลิกรหัสผ่านและการจัดการควบคุมการใช้รหัสผ่าน กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งาน หมายถึงผู้ใช้งานที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา
  - ควรได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาและผู้ดูแลระบบงานนั้น ๆ

- ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
- ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งานหรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น

- ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการดูแล รักษา User Name และรหัสผ่านของตนเอง รวมทั้งข้อมูลส่วนบุคคลที่อาจนำมาใช้เพื่อขอเปลี่ยนแปลงข้อมูลบัญชีการใช้งานระบบได้ ให้มีความมั่นคงปลอดภัยอย่างสม่ำเสมอ
- รหัสผ่านต้องได้รับการเปลี่ยนเมื่อเข้าใช้งานครั้งแรก และเปลี่ยนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดไว้ใน เอกสารขั้นตอนการปฏิบัติงานมาตรฐานการใช้รหัสผ่าน (Password Standard) รหัสผ่านต้องมีความมั่นคงปลอดภัยตามที่ได้กำหนดไว้ใน เอกสารขั้นตอนการปฏิบัติงานมาตรฐานการใช้รหัสผ่าน (Password Standard)
- รหัสผ่านถือเป็นข้อมูลลับ และเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านอย่างมั่นคงปลอดภัย ห้ามใช้ Account ร่วมกันหรือให้ผู้อื่นเข้าใช้งาน Account ของตนโดยเด็ดขาด ทั้งนี้ เมื่อเกิดความเสียหายเจ้าของรหัสผ่านต้องรับผิดชอบต่อความเสียหายนั้นทุกประการ
- ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่กระทำผ่าน User ID และรหัสผ่านของตนทั้งหมด หากผู้ใช้งานสงสัยว่า User ID หรือรหัสผ่านของตนถูกล่วงละเมิด ให้ผู้ใช้งานแจ้งเหตุต่อฝ่ายเทคโนโลยีสารสนเทศและทำการเปลี่ยนแปลงรหัสผ่านทั้งหมดทันที
- ผู้จัดการโครงการของระบบใหม่ที่เกิดขึ้นในบริษัทต้องตรวจสอบให้มั่นใจว่า ระบบในความดูแลของตนสอดคล้องกับเนื้อหาของนโยบายฉบับนี้ รวมถึงเอกสารสนับสนุนอื่น ๆ ที่เกี่ยวข้องทั้งหมด และต้องประสานงานกับผู้ดูแลระบบให้ทำการควบคุม และปรับแต่งค่าต่าง ๆ ของระบบให้เป็นไปตามข้อกำหนดที่เกี่ยวข้องทั้งหมดนี้ก่อนเริ่มนำมาใช้งานจริง
- การ Reset Password ต้องผ่านกระบวนการมาตรฐานของบริษัทเท่านั้น เพื่อให้มั่นใจว่าตรงกับ User ที่ต้องการ Reset รหัสผ่านจริง อีกทั้งเจ้าหน้าที่ที่ดูแลระบบมีสิทธิ์ในการขอข้อมูลและพิสูจน์ตัวตนของผู้ใช้งานตามความเหมาะสม ในทางกลับกัน ผู้ใช้งานอาจได้รับการร้องขอจากฝ่ายสารสนเทศ ให้ทำการเปลี่ยนรหัสผ่านใหม่ ในกรณีที่รหัสผ่านของผู้ใช้งานไม่มีความมั่นคงปลอดภัย สามารถถูกคาดเดา หรือถูกล่วงละเมิดได้ง่าย ทั้งนี้ ผู้ใช้งานต้องตรวจสอบความถูกต้องของแหล่งที่มาของคำร้องขอดังกล่าวด้วย เพื่อให้มั่นใจว่าการร้องขอนั้นไม่ได้เป็นการหลอกลวง
- ต้องกำหนดการป้องกันไม่ให้ผู้ไม่มีสิทธิ์เข้าถึงอุปกรณ์สำนักงานที่ไม่มีผู้ดูแล
- เจ้าหน้าที่ต้องกำหนดการควบคุมเอกสาร ข้อมูล หรือสื่อต่าง ๆ ที่มีข้อมูลสำคัญจัดเก็บ หรือบันทึกอยู่ ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือในสถานที่ไม่ปลอดภัยในขณะไม่ได้นำมาใช้งาน ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ (Desktop) ไม่ให้มีข้อมูลสำคัญ ปรากฏในขณะไม่ได้ใช้งาน

8.5 การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

จุดประสงค์เพื่อควบคุมการใช้บริการบนเครือข่ายของบริษัท

- ฝ่ายสารสนเทศ ต้องจัดทำแนวทาง/นโยบายควบคุมการเข้าถึงเครือข่ายและบริการบนเครือข่ายโดยเฉพาะเพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต
- สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ต้องมีการควบคุมการเข้า-ออก ที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ์และมีความจาเป็นผ่านเข้าใช้งานได้เท่านั้น
- ฝ่ายสารสนเทศ ต้องมีการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ และต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย
- ฝ่ายสารสนเทศ ต้องจัดแบ่งระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศที่มีการใช้งานแบ่งตามกลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ
- จัดแบ่งต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ต้องมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- ฝ่ายสารสนเทศ ต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น
- ฝ่ายสารสนเทศ ต้องจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน
- ระบบเครือข่ายคอมพิวเตอร์ภายในที่เชื่อมต่อกับระบบเครือข่ายอินเทอร์เน็ตต้องเชื่อมต่อผ่านระบบป้องกันเครือข่าย (Firewall) รวมทั้ง สามารถตรวจสอบการใช้งานในลักษณะที่ผิดปกติของผู้ใช้งานระบบเครือข่ายคอมพิวเตอร์
- ต้องควบคุมการเข้าถึงเครือข่ายและบริการบนเครือข่ายโดยเฉพาะ เพื่อรักษาความมั่นคงปลอดภัยให้แก่ข้อมูลและระบบเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ ใช้งานโปรโตคอลที่มั่นคงปลอดภัยในการบริหารจัดการระบบเครือข่าย เช่น Secure Socket Layer (SSL) Simple Network Management Protocol (SNMP)
- จำกัดการใช้งานเครือข่ายที่ส่งผลกระทบต่อ Bandwidth เช่น การรับ-ส่งไฟล์ขนาดใหญ่ยกเว้น กรณีที่ได้รับอนุญาตเห็นชอบเป็นลายลักษณ์อักษรจากผู้อำนวยการฝ่ายสารสนเทศ หรือ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่แทน
- ผู้ดูแลระบบเครือข่ายเท่านั้นที่มีสิทธิ์ หน้าที่เปลี่ยนแปลงแก้ไขระบบเครือข่ายเท่านั้น เช่น การเปลี่ยน IP Address , การแก้ไข VLAN
- ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์ หรือ อุปกรณ์มาใช้ในการปฏิบัติงานต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มขออนุญาตนำอุปกรณ์คอมพิวเตอร์มาใช้ในบริษัท

8.6 การควบคุมการใช้งานระบบปฏิบัติการ (Operating System Access Control)

จุดประสงค์เพื่อป้องกันการใช้งานระบบปฏิบัติการโดยไม่ได้รับอนุญาต

- ฝ่ายสารสนเทศ ต้องกำหนดกระบวนการในการเข้าถึงระบบให้มีความมั่นคงปลอดภัย เช่น กำหนดให้ระบบให้บริการจะปฏิเสธการใช้งานหากผู้ใช้พิมพ์รหัสผ่านผิดพลาดเกิน 3 ครั้ง เป็นต้น
- ฝ่ายสารสนเทศ ต้องกำหนดให้มีการพิสูจน์ตัวตนสำหรับผู้ใช้งานระบบเป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบ
- ฝ่ายสารสนเทศ ต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้ผู้ใช้งานระบบเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด
- ฝ่ายสารสนเทศ ต้องกำหนดให้มีการควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบ เพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่
  - ก่อนใช้ต้องทำการพิสูจน์ตัวตนก่อน
  - ให้ทำการแยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน
  - จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
  - ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้ อาทิ ผู้ใช้งานระบบ
- ฝ่ายสารสนเทศ ต้องมีวิธีการตัดเวลาการใช้งานเครื่องคอมพิวเตอร์ลูกข่าย เมื่อเครื่องคอมพิวเตอร์ลูกข่ายนั้นไม่ได้มีการใช้งานเป็นระยะเวลา หนึ่งอาทิ กลไกการล็อกหน้าจอ และต้องใช้รหัสผ่านในการเข้าสู่ระบบ

8.7 การควบคุมการติดตั้งซอฟท์แวร์บนระบบปฏิบัติการ (Control of Operational Software)

จุดประสงค์เพื่อป้องกันการติดตั้งซอฟท์แวร์โดยไม่ได้รับอนุญาต

- ควบคุมและจำกัดสิทธิการติดตั้งซอฟท์แวร์บนระบบปฏิบัติการ โดยผู้ใช้งานที่ไม่ได้รับอนุญาต เพื่อให้ระบบปฏิบัติงานมีความถูกต้องครบถ้วน และน่าเชื่อถือ
- การติดตั้งซอฟท์แวร์และแก้ไขเปลี่ยนแปลงโปรแกรมบนระบบปฏิบัติการใด ๆ ในเครื่องคอมพิวเตอร์ต้องได้รับการอนุญาตจากผู้อำนวยการฝ่ายสารสนเทศ หรือ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่แทน
- ผู้ดูแลระบบปฏิบัติการต้องทำการทดสอบการเจาะระบบ (penetration test) กับระบบงานที่มีความสำคัญที่เชื่อมต่อกับระบบเครือข่ายภายนอกก่อนทำการติดตั้งบนระบบปฏิบัติการใด ๆ เพื่อตรวจหาช่องโหว่ที่อาจเกิดขึ้น (Technical Vulnerability Management) ของซอฟแวร์ที่จะติดตั้งใหม่อย่างเหมาะสม
- ต้องมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี่ ซอฟต์แวร์อุดช่องโหว่ ลงในเครื่องที่ใช้งานหรือเครื่องให้บริการ โดยก่อนการติดตั้งในระบบจริงจะต้องผ่านการทดสอบ การใช้งานมาเป็นอย่างดี ว่าไม่ก่อให้เกิดปัญหากับเครื่องที่ให้บริการ
- ในกรณีที่มีการติดตั้ง feature เพิ่มเติมบนระบบงานปฏิบัติการเก่า ผู้ดูแลระบบต้องพิจารณาทำการทดสอบหาก feature ใหม่มีผลกระทบต่อระบบปฏิบัติการที่ใช้อยู่
- โปรแกรมคอมพิวเตอร์ตามมาตรฐานที่ฝ่ายสารสนเทศกำหนดให้สามารถติดตั้งได้มีดังนี้
  - ชุดโปรแกรมระบบปฏิบัติการ Microsoft Windows
  - ชุดโปรแกรมสำนักงาน Microsoft Office

- โปรแกรม Microsoft Team
- โปรแกรม Acrobat Reader
- โปรแกรมประเภท 7-Zip File
- โปรแกรม Anti-virus (Web root)
- โปรแกรมเขียนแผ่นข้อมูล (Nero Burning ROM)
- โปรแกรมประเภท Browser (Chrome)
- โปรแกรมประเภทให้ความช่วยเหลือ (Any Desk, Tight VNC)
- โปรแกรมเฉพาะที่ได้รับอนุญาตเป็นกรณี เช่น (SUN, HRMI, Microsoft SQL Studio Management)

8.8 **การควบคุมการใช้งานระบบสารสนเทศและข้อมูลสารสนเทศ** (Application and Information Access Control)

จุดประสงค์เพื่อป้องกันการใช้งานระบบสารสนเทศและข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

- ฝ่ายสารสนเทศ ต้องมีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิ์ในการใช้งาน อาทิ เขียน อ่าน ลบ ได้ กำหนดกลุ่มของผู้ใช้ที่สามารถ ใช้งานได้ ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้
- บัญชีผู้ใช้งานที่มีสิทธิ์การเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นและมีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น
- บุคคลภายนอก ต้องแสดงความยินยอมปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (ICT Security Policy) ของบริษัทอย่างเคร่งครัด ก่อนที่จะได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท
- ฝ่ายสารสนเทศ ต้องมีการแยกระบบสารสนเทศที่มีความสำคัญ หรือมีความเสี่ยงสูงไว้อีกบริเวณหนึ่ง เช่น การแบ่งระหว่างระบบที่เชื่อมต่ออินเทอร์เน็ตกับระบบอินทราเน็ตภายในที่ใช้งานในบริษัท เป็นต้น

8.9 **การควบคุมการเข้าถึงข้อมูลสารสนเทศ** (Information Technology Access Control)

จุดประสงค์เพื่อป้องกันการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

- สิทธิ์การเข้าถึงไฟล์ข้อมูลสารสนเทศต้องได้รับการควบคุม และได้รับการพิจารณาอนุมัติเท่าที่จำเป็นเท่านั้น เพื่อให้ไฟล์ข้อมูลสารสนเทศได้รับการรักษาความมั่นคงปลอดภัยอย่างมีประสิทธิภาพ รวมทั้งเป็นการแบ่งแยกสิทธิ์ และหน้าที่ของผู้ใช้งาน

8.10 **มาตรการควบคุมการเข้ารหัสข้อมูล** (Cryptographic Controls)

จุดประสงค์เพื่อควบคุมการใช้งานระบบ การเข้ารหัสข้อมูลที่คำนึงถึงชนิดและวิธีการเข้ารหัสข้อมูลที่สอดคล้องเหมาะสมกับ ระดับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลที่เป็นความลับ หรือ มีความสำคัญ

- ผู้ดูแลระบบต้องกำหนดรูปแบบ Wireless Security ให้เป็น WPA/WPA2 (WIFI Protected Access) ในการเข้ารหัสข้อมูลระหว่างเครื่องลูกข่าย (Wireless LAN Client) และอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point)
- การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup) ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีรหัสก่อนเข้าถึงข้อมูลสำรองที่สำคัญโดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสารองเหล่านั้นถูกเปิดเผย
- การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (E-Mail)เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูลที่ฝ่ายสารสนเทศกำหนดไว้ และให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail) ของผู้รับให้ถูกต้อง เพื่อป้องกันการส่งผิด
- การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายคอมพิวเตอร์สาธารณะ ควรได้รับการเข้ารหัสลับ (Encryption)ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML encryption เป็นต้น
- การนำเทคนิคการเข้ารหัสข้อมูลมาใช้ในการรับส่งข้อมูลสารสนเทศ ผ่านช่องทางการสื่อสารบางประเภทที่ต้องการรักษาความมั่นคงปลอดภัย เช่น การใช้งานระบบ Cloud Computing

8.11 คอมพิวเตอร์ประเภทพกพาและการปฏิบัติงานนอกสถานที่ (Mobile Computing)

จุดประสงค์เพื่อควบคุมการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทเคลื่อนที่ได้ รวมทั้งการปฏิบัติงานนอกสำนักงานให้เป็นไปอย่างปลอดภัย

8.11.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile Computing and Communication)

- อุปกรณ์ใด ๆ ที่ต้องนำไปใช้ในกิจกรรมภายนอกสถานที่ต้องได้รับการอนุมัติจากผู้บริหาร โดยอุปกรณ์ดังกล่าวต้องมีการควบคุมด้านความมั่นคงปลอดภัยในระดับเดียวกับอุปกรณ์ที่ใช้ภายใน
- เจ้าหน้าที่มีหน้าที่รับผิดชอบในดูแล และป้องกันอุปกรณ์พกพา และคอมพิวเตอร์พกพาที่ได้รับ
- ต้องมีการป้องกัน หรือ การล็อคอย่างเหมาะสมเมื่อไม่ได้ใช้งานภายในบริษัท
- ต้องไม่วางอุปกรณ์ไว้ในที่สาธารณะโดยที่ไม่มีคนดูแล
- ต้องมีการตรวจสอบความพร้อมของคอมพิวเตอร์และอุปกรณ์ที่จะนำไปใช้งาน ว่าอยู่ในสภาพพร้อมใช้งาน หรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์ หรือ ไม่
- ต้องติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ (Antivirus) บนอุปกรณ์พกพา และทำการปรับปรุงข้อมูลไวรัส (Virus Pattern) ให้ทันสมัยอยู่เสมอ
- ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

- เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที
- เจ้าหน้าที่รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย
- หากปรากฏความเสียหายที่เกิดขึ้นนั้น เกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

8.11.2 การปฏิบัติงานจากภายนอกบริษัท (Teleworking)

- การควบคุมการเข้าใช้งานระบบจากภายนอกบริษัท ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้เหมือนในบริษัท เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก ป้องกันข้อมูลที่ได้รับการเข้าถึง การประมวลผลหรือ การจัดเก็บจาก สถานที่ที่มีการปฏิบัติงานจากระยะไกล มีแนวทางปฏิบัติ ดังนี้
  - การเข้าสู่ระบบระยะไกล (Remote Access) สู่ระบบเครือข่ายคอมพิวเตอร์ ต้องควบคุมบุคคลที่จะเข้าสู่ระบบจากระยะไกล โดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน
  - วิธีการใด ๆ ก็ตามที่สามารถเข้าถึงข้อมูล หรือ ระบบข้อมูลจากระยะไกล ต้องได้รับการอนุมัติจากผู้อำนวยการฝ่ายสารสนเทศก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดในการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด
  - การให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐาน ระบุเหตุผล หรือ ความจำเป็นในการดำเนินงานกับฝ่ายสารสนเทศอย่างเพียงพอ และต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ
  - มีการควบคุม Port ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุมและไม่ควรเปิดพอร์ตทิ้งไว้โดยไม่จำเป็นควรตัดการเชื่อมต่อเมื่อไม่ได้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น
  - การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น
- การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก มีการตรวจสอบการทำงานอย่างเคร่งครัด โดยผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบ ต้องผ่านการพิสูจน์ตัวตนจากระบบเทคโนโลยีสารสนเทศและการสื่อสารที่กำหนด แต่ละระบบ ดังนี้
  - แสดงชื่อผู้ใช้งาน (Username)
  - ใส่รหัสผ่าน (Password)

หมวด 9

การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information System Acquisition, Development and Maintenance)

9.1 การกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems)

จุดประสงค์เพื่อการสร้างความปลอดภัยให้กับระบบสารสนเทศ

- ฝ่ายสารสนเทศ ต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยไว้อย่างชัดเจนในระบบที่จะพัฒนาขึ้นมาใช้งาน หรือซื้อมาใช้งาน
- หน่วยงานดูแลระบบเทคโนโลยีสารสนเทศ จะต้องทำการวิเคราะห์ระบบเทคโนโลยีสารสนเทศ ว่ามีความเสี่ยงใดบ้างที่จะทำให้ข้อมูลเกิดความเสียหาย โดยมุ่งเน้นในส่วนต่าง ๆ ดังนี้
  - มาตรการปฏิบัติก่อนที่จะเกิดความเสียหาย อาทิ การสำรองข้อมูล ระบบเครือข่ายสำรอง
  - มาตรการปฏิบัติหลังจากเกิดความเสียหาย อาทิ แผนการกู้คืนข้อมูล ระยะเวลาในการกู้คืนข้อมูล

9.2 การประมวลผลระบบสารสนเทศ (Correct Processing in Applications)

จุดประสงค์เพื่อป้องกันความผิดพลาดของระบบสารสนเทศ จากความถูกต้องของข้อมูล การสูญหายและการแก้ไขอย่างไม่ถูกต้อง

- ผู้พัฒนาระบบสารสนเทศ ต้องตรวจสอบข้อมูลนำเข้าระบบสารสนเทศ ได้แก่ ตรวจสอบช่วงของค่าตัวเลขที่ใส่เข้ามา ตรวจสอบแต่ละตัวอักษรที่ใส่เข้ามา ตรวจสอบว่าข้อมูลใส่เข้ามาครบทุกฟิลด์ เป็นต้น เพื่อตรวจสอบความครบถ้วนและไม่ก่อให้เกิดความเสียหายต่อระบบ
- ผู้พัฒนาระบบสารสนเทศต้องวิเคราะห์ความเสี่ยงที่ทำให้ข้อมูลเสียหาย (Areas of Risk) ทำการวิเคราะห์ว่ามีความเสี่ยงใดบ้างที่อาจทำให้ข้อมูลเกิดความเสียหาย
- ผู้พัฒนาระบบสารสนเทศต้องมีวิธีการตรวจสอบการประมวลข้อมูลสารสนเทศ (Checks and Controls) ว่ามีข้อผิดพลาดหรือไม่
- ผู้พัฒนาระบบสารสนเทศต้องมีวิธีการตรวจสอบการส่งข้อมูลในระบบสารสนเทศ เพื่อให้แน่ใจว่าข้อมูลในระบบสารสนเทศมีความปลอดภัยและมีความถูกต้องสมบูรณ์
- ผู้พัฒนาระบบสารสนเทศต้องมีขั้นตอนการตรวจสอบ ทดสอบและประมวลผล เพื่อให้มั่นใจว่าระบบสามารถใช้ได้จริงและมีผลลัพธ์ที่ถูกต้อง

9.3 ความมั่นคงปลอดภัยของแฟ้มข้อมูลระบบ (Security of System Files)

จุดประสงค์เพื่อให้โครงการสารสนเทศได้รับการดำเนินการอย่างปลอดภัย

- ผู้พัฒนาระบบสารสนเทศต้องมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี่ ซอฟต์แวร์อุดช่องโหว่ลงในเครื่องที่ใช้งานหรือเครื่องให้บริการ โดยก่อนการติดตั้งในระบบจริงจะต้องผ่านการทดสอบการใช้งานมาเป็นอย่างดีว่าไม่ก่อให้เกิดปัญหากับเครื่องที่ให้บริการอยู่
- ข้อมูลจริงที่จะนำไปใช้ในการทดสอบระบบจะต้องได้รับอนุญาตจากผู้รับผิดชอบในการรักษาข้อมูลนั้น ๆ ก่อน เมื่อใช้งานเสร็จ จะต้องทำการลบข้อมูลจริงออกจากระบบทดสอบทันที และทำการบันทึกไว้เป็นหลักฐานว่าได้นำข้อมูลจริงไปใช้ในการทดสอบอะไรบ้าง รวมถึงวัน เวลา และหน่วยงานที่ทดสอบ แจ้งไปยังผู้รับผิดชอบในการรักษาข้อมูลนั้นอีกครั้ง
- ผู้พัฒนาระบบสารสนเทศต้องจัดให้มีการควบคุมการเข้าถึง Source Code ของระบบที่ ใช้งานจริงหรือให้บริการ เช่น
  - ไม่ควรเก็บ Source Code ไว้ในเครื่องที่ใช้งานจริงและต้องเก็บ Source Code ไว้ในที่ที่ปลอดภัย
  - ต้องไม่เก็บ Source Code ที่อยู่ในระหว่างทำการทดสอบรวมไว้กับ Source Code ที่ ใช้งานได้จริงแล้ว

9. 4 **ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ** (Security in Development and Support Processes)

จุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศ รวมทั้งข้อมูลสารสนเทศในระบบด้วย

- ผู้พัฒนาระบบสารสนเทศต้องมีกระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริง หรือให้บริการอยู่แล้ว อาทิ
  - คำขอให้แก้ไขต้องมาจากผู้ที่มีสิทธิ์
  - ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ
  - ต้องมีการควบคุมผลข้างเคียงที่อาจเกิดขึ้นหลังจากมีการแก้ไข
  - เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจ
  - ต้องเก็บรายละเอียดของคำขอไว้
- เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลงซอฟต์แวร์ต่าง ๆ ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบและทดสอบว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัย
- เมื่อมีการใช้งานซอฟต์แวร์สำเร็จรูปต้องมีการควบคุมการเปลี่ยนแปลงเท่าที่จำเป็น และการเปลี่ยนแปลงทั้งหมดจะต้องถูกทดสอบและจัดทำเป็นเอกสารเพื่อให้สามารถนำมาใช้งานได้เมื่อมีการปรับปรุงซอฟต์แวร์ในอนาคต ผู้พัฒนาระบบสารสนเทศต้องมีการป้องกันโอกาสการรั่วไหลของข้อมูล อาทิ การดักจับข้อมูลจากสายสัญญาณภายนอกบริษัท การปลอมแปลง การใช้ซอฟต์แวร์ที่มีความเสี่ยงในการรั่วไหลของข้อมูล
- ในการทำสัญญาว่าจ้างการพัฒนาระบบของบริษัทต้องมีความชัดเจนและครอบคลุมถึงสัญญาทางด้านลิขสิทธิ์ซอฟต์แวร์ การใช้ระบบ การตรวจสอบระบบ โดยละเอียดก่อนติดตั้งใช้งานจริง รวมถึงการรับรองคุณภาพของระบบ และการกำหนดขอบเขตในการจ้างพัฒนาระบบ

9. 5 การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)

จุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศ รวมทั้งสารสนเทศในระบบด้วย เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ

9.5.1 แนวทางดำเนินการการบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

- กำหนดผู้มีหน้าที่รับผิดชอบในการจัดการเกี่ยวกับช่องโหว่ทางเทคนิค โดยครอบคลุมถึงการประเมินความเสี่ยงของทรัพย์สินระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เกี่ยวข้อง
- มีการติดตามข้อมูลข่าวสารเกี่ยวกับช่องโหว่ทางเทคนิคที่อาจเป็นความเสี่ยงต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร อย่างทันต่อเหตุการณ์
- มีการประเมินช่องโหว่ของระบบ (vulnerability assessment) กับระบบงานที่มีความสำคัญทุกระบบอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ และรายงานผลไปยังหน่วยงานกำกับ
- ติดตามข้อมูลข่าวสารเกี่ยวกับช่องโหว่ทางเทคนิคที่อาจเป็นความเสี่ยงต่อระบบสารสนเทศอย่างทันต่อเหตุการณ์ รวมทั้ง มีมาตรการดำเนินการเพื่อปิดช่องโหว่ หรือ กำหนดแผนรองรับกรณีที่ระบบถูกบุกรุกผ่านช่องโหว่ดังกล่าวโดยควรกำหนดแนวทางดำเนินการดังนี้
  - กำหนดผู้มีหน้าที่รับผิดชอบในการจัดการเกี่ยวกับช่องโหว่ทางเทคนิคโดยครอบคลุมถึงการประเมินความเสี่ยงของทรัพย์สินสารสนเทศที่เกี่ยวข้องซึ่งอาจได้รับผลกระทบจากช่องโหว่ดังกล่าวโดยเฉพาะทรัพย์สินสารสนเทศที่มีความเสี่ยงสูง การดำเนินการเพื่อปิดช่องโหว่ (patching) และการประสานงานกับบุคคลที่เกี่ยวข้อง
  - จัดให้มีการปิดช่องโหว่ที่พบโดยไม่ชักช้า โดยควรมีการประเมินความเสี่ยงของโปรแกรมเพื่อปิดช่องโหว่ (patches) ก่อนการติดตั้งโปรแกรมเพื่อทดสอบและประเมินผลกระทบที่อาจเกิดจากการติดตั้งโปรแกรมดังกล่าว
  - กรณีที่ไม่มีโปรแกรมเพื่อปิดช่องโหว่ ให้ปฏิบัติตามคำแนะนำของบริษัทผู้ผลิตทรัพย์สินสารสนเทศที่เกี่ยวข้อง
- มีการบันทึกและจัดเก็บหลักฐานเพื่อการตรวจสอบในการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับการจัดการช่องโหว่ทางเทคนิค

9.5.2 การจำกัดการติดตั้งซอฟท์แวร์ (Restrictions on Software Installation)

- ผู้ใช้งานต้องปฏิบัติตามกฎเกณฑ์ควบคุมการติดตั้งซอฟท์แวร์ ไม่ติดตั้งซอฟท์แวร์ที่ละเมิดลิขสิทธิ์ในเครื่องคอมพิวเตอร์

- ต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับ ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้อง หรือไม่
- ไม่ควรจะติดตั้ง โปรแกรมใด ๆ ลงในเครื่องคอมพิวเตอร์ของบริษัท โดยไม่ได้รับการอนุญาต
- กำหนดให้มีการตรวจสอบเครื่องคอมพิวเตอร์ของบริษัทอย่างน้อยปีละ 1 ครั้งเพื่อตรวจดูรายการของซอฟต์แวร์ในเครื่องคอมพิวเตอร์ และเพื่อให้แน่ใจว่ามีใบอนุญาตการใช้งานสำหรับผลิตภัณฑ์ซอฟต์แวร์แต่ละตัวในเครื่องคอมพิวเตอร์ ถ้าพบว่ามีซอฟต์แวร์ที่ไม่ได้รับอนุญาต ซอฟต์แวร์เหล่านั้นจะถูกลบทิ้ง และถ้าหากมีความจำเป็นฝ่ายสารสนเทศอาจจะมีการพิจารณาให้นำซอฟต์แวร์ที่มี ใบอนุญาตอย่างถูกต้องอื่นมาใช้แทนซอฟต์แวร์ดังกล่าวได้

หมวด 10

การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท

(Information security incident management)

10.1 การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคง (Reporting Information Security Events and Weaknesses)

จุดประสงค์เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของบริษัทได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

- เจ้าหน้าที่และผู้ใช้งานทุกคนต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท และฝ่ายสารสนเทศ จะต้องดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้ เพื่อเตรียมการในการรองรับเหตุการณ์ผิดปกติที่อาจเกิดขึ้น
- ให้ฝ่ายสารสนเทศ ทำหน้าที่เป็นศูนย์กลางประสานงานและดำเนินการแก้ไขปัญหาที่เกิดจากเหตุการณ์ผิดปกติและเพื่อประโยชน์ในการนี้ ให้ดำเนินการดังต่อไปนี้
- จัดตั้งคณะทำงานขึ้นชุดหนึ่งเรียกว่า "คณะทำงานเพื่อแก้ไขปัญหาจากเหตุการณ์ผิดปกติ" เพื่อทำหน้าที่
  - จัดทำแผนฉุกเฉินรองรับเหตุการณ์ผิดปกติที่อาจเกิดขึ้น ประสานงานกับส่วนงานที่เกี่ยวข้อง และดำเนินการแก้ไขปัญหาเมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น
  - กำหนดวิธีปฏิบัติในการแก้ไขปัญหาจากเหตุการณ์ผิดปกติที่เกิดขึ้น เพื่อเป็นแนวทางสำหรับผู้ใช้งานและคณะทำงาน
  - ประเมินวิธีปฏิบัติในการแก้ไขปัญหาจากเหตุการณ์ผิดปกติทุก 1 ปี และ ปรับปรุงแก้ไขวิธีปฏิบัติให้เหมาะสม หากพบข้อบกพร่อง
- ให้ส่วนงานต่าง ๆ ให้ความร่วมมือและประสานงานกับฝ่ายสารสนเทศ และและคณะทำงานในการจัดทำแผนฉุกเฉิน และการแก้ไขปัญหาเมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น
- ผู้ใช้งานและบุคคลภายนอกทุกคนมีหน้าที่รายงานเหตุละเมิดความมั่นคงปลอดภัย จุดอ่อน หรือการกระทำที่ไม่เหมาะสมใด ๆ ที่เกิดขึ้น หรือต้องสงสัยว่าเกิดขึ้นภายในบริษัทต่อผู้บังคับบัญชา หรือหน่วยงานจัดการความปลอดภัย (Security Management) ทันทีที่พบเหตุ เพื่อให้สามารถดำเนินการแก้ไขปัญหาได้อย่างทันท่วงที
- ผู้ใช้งานที่พบหรือรับทราบถึงการทำงานที่ผิดปกติ ข้อผิดพลาด หรือจุดอ่อนของซอฟต์แวร์ ต้องรายงานต่อคณะทำงานเพื่อแก้ไขปัญหาจากเหตุการณ์ผิดปกติทันที
- ผู้ใช้งานที่พบว่าฮาร์ดแวร์หรืออุปกรณ์ใด ๆ เกิดความเสียหาย หรือทำงานผิดปกติ ต้องรายงานต่อคณะทำงานเพื่อแก้ไขปัญหาจากเหตุการณ์ผิดปกติทันที
- ผู้ใช้งานและบุคคลภายนอกที่พบเหตุละเมิดความมั่นคงปลอดภัยหรือจุดอ่อนใด ๆ ในบริษัทต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้น ผู้บังคับบัญชา หน่วยงานจัดการความปลอดภัย (Security Management) และห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยนั้นด้วยตนเอง

- การกระทำอื่น ๆ ที่ถือเป็นข้อห้ามของบริษัทมีดังนี้
  - การกระทำใด ๆ ที่กฎหมายบัญญัติว่าเป็นความผิด ตลอดจนการกระทำในลักษณะอื่น ๆ ที่กล่าวถึงด้านล่างนี้ถือเป็นข้อห้ามของบริษัทไม่ยินยอมให้เจ้าหน้าที่ดำเนินการโดยเด็ดขาด ทั้งนี้บริษัทมิได้เขียนระบุถึงข้อห้ามทั้งหมดที่ห้ามกระทำไว้ แต่เขียนเพื่อเป็นแนวทางให้แก่ผู้ใช้งานได้รับทราบเท่านั้น

    หมายเหตุ : เจ้าหน้าที่บางส่วนอาจได้รับยกเว้นจากข้อห้ามบางข้อที่กล่าวไว้ด้านล่างนี้ (ตราบเท่าที่ไม่ขัดต่อกฎหมาย) หากเป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย เช่น ผู้ดูแลระบบสามารถระงับการเข้าถึงระบบเครือข่ายของอุปกรณ์ใด ๆ หากการเข้าถึงนั้นรบกวนการทำงานของระบบเทคโนโลยีสารสนเทศ
  - การใช้งานทรัพยากรของบริษัทเพื่อการจัดหาหรือส่งต่อ วัสดุ เอกสาร หรือรูปภาพลามกอนาจาร หรือที่ขัดต่อกฎหมาย
  - การฉ้อโกงโดยใช้ User ID และรหัสผ่านที่บริษัทกำหนดให้ เพื่อเสนอขายสินค้าหรือบริการใด ๆ
  - การพยายามล่วงละเมิดความมั่นคงปลอดภัย หรือรบกวนการทำงานของระบบเครือข่าย ตัวอย่างของการล่วงละเมิดความมั่นคงปลอดภัย ได้แก่ การเข้าถึงข้อมูลหรือเครื่องคอมพิวเตอร์แม่ข่ายที่ตนไม่ได้รับอนุญาต เป็นต้น ส่วนตัวอย่างของการรบกวนการทำงานของระบบเครือข่าย ได้แก่ Sniffing, Pinged Floods, Pack Spoofing, Denial of Service และ Forged Routing Information ด้วยเจตนามุ่งร้าย เป็นต้น
  - การใช้งาน Bandwidth จำนวนมากโดยเฉพาะอย่างยิ่งการใช้งานโปรแกรมประเภท P2P File Sharing
  - การทำ Port Scanning และ Security Scanning เว้นแต่เป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย
  - การดักฟังหรือดักจับข้อมูลที่เจ้าหน้าที่ไม่ได้รับอนุญาตให้รับรู้ด้วยวิธีการใด ๆ เว้นแต่เป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย
  - การค้นหาจุดบกพร่องของระบบ เพื่อทำการเข้าถึงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต
  - การหลบเลี่ยงการพิสูจน์ตัวตนผู้ใช้งานหรือมาตรการด้านความมั่นคงปลอดภัยของคอมพิวเตอร์ ระบบเครือข่ายใด ๆ
  - การใช้โปรแกรม/สคริปต์/คำสั่ง หรือการส่งข้อความใด ๆ โดยมีเจตนารบกวน ลดประสิทธิภาพการให้บริการ หรือระงับการใช้งานของผู้ใช้งาน ทั้งโดยผ่านระบบภายใน หรือผ่านระบบเครือข่ายต่าง ๆ
  - การให้ข้อมูลลับเกี่ยวกับรายชื่อเจ้าหน้าที่ รายชื่อลูกค้า ความลับของ บริษัทและข้อมูลลับอื่น ๆ แก่บุคคลภายนอก
  - การข่มขู่คุกคามทุกรูปแบบผ่านอีเมล์ โทรศัพท์ หรือระบบส่งข้อความ ไม่ว่าจะด้วยภาษา ความถี่ หรือขนาดของข้อความการแสดงความคิดเห็น หรือส่งข้อความใด ๆ ที่ไม่เกี่ยวข้องกับการทำงานไปหาบุคคลจำนวนมาก (Newsgroup Spam)
  - การละเมิดสิทธิส่วนบุคคล ลิขสิทธิ์ของบริษัท ความลับของบริษัท สิทธิบัตร ทรัพย์สินทางปัญญา หรือกฎหมายอื่นใด

- คณะทำงานเพื่อแก้ไขปัญหาจากเหตุการณ์ผิดปกติต้องบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัทที่สังเกตุพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่

10.2 **การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย** (Management of Information Security Incidents and Improvements)

จุดประสงค์เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศ

- คณะทำงานเพื่อแก้ไขปัญหาจากเหตุการณ์ผิดปกติต้องกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยและขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี
- คณะทำงานเพื่อแก้ไขปัญหาจากเหตุการณ์ผิดปกติต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายเกิดขึ้นจากความเสียหาย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า
- คณะทำงานเพื่อแก้ไขปัญหาจากเหตุการณ์ผิดปกติต้องรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่ง

หมวด 11

การบริหารความต่อเนื่องในการดำเนินงานของบริษัท

(Business Continuity Management)

11.1 การบริหารความต่อเนื่องในการดำเนินงานของบริษัท

จุดประสงค์เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่าง ๆ ทางด้านการปฏิบัติงานของบริษัท เพื่อป้องกันกระบวนการทางด้านการปฏิบัติงานของบริษัทที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบเทคโนโลยีสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

- กำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับการปฏิบัติงานของบริษัท การบริหารจัดการและการปรับปรุงกระบวนการดังกล่าวอย่างสม่ำเสมอ
- กำหนดให้มีการทดสอบกระบวนการในการสร้างความต่อเนื่องให้กับการปฏิบัติงานของบริษัท อย่างน้อยปีละ 1 ครั้ง

หมวด 12

การปฏิบัติตามข้อกำหนด (Compliance)

12.1 การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย(Compliance with Legal Requirements)

จุดประสงค์เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง พระราชบัญญัติ ระเบียบข้อบังคับรวมทั้งสัญญาต่าง ๆ

- ฝ่ายสารสนเทศ ต้องมีการศึกษาและกำหนดรายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศ
- พนักงานทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารที่กำหนดขึ้นอย่างเคร่งครัด โดยมีรายการดังต่อไปนี้เป็นอย่างน้อย
  - นโยบายการรักษาความมั่นคงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
  - พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
  - พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์
  - พ.ร.ฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ
  - พ.ร.บ. ลิขสิทธิ์
  - พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์
  - พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

- ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศของบริษัท ถือเป็นทรัพย์สินของบริษัท (ยกเว้น ข้อมูลที่เป็นทรัพย์สินของลูกค้า หรือบุคคลภายนอกรวมถึงซอฟต์แวร์ หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตร หรือลิขสิทธิ์ของบุคคลภายนอก) ทั้งนี้ บริษัทสามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า
- เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัท ขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบเครือข่ายของผู้ใช้งานเพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่นโยบายต่าง ๆ ที่กำหนดไว้ ตลอดจนการเข้าถึง ทบทวน และตรวจสอบ E-mal ของผู้ใช้งานโดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า อย่างไรก็ตามการตรวจสอบดังกล่าวจะดำเนินการต่อเมื่อมีความจำเป็นเท่านั้น และจะไม่เปิดเผยข้อมูลใด ๆ ของผู้ใช้งาน เว้นแต่เป็นการเปิดเผยตามคำสั่งศาล ตามบทบังคับของกฎหมาย หรือด้วยความยินยอมจากผู้ใช้งานเท่านั้น
- ห้ามพนักงานทุกคนใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศของบริษัท กระทำการใด ๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทย และกฎหมายระหว่างประเทศไม่ว่าโดยกรณีใดก็ตาม
- ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานทรัพย์สินทางปัญญาที่หน่วยงานจัดหามาใช้งานและต้องระมัดระวังที่จะไม่ละเมิด
- ต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด (Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อ ใช้งานซอฟต์แวร์ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไม่
- ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของบริษัท โดยเด็ดขาด
- เพื่อที่จะให้เกิดความแน่ใจว่าพนักงาน มิได้ละเมิดลิขสิทธิ์โดยไม่ได้ตั้งใจ หรือพลั้งเผลอ จึงไม่ควรจะทำสำเนาซอฟต์แวร์ใด ๆ ที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์ของบริษัท เพื่อจุดประสงค์ใด ๆ ก็ตาม โดยที่ไม่ได้รับอนุญาต
- กำหนดสิทธิ์ในการเข้าถึงข้อมูลที่สำคัญ หรือ ข้อมูลความลับ เพื่อป้องกันการเข้าถึงและแก้ไขเปลี่ยนแปลงข้อมูลโดยผู้ที่ไม่มีสิทธิ์ หรือ ไม่ได้รับอนุญาต ทั้งนี้ ต้องเพียงพอสำหรับใช้ในการทำงานปกติและสอดคล้องกับหน้าที่การปฏิบัติงานของเจ้าหน้าที่ที่เกี่ยวข้อง การควบคุมที่มีประสิทธิภาพจะต้องสามารถป้องกันและจำกัดการเข้าถึงตามที่สิทธิ์ที่กำหนดไว้ได้
- ความเป็นส่วนตัว และการป้องกันข้อมูลส่วนบุคคล (Privacy and Protection of Personal Identifiable Information) ต้องจัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมาย หลักเกณฑ์ และข้อกำหนดตามสัญญาต่าง ๆ
- ระเบียบข้อบังคับสำหรับมาตรการเข้ารหัสข้อมูล (Regulation of Cryptographic Controls) ต้องควบคุมการเข้ารหัสข้อมูลให้สอดคล้องกับกฎหมาย หลักเกณฑ์ และข้อกาหนดตามสัญญาต่าง ๆ

12.2 **การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยและรายละเอียดทางเทคนิค** (Reviews of Security Policy and Technical Compliance)

จุดประสงค์เพื่อตรวจสอบระบบให้มีความสอดคล้องกับนโยบายความมั่นคงปลอดภัย

- ฝ่ายงานเทคโนโลยีสารสนเทศต้องจัดให้มีการตรวจสอบระบบทั้งหมดของหน่วยงานตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและระยะเวลาที่กำหนดไว้
- ฝ่ายงเทคโนโลยีสารสนเทศต้องตรวจสอบรายละเอียดทางเทคนิคของระบบที่ใช้งาน หรือให้บริการอยู่แล้วตามระยะเวลาที่กำหนดไว้ว่ามีความมั่นคงปลอดภัยสารสนเทศอย่างพอเพียงหรือไม่ ได้แก่ การตรวจดูว่าระบบสามารถถูกบุกรุกได้หรือไม่ การปรับแต่งค่าพารามิเตอร์ที่ระบบ ใช้งานเป็นไปอย่างปลอดภัยหรือไม่ รวมทั้งมีการตรวจสอบระบบโดยทำการใช้ซอฟต์แวร์ค้นหาช่องโหว่ (Vulnerability Scanning) และทดสอบการโจมตีระบบ (Penetration Test) เพื่อตรวจสอบข้อบกพร่องของระบบ

12.3 **การพิจารณาการตรวจสอบระบบสารสนเทศ** (Information System Audit Considerations)

จุดประสงค์เพื่อทำให้กระบวนการตรวจสอบระบบสารสนเทศทั้งหมดมีผลกระทบน้อยที่สุดต่อการดำเนินงานของฝ่ายสารสนเทศ

- ฝ่ายสารสนเทศ ต้องวางแผนการตรวจสอบระบบทั้งหมด โดยการตรวจสอบที่จะดำเนินการจะต้องมีผลกระทบต่อระบบ และกระบวนการดำเนินงานของฝ่ายน้อยที่สุด
- ฝ่ายสารสนเทศ ต้องมีการป้องกันซอฟต์แวร์ที่ใช้ในการตรวจสอบระบบ มิให้มีการนำซอฟต์แวร์ไปใช้ในทางที่ผิด หรือป้องกันข้อมูลสำคัญที่เป็นผลลัพธ์จากการตรวจสอบโดยซอฟต์แวร์นั้น

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารฉบับนี้ ได้รับการอนุมัติทบทวนจากที่ประชุมคณะกรรมการบริหาร ครั้งที่ 9/2567 เมื่อวันที่ 26 กันยายน 2567 โดยมีผลบังคับใช้ตั้งแต่วันที่ 26 กันยายน 2567 เป็นต้นไป

(นายสรสิทธิ์ สุนทรเกศ)
ประธานกรรมการบริษัท