นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

Information Technology Security Policy

บริษัท เมเจอร์ ซีนีเพล็กซ์ กรุ๊ป จำกัด (มหาชน)

และ/หรือ กลุ่มบริษัทเมเจอร์

ประวัติการเปลี่ยนแปลงเอกสาร

Version No.	Date of Change	A/M/ D*	Owner	Description of Changes	Reviewed by	Approved by
Version 1				IT Director	Head of IT	BOD

**A = Added, M = Modified, D = Deleted*

สารบัญ

Contents

1. บทนำ 4

1.1 ขอบเขต 4

1.2 วัตถุประสงค์ 4

2. คำนิยาม 5

3. โครงสร้างการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและบทบาทหน้าที่ความรับผิดชอบ 9

3.1 โครงสร้างการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ 9

3.2 บทบาทหน้าที่ความรับผิดชอบ 10

4. นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ 13

5. องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ 14

หมวดที่ 1 การจัดการนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policies) 14

หมวดที่ 2 โครงสร้างการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Organization of IT Security) 15

หมวดที่ 3 ความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resource Security) 16

หมวดที่ 4 การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management) 17

หมวดที่ 5 การควบคุมการเข้าถึง (Access Control) 20

หมวดที่ 6 การเข้ารหัสข้อมูล (Cryptography) 23

หมวดที่ 7 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security) 24

หมวดที่ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security) 27

หมวดที่ 9 การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications Security) 32

หมวดที่ 10 การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ (System Acquisition and Development and Maintenance) 36

หมวดที่ 11 การบริหารจัดการสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security Incident Management) 38

หมวดที่ 12 การบริหารการจัดการด้านการบริหารหรือดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง (Information Security Business Continuity Management) 39

หมวดที่ 13 การปฏิบัติตามกฎเกณฑ์ด้านเทคโนโลยีสารสนเทศ (Compliance with IT Regulations) 41

6. การยกเว้นนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ 42

7. การสื่อสารนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ 42

8. การทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ 42

9. บทลงโทษ 43

10. เอกสารอ้างอิง 43

Appendix 1 44

นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

1. บทนำ

บริษัท เมเจอร์ ซีนีเพล็กซ์ กรุ๊ป จำกัด (มหาชน) และ/หรือ กลุ่มบริษัทเมเจอร์ จัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับวิสัยทัศน์ภารกิจ และยุทธศาสตร์ของบริษัทฯ ในการเพิ่มศักยภาพการบริหารขัดการ ยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศของบริษัทฯ โดยมีวัตถุประสงค์เพื่อรักษาความมั่นคงปลอดภัยให้แก่ทรัพย์สินด้านเทคโนโลยีสารสนเทศทุกประเภทของบริษัทฯ รวมถึงลดผลกระทบและความเสียหายต่างๆ ที่อาจเกิดขึ้นและคงไว้ซึ่งความสามารถในการดำเนินธุรกิจได้อย่างต่อเนื่อง

1.1 ขอบเขต

1) ข้อมูลทั้งหมด (ที่อยู่ในรูปเอกสารตีพิมพ์เอกสารและข้อมูลอิเล็กทรอนิกส์) ที่จัดเก็บใช้งานหรือใช้ในการสื่อสารเพื่อดำเนินกิจการของบริษัทฯ
2) บุคคลทั้งหมดที่มีส่วนเกี่ยวข้องในการใช้งานข้อมูลและระบบเทคโนโลยีสารสนเทศของบริษัทฯ โดยครอบคลุมถึงคณะกรรมการ ผู้บริหาร พนักงาน ลูกจ้างชั่วคราว บริษัทคู่ค้า บริษัทหรือบุคคลที่เป็นคู่สัญญาและผู้ให้บริการภายนอก
3) ทรัพย์สินด้านเทคโนโลยีสารสนเทศทั้งหมดที่เกี่ยวข้องกับข้อมูลและใช้ในการจัดเก็บ ส่งผ่าน หรือประมวลข้อมูลดังต่อไปนี้ เครื่องมือ อุปกรณ์ เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ ซอฟต์แวร์ โปรแกรมประยุกต์ เอกสารและข้อมูลอิเล็กทรอนิกส์ เอกสารตีพิมพ์ สถานที่ และสิ่งอำนวนความสะดวก ตลอดจนบริการอื่นๆ ด้านเทคโนโลยีสารสนเทศ

1.2 วัตถุประสงค์

1) เพื่อเป็นแนวทางในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและแนวทางการใช้งานระบบเทคโนโลยีสารสนเทศและข้อมูลของบริษัททิศทางเดียวกัน
2) เพื่อให้มั่นใจว่าการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ สอดคล้องกับยุทธศาสตร์ของบริษัทฯ และมาตรฐานสากลในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
3) เพื่อป้องกันและลดความเสี่ยงที่อาจก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการรักษาความลับของระบบงานและข้อมูล (Confidentiality) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (Integrity) ความพร้อมใช้งานของระบบและข้อมูล (Availability) หรือชื่อเสียงของบริษัทฯ
4) เพื่อสร้างความตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศแก่บุคคลทั้งหมดที่มีส่วนเกี่ยวข้องในการใช้งานระบบเทคโนโลยีสารสนเทศและข้อมูลของบริษัทฯ

2. **คำนิยาม**

คำ	ความหมาย
บริษัทฯ	บริษัท เมเจอร์ ซีนีเพล็กซ์ กรุ๊ป จำกัด (มหาชน) และ/หรือ กลุ่มบริษัทเมเจอร์
ฝ่าย	ฝ่ายเทคโนโลยีสารสนเทศ
ข้อมูล / ข้อมูลคอมพิวเตอร์	ข้อมูล ข้อมูลส่วนบุคคล ข้อความ ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์
ผู้ใช้งาน	บุคคลที่ได้รับอนุญาตในการเข้าถึงข้อมูลหรือระบบเทคโนโลยีสารสนเทศ โดยอาจเป็นเจ้าหน้าที่ของบริษัทฯมีหน้าที่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและเอกสารสนับสนุนที่เกี่ยวข้องอย่างเคร่งครัด
ทรัพย์สิน (สารสนเทศ)	สิ่งใดก็ตามที่มีมูลค่าแก่บริษัทฯ ประกอบไปด้วยข้อมูล ระบบงานเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ อุปกรณ์เครือข่ายสื่อสาร และซอฟต์แวร์
การเข้าถึงหรือการควบคุมการใช้งานเทคโนโลยีสารสนเทศ	การอนุญาต การกำหนดสิทธิ์ หรือมอบอำนาจในการเข้าถึง หรือใช้งานเครือข่าย หรือระบบเทคโนโลยีสารสนเทศทั้งทางกายภาพและทางอิเล็กทรอนิกส์ รวมทั้งการอนุญาตในลักษณะเดียวกันกับบุคคลภายนอก
ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ	การรักษาไว้ซึ่งคุณสมบัติทางด้านความมั่นคงปลอดภัยต่อทรัพย์สินของบริษัทฯ อันประกอบไปด้วยการรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (Confidentiality) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (Integrity) และความพร้อมใช้งานของระบบงานและข้อมูล (Availability) ของทรัพย์สินเทคโนโลยีสารสนเทศ รวมทั้งคุณสมบัติอื่น คือ ความถูกต้องแท้จริง (Authenticity) ความสำนึกรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)
ระบบเทคโนโลยีสารสนเทศ	อุปกรณ์หรือชุดอุปกรณ์ทางด้านเทคโนโลยีสารสนเทศที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลให้เป็นสารสนเทศ

คำ	ความหมาย
เหตุการณ์ด้านความมั่นคงปลอดภัย (Event)	กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่เกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลวหรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
สถานการณ์ความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศของบริษัทฯ ถูกบุกรุกหรือโจมตีและคุกคาม
เจ้าของสารสนเทศ (Information Owner)	ผู้บริหารของหน่วยงานที่สร้างข้อมูลขึ้นหรือใช้งานข้อมูลมากที่สุดโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นหรือได้รับผลกระทบโดยตรง หากข้อมูลเหล่านั้นเกิดสูญหายและยังเป็นผู้รับผิดชอบในการอนุมัติสิทธิ์ในการเข้าใช้สารสนเทศ
ผู้พัฒนาระบบเทคโนโลยีสารสนเทศ	พนักงานหรือ บุคคล/ หน่วยงาน/ องค์กร ซึ่งรับจ้างในการให้บริการซึ่งได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการพัฒนาระบบเทคโนโลยีสารสนเทศ
ผู้ดูแลระบบ	พนักงานที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์และสามารถเข้าถึงซอฟต์แวร์คอมพิวเตอร์หรือข้อมูลอื่น เพื่อจัดการระบบคอมพิวเตอร์และอุปกรณ์เครือข่ายสื่อสารได้
มาตรฐาน	มาตรฐานบรรทัดฐานที่บังคับใช้ในการปฏิบัติงานจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
รหัสผ่าน	ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นส่วนหนึ่งในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
โปรแกรมประยุกต์	โปรแกรมคอมพิวเตอร์ที่ถูกออกแบบให้รองรับการทำงานหรือกิจกรรมหลายด้านเพื่อประโยชน์ของผู้ใช้งาน

คำ	ความหมาย
ระบบเครือข่าย	ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของหน่วยงาน ดังต่อไปนี้ ➢ ระบบแลน (Local Area Network : LAN) ➢ ระบบแวน (Wide Area Network : WAN) ➢ ระบบ Wireless ➢ ระบบอินเตอร์เน็ต (Internet) ➢ ระบบ MAN (Metropolitan Area Network : MAN) ➢ ระบบ SD-WAN (Software-Defined Wide Area Network : SD WAN) ➢ ระบบ MPLS (Multi-Protocol Label Switching) ➢ ระบบ DATA Sim-card ➢ ระบบ Leased Line
ระบบแลน (Local Area Network) และระบบอินทราเน็ต (Intranet)	ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่ออุปกรณ์และระบบเทคโนโลยีสารสนเทศต่างๆ ภายในบริษัทฯ เข้าด้วยกันเป็นระบบเครือข่ายที่มีวัตถุประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในบริษัทฯ
ระบบแวน (Wide Area Network)	ระบบเครือข่ายที่อุปกรณ์และระบบเทคโนโลยีสารสนเทศถูกเชื่อมโยงเข้าด้วยกันอยู่ห่างกันมากกว่า 5 กิโลเมตร
ระบบ Wireless	การสื่อสารไร้สาย ซึ่งเป็นการถ่ายโอนข้อมูลเทคโนโลยีสารสนเทศ ระหว่างจุดสองจุด หรือมากกว่า โดยไม่ได้เชื่อมต่อกันด้วยตัวนำไฟฟ้า
ระบบอินเทอร์เน็ต (Internet)	ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล
ระบบ MAN (Metropolitan Area Network : MAN)	ระบบเครือข่ายที่เชื่อมต่อเครือข่ายหลายเครือข่ายเข้าด้วยกัน เพื่อให้บริการรับส่งข้อมูลในพื้นที่ใกล้เคียง
ระบบ SD-WAN (Software-Defined Wide Area Network : SD WAN)	ระบบเครือข่ายที่ใช้ซอฟต์แวร์ในการควบคุมการทำงานของเครือข่าย WAN เพื่อเพิ่มความยืดหยุ่นในการเชื่อมต่ออินเทอร์เน็ตระหว่างสาขาหรือศูนย์ข้อมูล ทำให้สามารถจัดการและควบคุมทราฟฟิกได้อย่างมีประสิทธิภาพจากศูนย์กลาง

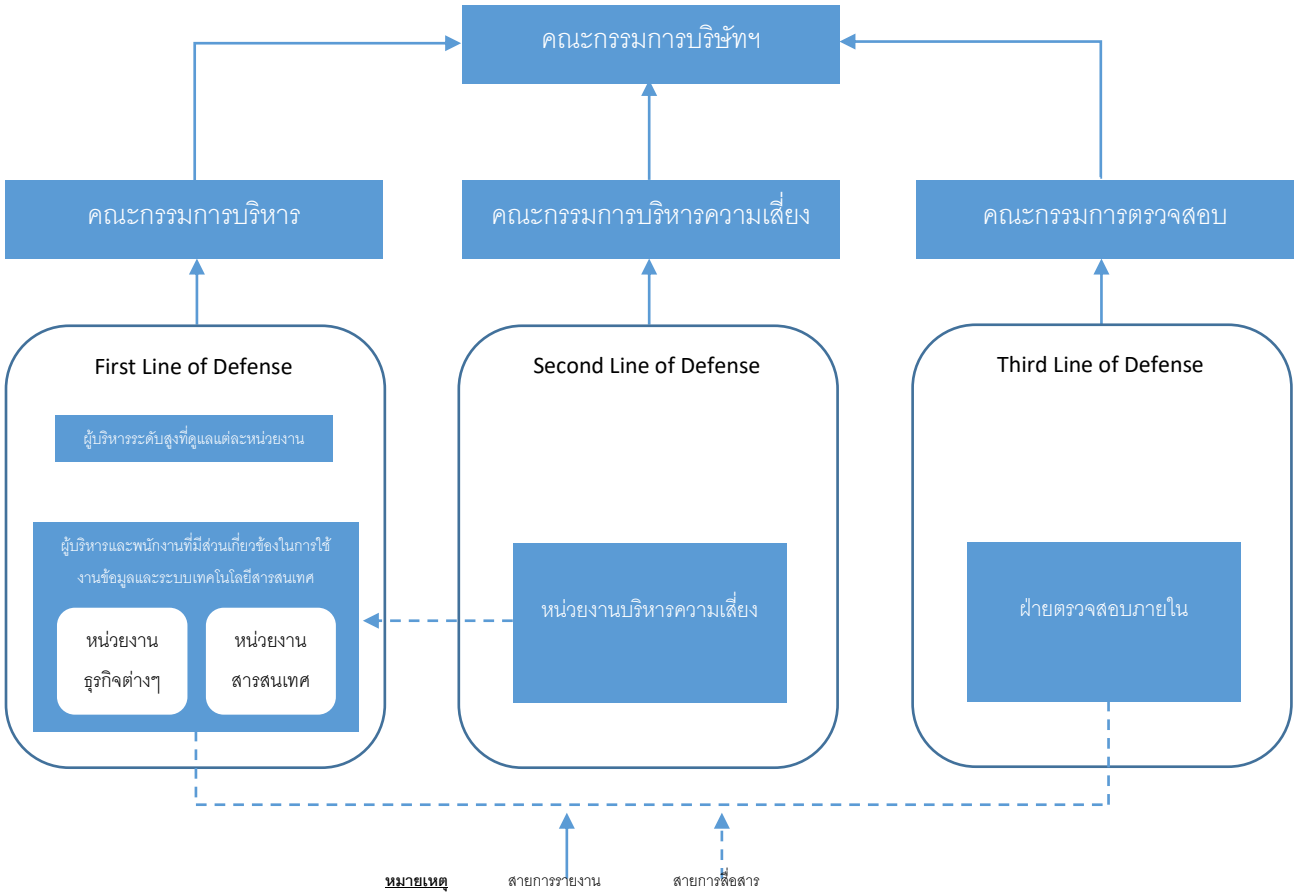
คำ	ความหมาย
ระบบ MPLS (Multi-Protocol Label Switching)	ระบบเครือข่ายที่ใช้เทคโนโลยีในการส่งข้อมูลแบบมีป้ายกำกับ เพื่อให้สามารถกำหนดเส้นทางการส่งข้อมูลได้อย่างรวดเร็วและมีประสิทธิภาพ โดยเฉพาะในเครือข่ายที่มีการใช้งานหลายโปรโตคอลพร้อมกัน เหมาะสำหรับการเชื่อมต่อข้อมูลข้ามพื้นที่
ระบบ DATA Sim-card	ระบบการเชื่อมต่อเครือข่ายอินเทอร์เน็ตผ่านซิมการ์ดที่ให้บริการอินเทอร์เน็ตความเร็วสูง โดยรองรับการใช้งานอุปกรณ์พกพา เช่น สมาร์ทโฟน แท็บเล็ต และโมเด็มไร้สาย สำหรับการเชื่อมต่อเครือข่ายภายนอก
ระบบ Leased Line	ระบบเชื่อมต่อเครือข่ายแบบสายสัญญาณเช่าที่ให้ความเร็วในการรับส่งข้อมูลสูงและมีเสถียรภาพสูง เหมาะสำหรับการเชื่อมต่ออินเทอร์เน็ตหรือสาขาต่าง ๆ แบบจุดต่อจุด
VPN (Virtual Private Network)	เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยใช้การรับส่งข้อมูลจริง ซึ่งในการรับส่งข้อมูลจะทำการเข้ารหัสเฉพาะ โดยผ่านเครือข่ายอินเทอร์เน็ตทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง
ลงบันทึกเข้า (Login)	กระบวนการที่ผู้ใช้บริการต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้งาน ระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้ถูกต้อง
ลงบันทึกออก (Logout)	กระบวนการที่ผู้ใช้บริการทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย
สื่อบันทึกพกพาและอุปกรณ์เคลื่อนที่ต่างๆ	สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูลที่มีขนาดกะทัดรัด ติดตั้ง หรือถอดได้ง่ายและสะดวกต่อการพกพา ดังต่อไปนี้ ➢ Flash Drive หรือ Handy Drive หรือ Thumb Drive ➢ External Hard Disk ➢ PDA หรือ Smart Phone หรือ Tablet หรือ Phablet ➢ CD-Rom ➢ หน่วยเก็บข้อมูลคลาวด์หรือคลาวด์คอมพิวติ้ง (Cloud Computing)
หน่วยงานภายนอก	องค์กรหรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของบริษัทฯ โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

คำ	ความหมาย
อัพเดต	การปรับให้เป็นปัจจุบันการปรับปรุงข้อมูลด้านต่างๆ ของระบบเทคโนโลยีสารสนเทศให้ทันตามกรอบเวลาที่กำหนด

3. โครงสร้างการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและบทบาทหน้าที่ความรับผิดชอบ

3.1 โครงสร้างการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

บริษัทฯ ได้กำหนดโครงสร้างการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังต่อไปนี้



แผนภาพที่ 1 : โครงสร้างการรักษาความมั่นคงความปลอดภัยด้านเทคโนโลยีสารสนเทศ

3.2 บทบาทหน้าที่ความรับผิดชอบ

จากโครงสร้างการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศข้างต้นบริษัทฯได้กำหนดรายละเอียดของบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังนี้

บทบาท หน้าที่ และความรับผิดชอบในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ	
ผู้ที่เกี่ยวข้อง	**ความรับผิดชอบ**
คณะกรรมการบริหาร	● อนุมัติการจัดทำและทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) ● กำกับดูแลให้คณะผู้บริหาร ฝ่ายงานด้านเทคโนโลยีสารสนเทศและฝ่ายงานที่เกี่ยวข้อง นำนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) ไปกำหนดกระบวนการในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ● ควบคุมการทำงานให้เป็นไปตามหลักเกณฑ์หรือกฎหมายอื่นที่เกี่ยวข้อง
คณะกรรมการบริหารความเสี่ยง	● ติดตามให้มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นไปตามที่แนวทางกำหนด
คณะกรรมการตรวจสอบ	● สอบทานประสิทธิภาพและประสิทธิผลของกระบวนการควบคุมภายในที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ● สอบทานการดำเนินงานของบริษัทฯ ให้ถูกต้องตามกฎหมาย ระเบียบข้อบังคับ วิธีปฏิบัติงานตามนโยบายรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและหลักเกณฑ์หรือกฎหมายอื่นที่เกี่ยวข้อง ● รายงานผลการดำเนินงานของคณะกรรมการตรวจสอบต่อคณะกรรมการบริษัทฯ
ผู้บริหารระดับสูงที่ดูแลฝ่ายเทคโนโลยีสารสนเทศ	● ดูแลและสอบทานเนื้อหาของนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) ก่อนนำเสนอต่อคณะกรรมการบริหารเพื่ออนุมัติ ● เป็นผู้ให้การสนับสนุนด้านทรัพยากรต่างๆ เพื่อให้การบริหารจัดการและการดำเนินการด้านระบบเทคโนโลยีสารสนเทศมีความปลอดภัยและสอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้

ผู้ที่เกี่ยวข้อง	ความรับผิดชอบ
	• ติดตามและควบคุมให้มีการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) ที่ได้รับการอนุมัติจากคณะกรรราการบริหาร
ผู้บริหารสูงสุดที่ดูแลแต่ละฝ่าย	• สนับสนุนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ • กำกับดูแลให้พนักงานและผู้ที่ทำสัญญาจ้างรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยปฏิบัติให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ แนวปฏิบัติ และขั้นตอนการปฏิบัติงานที่เกี่ยวข้อง
ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ	• กลั่นกรองการจัดทำและทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) พร้อมทั้งจัดสรรทรัพยากรเพื่อรองรับการดำเนินงานอย่างเพียงพอ • อนุมัติแนวปฏิบัติขั้นตอนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศต่างๆ ที่เกี่ยวข้อง • ทบทวนแนวปฏิบัติขั้นตอนการปฏิบัติงานและชุดเอกสารต่างๆ ที่เกี่ยวข้อง • กำกับ ดูแล และควบคุมการบังคับใช้นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Policy and Guideline) และชุดเอกสารต่างๆ ที่เกี่ยวข้อง • อื่นๆ ตามที่ได้รับมอบหมาย
ฝ่ายเทคโนโลยีสารสนเทศ	• ควบคุม ดูแล และปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) ที่กำหนดเพื่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและปฏิบัติตามข้อกฎหมายอื่นๆ ที่เกี่ยวข้องทั้งหมด • สื่อสารและเผยแพร่นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) รวมถึงแนวปฏิบัติและเอกสารที่เกี่ยวข้อง ให้แก่บุคลลที่มีส่วนเกี่ยวข้องในการใช้งานข้อมูลและระบบเทคโนโลยีสารสนเทศของบริษัทฯ

ผู้ที่เกี่ยวข้อง	ความรับผิดชอบ
ผู้บริหารฝ่ายและพนักงานที่มีส่วนเกี่ยวข้องในการใช้งานข้อมูลและระบบเทคโนโลยีสารสนเทศ	● ทำความเข้าใจกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) และชุดเอกสารที่เกี่ยวข้อง ● ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและชุดเอกสารความรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่กำหนดและปฏิบัติตามข้อกฎหมายอื่นๆ ที่เกี่ยวข้องทั้งหมด ● รายงานเหตุการณ์ขัดแย้งกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศแก่ผู้บริหารของฝ่ายงานและฝ่ายเทคโนโลยีสารสนเทศ ตามโครงสร้างองค์กร
ฝ่ายบริหารความเสี่ยง	● จัดให้มีกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)
ฝ่ายตรวจสอบภายใน	● ประเมินความเพียงพอ ประสิทธิภาพและประสิทธิผลของการควบคุมภายในกระบวนการปฏิบัติงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ● รายงานผลการตรวจสอบการควบคุมภายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการตรวจสอบเพื่อพิจารณารับทราบแผนการตรวจสอบที่กำหนด

ตารางที่ 2 : บทบาทและความรับผิดชอบในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ด้านงานเทคโนโลยีสารสนเทศ

4. **นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ**

การกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นการกำหนดทิศทางและแนวทางการควบคุมให้ทรัพย์สินด้านเทคโนโลยีสารสนเทศทุกประเภทของบริษัทฯ มีความมั่นคงปลอดภัย โดยครอบคลุมการรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (Confidentiality) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (Integrity) และความพร้อมใช้งานของระบบงานและข้อมูล (Availability) รวมทั้งเป็นการสื่อสารให้คณะกรรมการ ผู้บริหาร และพนักงานทุกคนรับทราบและนำไปปฏิบัติในทิศทางเดียวกัน นโยบายรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศมีรายละเอียดดังต่อไปนี้

1) คณะกรรมการบริหารอนุมัตินโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ เพื่อกำหนดทิศทางและแนวทางในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ โดยสอดคล้องกับยุทธศาสตร์ด้านเทคโนโลยีของบริษัทฯ นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และมาตรฐานสากลในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ประธานกรรมการซึ่งเป็นผู้บริหารสูงสุดขององค์กร รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายใดๆ แก่บริษัทฯ หรือผู้หนึ่งผู้ใดอันเนื่องมากจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสรนเทศ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยมอบหมายให้ผู้บริหารระดับสูงที่ดูแลฝ่ายเทคโนโลยีสารสนเทศ และฝ่ายเทคโนโลยีสารสนเทศเป็นผู้รักษาการให้เป็นไปตามนโยบายฯ ฉบับนี้
2) ผู้บริหารระดับสูงที่ดูแลฝ่ายเทคโนโลยีสารสนเทศ และฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีแนวทางปฏิบัติขั้นตอนการปฏิบัติงานและเอกสารสนับสนุนที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงกำกับดูแลให้มีการควบคุมเข้าถึงข้มูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย ทั้งนี้ต้องจัดให้มีการควบคุมด้านความมั่นคงปลอดภัยไซเบอร์ โดยรวมถึงการจัดการเพื่อรองรับสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Resilience) โดยครอบคลุมการควบคุม 6 ด้าน ได้แก่ การกำกับดูแล (Governance) การระบุความเสี่ยง (Risk Identification) การป้องกัน (Protection) การตรวจจับ (Detection) การตอบสนองและการกู้คืน (Response and Recovery) และการบริหารความเสี่ยงจากการใช้บริการผู้ให้บริการภายนอก (Third Party Risk Management)
3) ผู้บริหารระดับสูงที่ดูแลฝ่ายเทคโนโลยีสารสนเทศ และฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีกระบวนการในการรายงานสอบข้อเท็จจริง รับมือและจัดการกับเหตุละเมิดความมั่นคงปลอดภัยอย่างเหมาะสม โดยเหตุละเมิดความมั่นคงปลอดภัย ตลอดจนสิ่งผิดปกติ และเหตุการณ์น่าสงสัยอื่นๆ จะต้องได้รับการรายงานไปที่คณะกรรมการบริหารหรือผู้ที่ได้รับมอบหมายเพื่อดำเนินการตรวจสอบและแก้ไข
4) ฝ่ายเทคโนโลยีสารสนเทศ ร่วมกับฝ่ายงานที่เกี่ยวข้องต้องจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรพร้อมทั้งทำการดูแลรักษาและทดสอบแผนดังกล่าวอย่างเหมาะสม
5) ฝ่ายเทคโนโลยีสารสนเทศ ต้องสื่อสารนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงแนวปฏิบัติและเอกสารที่เกี่ยวข้องให้แก่บุคคลทั้งหมดที่มีส่วนเกี่ยวข้องในการใช้งานข้อมูลและระบบเทคโนโลยีสารสนเทศของบริษัทฯ อย่างเหมาะสมและจัดอบรมด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ให้แก่ คณะกรรมการ ผู้บริหาร และพนักงานทุกคน เพื่อให้เกิดความตระหนักและความเข้าใจถึงภัยคุกคามและผลกระทบที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมถึงการควบคุมเชิงป้องกันที่เกี่ยวข้อง

6) พนักงานทุกคนจะต้องปกป้องข้อมูล (ไม่ว่าจะถูกเก็บอยู่ในรูปแบบใดก็ตาม) ให้พ้นจากเหตุละเมิดต่างๆ ซึ่งอาจส่งผลกระทบต่อความลับของข้อมูล (Confidentiality) ความถูกต้องและสมบูรณ์ครบถ้วนของข้อมูล (Integrity) หรือความพร้อมใช้งานของข้มูล (Availability) รวมถึงต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่บริษัทฯ กำหนดเพื่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและปฏิบัติตามข้อกฎหมายอื่นๆ ที่เกี่ยวข้องทั้งหมด
7) ฝ่ายบริหารความเสี่ยงต้องจัดให้มีกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management) โดยส่วนกำกับการปฏิบัติงานต้องกำกับดูแลการปฏิบัติตามกฎหมายนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และฝ่ายตรวจสอบภายในมีหน้าที่ต้องดำเนินการตรวจสอบ (Internal Audit) ความมีประสิทธิภาพและความมีประสิทธิผลของการควบคุมภายในที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
8) ฝ่ายเทคโนโลยีสารสนเทศ ทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เพื่อให้มั่นใจได้ว่านโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศยังคงไว้ซึ่งความสมบูรณ์ มีประสิทธิภาพและสามารถนำไปปฏิบัติได้อย่างเหมาะสม

5. องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

หมวดที่ 1 การจัดการนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policies)

1.1 หน้าที่ของผู้บริหารระดับสูงที่ดูแลฝ่ายเทคโนโลยีสารสนเทศ และฝ่ายเทคโนโลยีสารสนเทศ

1.1.1 กำหนดและจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรและนำเสนอต่อผู้บริหารระดับสูงที่ดูแลฝ่ายเทคโนโลยีสารสนเทศ เพื่อพิจารณากลั่นกรองก่อนเสนอคณะกรรมการบริหารเพื่ออนุมัติ

1.1.2 ทบทวนหรือปรับปรุงนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เช่น มีการเปลี่ยนแปลงกฎเกณฑ์ หรือกฎหมายด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง การเปลี่ยนแปลงเทคโนโลยีใช้งาน การเปลี่ยนแปลงโครงสร้างบุคลากร การเปลี่ยนแปลงกระบวนการทำงานด้านเทคโนโลยีสารสนเทศ เป็นต้น โดยให้ผู้บริหารระดับสูงที่ดูแลฝ่ายเทคโนโลยีสารสนเทศ เพื่อทบทวนและปรับปรุงให้เป็นปัจจุบัน ก่อนนำเสนอคณะกรรมการบริหารเพื่ออนุมัติ

1.1.3 ประกาศ เผยแพร่ และสื่อสารนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้คณะกรรมการ ผู้บริหาร พนักงาน และผู้ให้บริการภายนอกที่เกี่ยวข้องตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศดังกล่าว รับทราบและถือปฏิบัติอย่างเคร่งครัด

หมวดที่ 2 โครงสร้างการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Organization of IT Security)

2.1 โครงสร้างการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศภายในบริษัทฯ (Internal Organization)

2.1.1 ผู้บริหารสูงสุดและผู้บริหารทุกคนให้ความสำคัญและมีหน้าที่รับผิดชอบในการสนับสนุนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และกำหนดให้ผู้บริหารระดับสูงที่ดูแล ฝ่ายเทคโนโลยีสารสนเทศ และฝ่ายเทคโนโลยีสารสนเทศ มีบทบาทและหน้าที่ความรับผิดชอบดูแลการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

2.1.2 ให้ฝ่ายเทคโนโลยีสารสนเทศ มีหน้าที่กำหนดรายละเอียดบทบาท หน้าที่ ความรับผิดชอบในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร (Information Security Roles and Responsibilities) รวมทั้งจัดสรรบุคลากรในการปฏิบัติหน้าที่ดังกล่าว และนำเสนอให้ผู้บริหารระดับสูงที่ดูแลฝ่ายเทคโนโลยีสารสนเทศ เพื่ออนุมัติ

2.1.3 ให้ฝ่ายเทคโนโลยีสารสนเทศ มีการแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties) ในการปฏิบัติงานอย่างชัดเจนเพื่อให้มีการสอบทานระหว่างกัน และป้องกันความเสี่ยงในการปฏิบัติงานที่อาจเกิดขึ้น เช่น แบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงาน (Developer) ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ (System Administration) ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริง (Production Environment) ทั้งนี้ในกรณีที่ไม่สามารถแบ่งแยกหน้าที่ ความรับผิดชอบ เนื่องจากข้อจำกัดทางด้านจำนวนบุคลากร ต้องจัดให้มีกระบวนการติดตามและตรวจสอบการปฏิบัติงานของบุคลากรที่เกี่ยวข้องอย่างใกล้ชิดและสม่ำเสมอเพื่อลดความเสี่ยงที่อาจเกิดขึ้น

2.1.4 การประสานงานกับหน่อยงานภายนอกที่เกี่ยวข้องด้านการมั่นคงปลอดภัย (Contact with Authorities) ให้ฝ่ายเทคโนโลยีสารสนเทศ มีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานที่จำเป็น เช่น ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) หน่วยงานกฎหมาย โรงพยาบาล สถานีตำรวจ สถานีดับเพลิง หรือหน่วยกู้ภัย เป็นต้น เพื่อใช้สำหรับการติดต่อประสานงานทางด้านความมั่นคงปลอดภัยในกรณีที่มีความจำเป็น พร้อมทั้งปรับปรุงรายชื่อและช่องทางสำหรับติดต่อดังกล่าวให้เป็นปัจจุบัน

2.1.5 ให้ฝ่ายสารสนแทศมีหน้าที่กำหนดแนวทางการควบคุมในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในการบริหารจัดการโครงการ (Information Security in Project Management) ทั้งโครงการที่เป็นโครงการภายในและโครงการจัดซื้อจัดจ้างผู้ให้บริการภายนอก และนำเสนอให้ผู้บริหารระดับสูงที่ดูแลฝ่ายเทคโนโลยีสารสนเทศ และคณะกรรมการที่เกี่ยวข้องกลั่นกรองและพิจารณาอนุมัติ โดยครอบคลุมถึงการกำหนดให้มีการประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อฝ่ายงานอื่นและระบบที่เกี่ยวข้องทั้งก่อนเริ่มโครงการ ระหว่างดำเนินการโครงการ และเมื่อโครงการเสร็จสิ้น การกำหนดข้อตกลงและความต้องการด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในข้อตกลงหรือสัญญาของโครงการ การกำหนดข้อตกลงในการพัฒนาและใช้งานเครื่องมือหรืออุปกรณ์ที่จำเป็นเพื่อให้เป็นมาตรฐานเดียวกัน การกำหนดบทลงโทษสำหรับผู้ไม่ปฏิบัติตามข้อตกลงและต้องการด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในข้อตกลงหรือสัญญาของโครงการ

2.2 การปฏิบัติงานโดยใช้อุปกรณ์เคลื่อนที่และปฏิบัติงานระยะไกลจากภายนอกบริษัทฯ (Mobile Devices and Teleworking)

2.2.1 ให้ฝ่ายเทคโนโลยีสารสนเทศ กำหนดการควบคุมเกี่ยวกับการใช้งานอุปกรณ์เคลื่อนที่ (Mobile Device) และการปฏิบัติงานระยะไกลจากภายนอกบริษัทฯ (Teleworking) โดยปฏิบัติตามเรื่องการควบคุมการเข้าถึง (Access Control) ที่ครอบคลุมถึงการระบุตัวตนและพิสูจน์ตัวตนและการเชื่อมต่อผ่านช่องทางที่มีความปลอดภัย เพื่อรักษาความมั่นคงปลอดภัยและบริหารจัดการความเสี่ยงที่อาจจะเกิดขึ้นได้ และสื่อสารให้ผู้ใช้งานและผู้ที่เกี่ยวข้องรับทราบและปฏิบัติในทิศทางเดียวกัน

2.2.2 การเชื่อมต่อระหว่างสถานที่ปฏิบัติงานภายนอกและเครือข่ายภายในของบริษัทให้ใช้งานผ่านเครือข่ายส่วนตัว (Virtual Private Network: VPN) และต้องทำการพิสูจน์ตัวตนด้วยวิธีการเข้ารหัสที่ได้รับอนุมัติจากผู้ดูแลระบบ และห้ามบุคคลอื่นนำไปใช้ (เพิ่ม)

หมวดที่ 3 ความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resource Security)

3.1 ข้อกำหนดในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศก่อนการจ้างงาน (Prior to Employment)

3.1.1 ในการพิจารณารับพนักงานเข้าทำงานให้ฝ่ายทรัพยากรบุคคลตรวจสอบประวัติและคุณสมบัติของบุคคลที่ได้รับคัดเลือกเข้ามาทำงานให้แก่บริษัทฯ ก่อนการจ้างงาน เช่น วุฒิการศึกษา ประวัติการทำงาน คุณสมบัติพิเศษเฉพาะด้านที่จำเป็นต่อการปฏิบัติงาน เป็นต้น โดยให้เป็นไปตามกฎหมาย กฎเกณฑ์ทางการ และจริยธรรมที่เกี่ยวข้อง โดยให้คำนึงถึงระดับชั้นความลับของข้อมูลเทคโนโลยีสารสนเทศ ที่จะให้เข้าถึงและระดับความเสี่ยงที่ได้ประเมินไว้

3.1.2 ในสัญญาจ้างหรือข้อตกลงการปฏิบัติงานของพนักงาน ลูกจ้าง หรือสัญญาว่าจ้างหน่วยงานหรือบุคคลภายนอกให้ระบุหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศไว้ในข้อตกลงหรือเงื่อนไขของสัญญาจ้าง ซึ่งผู้ที่ได้รับการว่าจ้างจะต้องให้ความยินยอมถือปฏิบัติตามเงื่อนไขที่กำหนดอย่างเป็นลายลักษณ์อักษร

3.1.3 สำหรับการจ้างงานผู้ให้บริการภายนอก ให้ฝ่ายเทคโนโลยีสารสนเทศ ตรวจสอบประวัติและคุณสมบัติของผู้ให้บริการภายนอกในกรณีที่เป็นการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ให้ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Securities Policies)

3.2 ข้อกำหนดในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในระหว่างการจ้างงาน (During Employment)

3.2.1 ให้ผู้บริหารของแต่ละฝ่ายกำกับดูแลให้พนักงานและผู้ที่ทำสัญญาจ้างทั้งหมดรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและขั้นตอนการปฏิบัติงานที่เกี่ยวข้อง

3.2.2 ให้ฝ่ายเทคโนโลยีสารสนเทศ อบรมให้ความรู้เพื่อเสริมสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้แก่คณะกรรมการ ผู้บริหาร พนักงานทุกคน และผู้ให้บริการภายนอกในส่วนที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตนเพื่อให้มั่นใจได้ว่า คณะกรรมการ ผู้บริหาร พนักงานทุกคน และผู้ให้บริการภายนอกได้รับการสื่อสารและนำไปปฏิบัติในทิศทางเดียวกัน

3.2.3 ให้ฝ่ายทรัพยากรบุคคลต้องกำหนดกระบวนการลงโทษทางวินัยสำหรับพนักงานที่ฝ่าฝืนหรือละเมิดนโยบายคำสั่งหรือระเบียบปฏิบัติที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ พร้อมทั้งสื่อสารให้ผู้บริหารและพนักงานทุกคนรับทราบ

3.3 ข้อกำหนดในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงานหรือสิ้นสุดสัญญาจ้าง (Termination and Change of Employment)

3.3.1 ให้ฝ่ายทรัพยากรบุคคล ฝ่ายเทคโนโลยีสารสนเทศ และฝ่ายกฎหมายร่วมกันกำหนดความรับผิดชอบหรือภาระผูกพันด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศภายหลังการจ้างงานไว้ในสัญญาจ้างและสื่อสารให้พนักงานหรือผู้ให้บริการภายนอกตามสัญญาจ้างรับทราบและถือปฏิบัติ

หมวดที่ 4 การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)

4.1 ความรับผิดชอบต่อทรัพย์สิน (Responsibility of Assets)

4.1.1 ให้ฝ่ายเทคโนโลยีสารสนเทศ จัดให้มีขั้นตอนการปฏิบัติงานเรื่องการจัดทำทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศโดยครอบคลุมรายละเอียดดังต่อไปนี้

(1) การจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (Inventory of assets) ครอบคลุมฮาร์ดแวร์ ซอฟต์แวร์ ที่รองรับระบบเทคโนโลยีสารสนเทศของบริษัทฯ และประกอบด้วยข้อมูลจำเป็นต่อการค้นหาหรือ เรียกใช้งาน เพื่อทำให้สามารถระบุรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศและผู้ใช้งานทรัพย์สินได้อย่างครบถ้วน

(2) การปรับปรุงทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศให้เป็นปัจจุบันอย่างสม่ำเสมอ โดยตรวจสอบทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีอยู่จริงกับทะเบียนรายการอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง รวมทั้งวางแผนรองรับสำหรับทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้จะสิ้นสุดตามอายุการใช้งานหรือสิ้นสุดการให้บริการเพื่อให้มั่นใจว่าทรัพย์สินด้านเทคโนโลยีสารสนเทศมีความพร้อมใช้งานและสามารถรองรับการดำเนินธุรกิจได้อย่างต่อเนื่อง

(3) การกำหนดให้มีฝ่ายงานผู้เป็นเจ้าของทรัพย์สินด้านเทคโนโลยีสารสนเทศ (Ownership for Assets) ในทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศโดยอาจเป็นฝ่ายงานที่มีหน้าที่ดูแล ใช้งาน หรือรับผิดชอบรายการทรัพย์สินนั้นๆ

(4) การยกเลิกและเรียกคืนทรัพย์สินด้านเทคโนโลยีสารสนเทศ (Return on Assets) เมื่อสิ้นสุดการใช้งาน ครอบคลุมทั้งทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใช้งานภายในบริษัทฯ และกรณีที่ผู้ให้บริการภายนอกใช้งานทรัพย์สินของบริษัทฯ ทันทีที่มีการยกเลิกสัญญาจ้าง

(5) การจัดเก็บและทำลายทรัพย์สินด้านเทคโนโลยีสารสนเทศ โดยต้องกำหนดการควบคุมหรือขั้นตอนการปฏิบัติงานที่เหมาะสมในการจัดเก็บและทำลายทรัพย์สินด้านเทคโนโลยีสารสนเทศให้เป็นไปตามระดับชั้นความลับที่กำหนดไว้

4.1.2 ให้ฝ่ายเทคโนโลยีสารสนเทศ จัดให้มีแนวปฏิบัติสำหรับผู้ใช้งานเทคโนโลยีสารสนเทศ (Acceptable Use Guideline) อย่างเป็นลายลักษณ์อักษรซึ่งระบุข้อกำหนดการใช้งานทรัพย์สินด้านเทคโนโลยีสารสนเทศและข้อมูลเทคโนโลยีสารสนเทศ ประกาศใช้และเผยแพร่สื่อสารแนวปฏิบัติดังกล่าวอย่างเป็นทางการให้พนักงานทุกคนรับทราบและถือปฏิบัติ

4.1.3 เมื่อสิ้นสุดข้อตกลงหรือสัญญาการจ้างงาน ให้พนักงานหรือผู้ให้บริการภายนอกทุกคนต้องคืนทรัพย์สินด้านเทคโนโลยีสารสนเทศของบริษัทฯ ที่ตนถือครองไว้โดยให้ฝ่ายเทคโนโลยีสารสนเทศ ดำเนินการยกเลิกสิทธิ์การเข้าถึงและใช้งานระบบทั้งหมดของพนักงานหรือผู้ให้บริการภายนอกที่สิ้นสุดสภาพการจ้างงานทันทีเมื่อถึงวันสิ้นสุดการจ้างงาน รวมถึงกรณีมีการโอนย้ายงานหรือมีการปรับเปลี่ยนบทบาทหน้าที่ความรับผิดชอบ ให้ฝ่ายเทคโนโลยีสารสนเทศ ดำเนินการตามขั้นตอนการเปลี่ยนแปลงแก้ไขสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศตามความจำเป็นและเหมาะสมของบทบาทหน้าที่ความรับผิดชอบที่เปลี่ยนแปลงไป

4.2 การรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security)

4.2.1 ให้ฝ่ายเทคโนโลยีสารสนเทศ ร่วมกับฝ่ายธุรกิจที่เกี่ยวข้องจัดให้มีแนวปฏิบัติเรื่องระดับชั้นข้อมูลเทคโนโลยีสารสนเทศ (Information Classification) ที่เหมาะสมกับประเภทข้อมูลและลักษณะการนำไปใช้ข้อกำหนดทางกฎหมาย มูลค่าของข้อมูล ความสำคัญของข้อมูล และความเสียหายหากข้อมูลถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต โดยครอบคลุมถึง

(1) กำหนดให้มีเจ้าของข้อมูล (Information Owner) รับผิดชอบในการกำหนดผู้ใช้งาน สิทธิ์การเข้าถึง และการใช้งานข้อมูลอย่างปลอดภัย

(2) กำหนดหลักเกณฑ์การจัดชั้นความลับของข้อมูล (Information Classification)

(3) กำหนดการควบคุมเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูล ที่สอดคล้องตามชั้นความลับของข้อมูลตามแนวทางการดำเนินงานที่กำหนดไว้ในระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ครอบคลุมข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (Data Endpoint) ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (Data in Transit) และข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล

(Data at Rest) กำหนดการควบคุมเกี่ยวกับการรักษาความมั่นคงปลอดภัยของสื่อบันทึกข้อมูลระหว่างขนส่ง (Physical Media Transfer)

4.2.2 ให้ฝ่ายเทคโนโลยีสารสนเทศ จัดให้มีการประทับตราหรือการจัดทำป้ายชื่อทรัพย์สินด้านเทคโนโลยีสารสนเทศ (Label) ที่ระบุรหัสอ้างอิงที่สามารถใช้เป็นข้อมูลชี้เฉพาะทรัพย์สินด้านเทคโนโลยีสารสนเทศแต่ละชิ้นได้ข้อมูลที่อยู่ในรูปแบบของเอกสาร ที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัย อย่างเหมาะสมตั้งแต่การเริ่มพิมพ์ การจัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการ ทำลาย และกำหนดเป็นระเบียบปฏิบัติให้เจ้าหน้าที่ต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุม และรักษาความปลอดภัย

4.2.3 ให้ฝ่ายเทคโนโลยีสารสนเทศ จัดให้มีการบริการจัดการทรัพย์สินเทคโนโลยีสารสนเทศ (Handling of Asset) เพื่อป้องกันข้อมูลลับต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงานเท่านั้น ผู้ใช้งานต้องตระหนักถึงการรักษาข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน ข้อมูลลับเหล่านี้ต้องได้รับการปกป้อง โดยการเข้ารหัส หรือโดยวิธีการอื่นใดของระบบปฏิบัติการ หรือระบบเทคโนโลยีสารสนเทศ อย่างเหมาะสม

4.3 การจัดการสื่อบันทึกข้อมูล (Media Handling)

4.3.1 ให้ฝ่ายเทคโนโลยีสารสนเทศ กำหนดการจัดการสื่อบันทึกข้อมูล ดังนี้

(1) กำหนดให้มีวิธีบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้าย (Management of Removable Media) ได้อย่างเหมาะสมตามชนิดและความสำคัญของสื่อนั้นๆ รวมทั้งมีแนวทางการควบคุมการจัดเก็บและการนำมาใช้งาน เพื่อป้องกันไม่ให้ข้อมูลในสื่อสูญหาย หรือถูกนำไปใช้ในทางที่ไม่ถูกต้อง

(2) กำหนดการควบคุมเพื่อดูสื่อบันทึกข้อมูลระหว่างขนย้าย เพื่อควบคุมการเข้าถึงสื่อที่มีข้อมูลสำคัญในระหว่างขนย้ายโดยไม่ได้รับอนุญาต

4.4 การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

4.4.1 ให้ฝ่ายเทคโนโลยีสารสนเทศ กำหนดการทำลายสื่อบันทึกข้อมูล ดังนี้

(1) กำหนดการทำลายสื่อที่ใช้ในการบันทึกข้อมูลอย่างเป็น ลายลักษณ์อักษรโดยปฏิบัติตามวิธีปฏิบัติงานเรื่องการทำลายสื่อบันทึกข้อมูลและข้อมูลบนสื่อบันทึกข้อมูล (Disposal of media procedure) การทำลายเอกสารและสื่อที่ใช้ในการบันทึกข้อมูล จะต้องได้รับการอนุมัติจากเจ้าของข้อมูล รวมทั้งบันทึกรายละเอียดอย่างเหมาะสม ควรทำลายสื่อที่ใช้ในการบันทึกข้อมูลเอกสารและอุปกรณ์สำนักงานภายใต้สิ่งแวดล้อมที่ได้มีการควบคุม (Controlled Environment) รวมทั้งจัดให้มีการจัดทำทะเบียนการทำลายข้อมูลสำคัญโดยระบุผู้รับผิดชอบในการทำลายข้อมูลวันที่เวลา ชนิดของสื่อบันทึก ข้อมูลserial number และวิธีการที่ใช้ทำลายข้อมูล

4.5 การเคลื่อนย้ายสื่อบันทึกข้อมูล (Physical Media Transfer)

4.5.1 ให้ฝ่ายเทคโนโลยีสารสนเทศ กำหนดการเคลื่อนย้ายสื่อบันทึกข้อมูล ดังนี้

(1) กำหนดวิธีการจัดส่งสื่อบันทึกข้อมูล(เทคโนโลยีสารสนเทศหรือซอฟต์แวร์) ให้มีความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ในกรณีที่มีการเคลื่อนย้ายสื่อบันทึกข้อมูลออกจากพื้นที่ติดตั้งหรือพื้นที่ปฏิบัติงาน

หมวดที่ 5 การควบคุมการเข้าถึง (Access Control)

5.1 ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business Requirements of Access Control)

5.1.1 ให้ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดแนวปฏิบัติสำหรับผู้ใช้งานเทคโนโลนยีสารสนเทศ (Acceptable Use Guideline) อย่างเป็นลายลักษณ์อักษร รวมทั้งทบทวนเพื่อปรับปรุงแก้ไขอย่างน้อยปีละ 1 ครั้ง โดยเผยแพร่ให้ คณะกรรมการ ผู้บริหาร พนักงานทุกคนรับทราบและถือปฏิบัติในทิศทางเดียวกันเพื่อป้องกันการเข้าถึงและการเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มีสิทธิ์หรือไม่ได้รับอนุญาต

5.1.2 ให้ฝ่ายเทคโนโลยีสารสนเทศ ควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์เฉพาะผู้ใช้งานที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงเครือข่ายและบริการเครือข่ายได้ โดยกำหนดประเภทหรือบริการทางเครือข่าย รวมถึงผู้ที่ได้รับอนุญาตให้เข้าถึงและการเชื่อมต่อเครือข่ายกระบวนการในการควบคุมและป้องกันการเข้าถึงวิธีการเข้าถึงแบบปลอดภัยการพิสูจน์ตัวตนและติดตามการใช้งานของผู้ที่ได้รับอนุญาตให้เข้าถึง

5.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

5.2.1 ให้ฝ่ายเทคโนโลยีสารสนเทศ จัดให้มีขั้นตอนการปฏิบัติงานการลงทะเบียนผู้ใช้งาน การขอใช้สิทธิ์ และการเข้าถึงระบบ สำหรับการเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัทฯ โดยครอบคลุมเรื่องดังต่อไปนี้

(1) ขั้นตอนการลงทะเบียนบัญชีผู้ใช้งานและยกเลิกบัญชีผู้ใช้งานของพนักงาน (User Registration and De-Registration) รวมถึงผู้ให้บริการภายนอกที่ได้รับอนุญาตจากบริษัทฯ หรือฝ่ายงานเจ้าของระบบเพื่อควบคุมให้เฉพาะผู้ที่ได้รับอนุญาตตามบทบาทหน้าที่ความรับผิดชอบเท่านั้นที่สามารถเข้าใช้งานระบบเทคโนโลยีสารสนเทศได้

(2) ขั้นตอนการจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Provisioning) การเปลี่ยนแปลงแก้ไขสิทธิ์ยกเลิกสิทธิ์การใช้งาน เมื่อมีการสิ้นสุดสภาพการจ้างงานหรือการปรับเปลี่ยนตำแหน่งการทำงานหรือครบระยะเวลาการทำงานตามสัญญาจ้าง

(3) การควบคุมและจำกัดการใช้งานสิทธิ์จำเพาะหรือสิทธิ์สูงหรือสิทธิ์พิเศษ (Management of Privileged Access Rights) เพื่อควบคุมการกำหนดสิทธิ์สำคัญในการเข้าถึงระบบเทคโนโลยีสารสนเทศให้เฉพาะผู้มีหน้าที่ความรับผิดชอบและเป็นไปตามหลักการการได้สิทธิ์ให้น้อยที่สุดและเท่าที่จำเป็น รวมถึงต้องมีการบันทึกและจัดเก็บหลักฐานการขอใช้งานสิทธิ์สูงหรือสิทธิ์พิเศษเพื่อใช้ในการตรวจสอบภายหลัง

(4) ขั้นตอนการทบทวนสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน (Review of User Access Rights) ซึ่งรวมถึงผู้ให้บริการภายนอก เพื่อให้มั่นใจว่าสิทธิ์การใช้งานสอดคล้องกับหน้าที่ความ

รับผิดชอบและความจำเป็นในการปฏิบัติงาน โดยกำหนดให้ทบทวนสิทธิ์อย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง พร้อมทั้งบันทึกรายการเปลี่ยนแปลงแก้ไขสิทธิ์

(5) การถอนหรือการจัดการสิทธิ์การเข้าถึง (Removal or Adjustment of Access Rights) สิทธิ์การเข้าถึงของพนักงานและลูกจ้างของหน่วยงานภายนอกต่อเทคโนโลยีสารสนเทศและอุปกรณ์ ประมวลผลเทคโนโลยีสารสนเทศต้องได้รับการถอดถอนเมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง และต้องได้รับการปรับปรุงให้ถูกต้องอย่างสม่ำเสมอ

5.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

5.3.1 การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of Secret Authentication Information) พนักงานต้องเก็บรักษา Username และ Password ต้องเป็นความลับห้ามเปิดเผยให้บุคคลอื่นทราบ ต้องหลีกเลี่ยงการเก็บบันทึกข้อมูลการตรวจสอบความลับ เว้นแต่สามารถเก็บไว้อย่างปลอดภัย และเมื่อพนักงานได้รับข้อมูล Password ซึ่งเป็นข้อมูล Default ควรมีการแก้ไขทันทีเมื่อเข้าใช้งานระบบครั้งแรก

5.3.2 ให้ผู้ใช้งานต้องปฏิบัติตามหน้าที่ความรับผิดชอบที่กำหนดในแนวทางปฏิบัติสำหรับผู้ใช้งานเทคโนโลยีสารสนเทศ (Acceptable Use Guideline) เช่น เรื่องของการใช้บัญชีผู้ใช้งานระบบเทคโนโลยีสารสนเทศ การป้องกันอุปกรณ์เทคโนโลยีสารสนเทศที่ไม่มีพนักงานดูแลและแนวปฏิบัติเมื่อมีการละทิ้งทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีความสำคัญไว้ในสถานที่ที่ไม่ปลอดภัย เป็นต้น

5.4 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและโปรแกรมประยุกต์ (System and Application Access Control)

5.4.1 การจำกัดการเข้าถึงเทคโนโลยีสารสนเทศ (Information Access Restriction)

(1) สิทธิ์การเข้าถึงไฟล์ข้อมูลต้องได้รับการควบคุมตามหน้าที่ความรับผิดชอบ

(2) เจ้าของข้อมูลต้องพิจารณาอนุมัติให้สิทธิ์การเข้าถึงข้อมูลแก่ผู้ใช้งานเท่าที่จำเป็นเท่านั้น

(3) ป้องกันไม่ให้ผู้ไม่มีสิทธิ์เข้าถึง ระบบเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่าย ที่ไม่มีผู้ดูแล(เพิ่ม)

5.4.2 ขั้นตอนการปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความปลอดภัย (Secure Log-on Procedures)

(1) กำหนดให้มีการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบปฏิบัติการและระบบเทคโนโลยีสารสนเทศ

(2) ไม่แสดงข้อมูลของระบบใดๆ จนกว่าจะทำการเข้าสู่ระบบสำเร็จ

(3) ไม่แสดงข้อความช่วยเหลือในระหว่างขั้นตอนการเข้าสู่ระบบ

(4) แสดงข้อความแจ้งเตือนให้ทราบว่าระบบ

(5) สามารถเข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

(6) ตรวจสอบข้อมูลการเข้าสู่ระบบของผู้ใช้งานเมื่อเสร็จสิ้นการป้อนข้อมูลทั้งหมดเท่านั้น หากมีข้อผิดพลาดเกิดขึ้น ระบบต้องไม่แสดงข้อมูลการเข้าสู่ระบบทั้งที่ถูกต้องและไม่ถูกต้อง

(7) จำกัดจำนวนครั้งของการเข้าสู่ระบบไม่สำเร็จให้ไม่เกิน 3 ครั้ง เพื่อป้องกันการคาดเดาบัญชีผู้ใช้งานและรหัสผ่านเพื่อเข้าสู่ระบบ

5.4.3 ระบบบริหารจัดการรหัสผ่าน (Password Management System)

ต้องมีระบบบริหารจัดการรหัสผ่านที่สามารถให้บริการผู้ใช้งานดำเนินการจัดการด้วยตัวเอง (Self Service) เพื่อให้รหัสมีคุณภาพ รวมทั้งในกรณีที่ผู้ใช้งานกำหนดรหัสผ่านไม่เป็นไปตามข้อกำหนดดังกล่าว ระบบต้องไม่อนุญาตการใช้รหัสผ่านนั้นพร้อมแจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่จนกว่าการกำหนดรหัสผ่านจะเป็นไปตามข้อกำหนด

5.4.4 การใช้งานโปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs)

(1) โปรแกรมอรรถประโยชน์สำหรับระบบปฏิบัติการ (OS Utilities Programs) ซึ่งติดตั้งมาพร้อมกับระบบปฏิบัติการอยู่แล้ว ได้แก่ โปรแกรมจัดการไฟล์ (File Explorer) โปรแกรมยกเลิกการติดตั้งโปรแกรม (Uninstaller) โปรแกรมสแกนดิสก์ (Disk Scanner) โปรแกรมจัดเรียงพื้นที่จัดเก็บบข้อมูลบนฮาร์ดไดรฟ์ (Hard Drive) โปรแกรมรักษาหน้าจอ (Screen Saver) เป็นโปรแกรมที่อนุญาตให้ผู้ใช้งานใช้งานได้ การใช้โปรแกรมอรรถประโยชน์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยของระบบต้องมีการขออนุมัติจากหัวหน้าสายงาน และ ต้องได้รับการตรวจสอบ จากฝ่ายเทคโนโลยีสารสนเทศ ต้องมีการจำกัดและควบคุมการใช้อย่างใกล้ชิด

(2) ผู้ดูแลระบบคอมพิวเตอร์ต้องควบคุมการติดตั้งและใช้งานโปรแกรมอรรถประโยชน์อื่นๆ ซึ่งเป็นโปรแกรมที่ช่วยให้เครื่องคอมพิวเตอร์ทำงานได้อย่างมีประสิทธิภาพ เช่น โปรแกรมบีบอัดไฟล์ (File Compression) โปรแกรมไฟร์วอลล์ (Firewall) โปรแกรมป้องกันไวรัส (Antivirus Program) เป็นต้น

5.4.5 การควบคุมการเข้าถึงรหัสต้นฉบับของโปรแกรม (Access Control to Program Source Code)

(1) ผู้พัฒนาระบบเทคโนโลยีสารสนเทศต้องจัดให้มีการควบคุมการเข้าถึง Source Code ของระบบที่ใช้งานจริงหรือให้บริการ เช่น

- ไม่ควรเก็บ Source Code ไว้ในเครื่องที่ใช้งานจริงและต้องเก็บ Source Code ไว้ในที่ที่ปลอดภัย
- ต้องไม่เก็บ Source Code ที่อยู่ในระหว่างทำการทดสอบรวมไว้กับ Source Code ที่ใช้งานได้จริงแล้ว

5.4.6 การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลและการควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบคอมพิวเตอร์แม่ข่ายที่ให้บริการ

(1) ผู้ดูแลระบบคอมพิวเตอร์เป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบคอมพิวเตอร์แม่ข่าย (Server) ในการแก้ไขหรือเปลี่ยนแปลงค่าต่างๆ ของโปรแกรมระบบ (System Software)

(2) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดทำคู่มือปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติจะต้องดำเนินการแก้ไขรวมทั้งมีการรายงานให้เจ้าของระบบเทคโนโลยีสารสนเทศทราบทันที

(3) ผู้ดูแลระบบคอมพิวเตอร์ต้องเปิดใช้บริการเท่าที่จำเป็นเท่านั้น

(4) การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบคอมพิวเตอร์แม่ข่ายต้องมีการขออนุมัติจากผู้อำนวยการสารสนเทศและ/หรือผู้ดูแลระบบที่ได้รับมอบหมาย

(5) ในการทดสอบระบบเทคโนโลยีสารสนเทศก่อนการใช้งานจริง ผู้พัฒนาระบบเทคโนโลยีสารสนเทศ ต้องทำการทดสอบโปรแกรมบนระบบคอมพิวเตอร์แม่ข่ายที่ผู้ดูแลระบบคอมพิวเตอร์จัดไว้สำหรับการทดสอบเท่านั้น

(6) ให้ผู้ดูแลระบบคอมพิวเตอร์เป็นผู้ติดตั้งระบบเทคโนโลยีสารสนเทศที่ได้จากการพัฒนาลงบนระบบคอมพิวเตอร์แม่ข่ายเพื่อเปิดให้บริการแก่ผู้ใช้งาน

(7) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดเก็บซอฟต์แวร์เวอร์ชั่นเก่าและข้อมูลที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเดิมและขั้นตอนการปฏิบัติที่เกี่ยวข้องของระบบเทคโนโลยีสารสนเทศ ในกรณีที่จำเป็นต้องกลับไปใช้ซอฟต์แวร์เวอร์ชั่นเก่าเหล่านั้น

(8) ผู้แลระบบคอมพิวเตอร์ต้องเปิดเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น

5.4.7 การจำกัดระยะเวลาการเชื่อมต่อ (Limitation of Connection Time) เพื่อให้มีความมั่นคง ปลอดภัยมากขึ้นสำหรับระบบเทคโนโลยีสารสนเทศ ที่มีความสำคัญหรือมีความเสี่ยงสูงให้ปฏิบัติดังนี้

(1) ผู้ดูแลจัดการระบบงานต้องกำหนดให้มีการยุติการใช้งานระบบเทคโนโลยีสารสนเทศ (Session Time-out) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งอย่างน้อย 15 นาทีหรือตามความเหมาะสมแก่ระบบเทคโนโลยีสารสนเทศนั้นๆ

(2) ผู้ดูแลระบบงานต้องจำกัดระยะเวลาการเชื่อมต่อ (Limitation of Connection Time) สำหรับการใช้งานระบบเทคโนโลยีสารสนเทศที่มีความเหมาะสมแก่ระบบเทคโนโลยีสารสนเทศนั้น

หมวดที่ 6 การเข้ารหัสข้อมูล (Cryptography)

6.1 ให้ฝ่ายเทคโนโลยีสารสนเทศ จัดให้มีแนวปฏิบัติการเข้ารหัสข้อมูลและการบริหารจัดการกุญแจเข้ารหัสข้อมูลที่สอดคล้องกับแนวปฏิบัติเรื่องระดับชั้นข้อมูลเทคโนโลยีสารสนเทศ (Information Classification) โดยครอบคลุมถึง

6.1.1 ประเภทข้อมูลสำคัญที่ต้องได้รับการเข้ารหัสและช่องทางการสื่อสารที่ใช้รับส่งข้อมูลสำคัญกับภายนอกเป็นอย่างน้อย

6.1.2 วิธีการเข้ารหัสข้อมูลโดยใช้มาตรฐานการเข้ารหัสข้อมูลที่เชื่อถือได้และเป็นมาตรฐานสากล มีการทบทวนประสิทธิภาพของวิธีการเข้ารหัสข้อมูลอย่างสม่ำเสมอเพื่อให้มั่นใจว่าวิธีการเข้ารหัสข้อมูลที่ใช้งานยังคงมีความแข็งแรงเพียงพอ

6.1.3 กระบวนการบริหารจัดการกุญแจเข้ารหัสข้อมูล (Key Management) ที่มีความรัดกุม ปลอดภัย ครอบคลุมตั้งแต่ การสร้างและติดตั้ง การจัดเก็บ และการยกเลิกกุญแจเข้ารหัสข้อมูล

หมวดที่ 7 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

7.1 ความมั่นคงปลอดภัยของพื้นที่ปฏิบัติงาน (Secure Areas)

7.1.1 การกำหนดบริเวณหรือพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัยทางกายภาพ (Secure Area)

(1) กำหนดให้พื้นที่ศูนย์ข้อมูล พื้นที่จัดเก็บข้อมูล พื้นที่ทำงานของผู้ดูแลระบบฯ พื้นที่ติดตั้งอุปกรณ์เครือข่าย และพื้นที่ติดตั้งอุปกรณ์คอมพิวเตอร์สำหรับผู้ใช้งานเป็นพื้นที่ควบคุมเฉพาะ

7.1.2 การควบคุมการเข้า-ออกทางกายภาพ (Physical Entry Controls)

(1) มาตรการรักษาความปลอดภัยทางกายภาพและมาตรการควบคุมบุคคล ผ่านเข้า-ออกของพื้นที่ควบคุม และพื้นที่ควบคุมเฉพาะให้เป็นไปตามประกาศบริษัทฯ

(2) กำหนดมาตรการรักษาความปลอดภัยทางกายภาพและมาตรการควบคุมบุคคล ผ่านเข้า-ออกพื้นที่ศูนย์ข้อมูล (Data Center) เพิ่มเติมดังนี้

- พื้นที่ศูนย์ข้อมูล (Data Center) ต้องมีระบบควบคุมการเข้า-ออก เพื่อพิสูจน์ตัวตนของผู้ใช้พื้นที่ศูนย์ข้อมูล (Data Center) เฉพาะผู้มีหน้าที่เกี่ยวข้อง
- มีระบบบันทึกการเข้า-ออกพื้นที่ศูนย์ข้อมูล (Data Center) และต้องบันทึกรายละเอียดเกี่ยวกับบุคคล เวลาผ่านเข้า- ออก แล้วเหตุผลหรือความจำเป็นของการเข้าใช้งาน
- กรณีบุคคลภายนอกมีความจำเป็นต้องเข้า-ออกพื้นที่ศูนย์ข้อมูล (Data Center) ต้องได้รับอนุญาตจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ และ/หรือผู้บริหารที่ได้รับมอบหมาย และผู้ดูแลระบบคอมพิวเตอร์ต้องอยู่กับบุคคลภายนอกตลอดระยะเวลาการปฏิบัติงานของบุคคลภายนอก ต้องตรวจสอบเหตุผลและความจำเป็น ก่อนที่จะอนุญาต หรือไม่อนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราว ต้องมีการบันทึกข้อมูลการเข้าออกห้องคอมพิวเตอร์แม่ข่าย (Data Center) ของบุคคลภายนอกทุกครั้ง พร้อมทั้งจัดเก็บบันทึกดังกล่าวไว้อย่างน้อย 1 ปี
- ห้ามถ่ายภาพ สูบบุหรี่ นำอาหารและเครื่องดื่มเข้ามาในบริเวณศูนย์ข้อมูล (Data Center)

7.1.3 กำหนดมาตรการการเข้า-ออกทางกายภาพเพิ่มเติมของพื้นที่ควบคุมเฉพาะในส่วนของพื้นที่ติดตั้งอุปกรณ์คอมพิวเตอร์สำหรับผู้ใช้งานดังนี้

(1) ผู้ใช้งานต้องไม่เปิดประตูสำนักงานทิ้งไว้หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่สำนักงานโดยเด็ดขาด เว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัว หรือบัตรผู้มาติดต่อได้ เพื่อเป็นการป้องกันการเข้าถึงพื้นที่สำนักงานและพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ได้รับอนุญาตไม่สามารถโอนกรรมสิทธิ์หรือหยิบยืมใช้งานแทนกันได้

(2) ผู้ใช้งานต้องปิดล็อคตู้เซฟ ตู้เอกสาร ลิ้นชัก และตู้อุปกรณ์ต่างๆ อย่างเหมาะสม โดยกุญแจที่ปิดล็อคดังกล่าวจะต้องถูกเก็บรักษาไว้อย่างปลอดภัย

(3) ผู้ใช้งานต้องไม่ทิ้งข้อมูล สื่อบันทึก และอุปกรณ์ที่จัดเก็บข้อมูลลับไว้บนโต๊ะทำงาน ในห้องประชุม หรือในตู้ที่ไม่ได้ล็อกกุญแจโดยเด็ดขาด

7.1.4 กำหนดมาตรการการเข้า-ออกทางกายภาพของพื้นที่ควบคุมที่เป็นพื้นที่ขนส่งและส่งมอบเพิ่มเติมดังนี้

(1) ผู้ดูแลอาคารและสถานที่ต้องจำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายอุปกรณ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(2) จัดพื้นที่ส่งมอบไว้ในบริเวณต่างหากเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่นๆ ภายในบริษัทฯ

(3) ตรวจนับและลงทะเบียนหรือขึ้นบัญชีคุมอุปกรณ์ที่ส่งมอบโดยผู้ถูกจ้าง ผู้ขาย หรือผู้ให้บริการภายนอก

7.1.5 การป้องกันภัยพิบัติและภัยคุกคามจากภายนอก (Protecting Against External and Environment) เพื่อประโยชน์ในการรักษาความปลอดภัยสถานที่ติดตั้งและเก็บทรัพย์สินเทคโนโลยีสารสนเทศ ต้องจัดให้มีการป้องกันต่อภัยคุกคามต่างๆ ได้แก่ อัคคีภัย ความไม่สงบของบ้านเมือง หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ พร้อมทั้งให้ทดสอบระบบรักษาความปลอดภัยภายในขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

7.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment) ดังนี้

7.2.1 การจัดตั้งและการป้องกันอุปกรณ์ (Equipment Setting and Protection)

(1) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อให้เกิดความเป็นระเบียบเรียบร้อย และไม่เกิดความเสี่ยงจากความร้อน แสงแดด ฝุ่นละออกและความชื้น

(2) อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่งที่มีความมั่นคงปลอดภัย

(3) ดำเนินการตรวจสอบสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศ อยู่ภายในเพื่อห้องกันความเสียหายต่ออุปกรณ์ ตรวจสอบระดับอุณหภูมิ ความชื้น ให้อยู่ในระดับปกติ

(4) ไม่นำอุปกรณ์เทคโนโลยีสารสนเทศ ข้อมูลเทคโนโลยีสารสนเทศ หรือซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานของบริษัทโดยมิได้รับอนุญาติ

7.2.2 การดูแลอุปกรณ์ต่าง ๆ (Supporting Utilities)

(1) ระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศ ที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้ ระบบสำรองกระแสไฟฟ้า (UPS) เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator) ระบบระบายอากาศ ระบบปรับอากาศ และควบคุมความชื้น ระบบดังเพลิง ระบบกล้องวงจรปิด

(2) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านี้อย่างสม่ำเสมอเพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

7.2.3 การเดินสายไฟและสายเคเบิล (Cabling Security) ฝ่ายเทคโนโลยีสารสนเทศ มีการดูแลให้การติดตั้งและการบำรุงรักษาสายไฟและสายสื่อสารในพื้นที่ปฏิบัติงานและห้องคอมพิวเตอร์เป็นไปตามมาตรฐานความปลอดภัยอุตสาหกรรม เพื่อป้องกันไม่ให้มีการเข้าถึงหรือดักจับข้อมูล หรือเกิดความเสียหายทางกายภาพ

7.2.4 การดูแลรักษาอุปกรณ์ (Equipment Maintenance)

(1) ฝ่ายเทคโนโลยีสารสนเทศ มีการควบคุมดูแลให้อุปกรณ์ระบบเทคโนโลยีสารสนเทศ หลักทั้งหมดซึ่งใช้ในการประมวลผลในระดับปฏิบัติการ รวมถึงอุปกรณ์สนับสนุนกการทำงานได้รับการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่ผู้ผลิตแนะนำ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้งาน

(2) ฝ่ายเทคโนโลยีสารสนเทศ มีการควบคุมให้มีการบันทึกกิจกรรมการบำรุงอุปกรณ์ รวมถึงบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ให้อยู่ในสภาพพร้อมใช้งานเสมอ

7.2.5 การนำสินทรัพย์ขององค์กรออกนอกสำนักงาน (Removal of Asset)

(1) ผู้ทำหน้าที่กำกับดูแลพื้นพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยและอาคารสถานที่ ต้องไม่อนุญาตให้นำอุปกรณ์เทคโนโลยีสารสนเทศ ออกจากองค์กร ยกเว้นจะมีการอนุญาตให้นำออกโดยผู้ที่ได้รับมอบหมายในการอนุญาตให้นำทรัพย์สินออก

(2) ผู้ใช้งาน ต้องไม่นำอุปกรณ์เทคโนโลยีสารสนเทศ ข้อมูลเทคโนโลยีสารสนเทศ หรือซอฟต์แวร์ออกนอกองค์กร ยกเว้นจะได้รับอนุญาตจากผู้ที่ได้รับมอบผู้มายในการอนุญาตให้นำทรัพย์สินออก

(3) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดขั้นตอนปฏิบัติสำหรับการนำทรัพย์สินออกนอกสำนักงานอย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม

7.2.6 การป้องกันอุปกรณ์และสินทรัพย์เทคโนโลยีสารสนเทศ ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment and asset Off-Premises)

(1) กำหนดให้ผู้บริหารระดับฝ่ายขึ้นไป เป็นผู้มีอำนาจในการอนุญาตให้นำอุปกรณ์เทคโนโลยีสารสนเทศขององค์กรไปใช้งานภายนอกสำนักงาน และต้องกำหนดให้มีการป้องกันอุปกรณ์เทคโนโลยีสารสนเทศต่างๆ ที่ใช้งานอยู่ภายนอกสำนักงานเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์ โดยพิจารณาจากความเสี่ยงที่อาจเกิดขึ้นกับอุปกรณ์เหล่านั้น

(2) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดมาตราการความมั่นคงปลอดกันในการควบคุมทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน เพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์ทรัพย์สิบขององค์กรออกไปใช้งาน

7.2.7 การจัดการอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้ใหม่ (Secure Disposal or Re-use of Equipment)

(1) ผู้ใช้งาน ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อให้มั่นใจว่าข้อมูลเทคโนโลยีสารสนเทศ ที่สำคัญหรือซอฟต์แวร์ลิขสิทธิ์ที่อยู่ภายในสื่อบันทึกข้อมูลได้มีการลบ ย้าย หรือทำลายอย่างเหมาะสมตามลำดับขั้นความลับข้อมูล ก่อนที่จะทำลายหรือจำหน่ายอุปกรปกรณ์หรือนำอุปกรณ์กลับมาใช้ใหม่

(2) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดทำขั้นตอนปฏิบัติสำหรับการทำรายข้อมูลหรือหรือทรัพย์สินเทคโนโลยีสารสนเทศ และมาตรการสำหรับการทำลายข้อมูลเพื่อนำอุปกรณ์เทคโนโลยีสารสนเทศ กลับมาใช้งานซ้ำ โดยต้องมีความสอดคล้องกับการจัดลำดับชั้นความลับข้อมูล และต้องกำหนดผู้รับผิดชอบในการทำหน้าที่ทำลายข้อมูลเทคโนโลยีสารสนเทศ ที่ไม่จำเป็นต่อการดำเนินกิจการขององค์กรซึ่งจัดเก็บอยู่บนสื่อบันทึกข้อมูล

7.2.8 การป้องกันอุปกรณ์ของผู้ใช้งานที่ไม่มีผู้ดูแล (Unattended User Equipment)

(1) ผู้ใช้งานต้องออกจากระบบเทคโนโลยีสารสนเทศ โดยทันทีเมื่อเสร็จสิ้นการปฏิบัติงาน และปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อเสร็จสิ้นการปฏิบัติงานประจำวัน

(2) ผู้ใช้งานต้องล็อคอุปกรณ์เมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

(3) ผู้ใช้งานต้องปิด ล็อกพื้นที่เพื่อจัดเก็บอุปกรณ์ในสถานที่ปลอดภัยเมื่อไม่มีการใช้งาน

(4) กำหนดให้เครื่องคอมพิวเตอร์พักหน้าจอเมื่อไม่มีผู้ใช้งานนานเกินกว่า 15 นาที และมีการใส่รหัสผ่านในการเข้าถึงใหม่อีกครั้ง

7.2.9 การควบคุมการไม่ทิ้งสินทรัพย์เทคโนโลยีสารสนเทศ ที่สำคัญไว้ในที่ไม่ปลอดภัย (Clear Desk and Clear Screen Policy) ผู้ควบคุมระบบต้องควบคุมให้มีการล็อคหน้าจอคอมพิวเตอร์เมื่อไม่ได้ใช้งาน (Clear Screen) เช่น การตัดออกจากระบบ (Session time out) และการล็อคหน้าจอ (Lock Screen) อัตโนมัติ เป็นต้น

หมวดที่ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security)

8.1 หน้าที่ความรับผิดชอบและการปฏิบัติงาน (Operation Procedures and Responsibilities)

8.1.1 ขั้นตอนการปฏิบัติงานให้เป็นลายลักษณ์อักษร (Document Operating Procedures)

(1) ผู้ดูแลระบบฯต้องจัดทำเอกสารวิธีปฏิบัติที่เหมาะสมสำหรับแต่ละระบบเทคโนโลยีสารสนเทศ ที่อยู่ในความรับผิดชอบของตนและประกาศให้ผู้ปฏิบัติงานทราบ

(2) ผู้ดูแลระบบฯ ต้องปรับปรุงเอกสารวิธีปฏิบัติตามความเหมาะสมต่อสภาวะแวดล้อมการปฏิบัติงาน

(3) ผู้ดูแลระบบฯ มีการป้องกันมิให้ข้อมูลหรือเอกสารเกี่ยวกับระบบเทคโนโลยีสารสนเทศ ถูกเข้าถึงโดยมิได้รับอนุญาต

8.2 การจัดการการเปลี่ยนแปลง (Change Management)

จัดทำขึ้นเพื่อเป็นแนวทางปฏิบัติสำหรับการควบคุมติดตามการเปลี่ยนแปลงหรือแก้ไขให้ดำเนินการผ่านระบบที่ถูกจัดเตรียมไว้และช่วยลดผลกระทบหรือให้เกิดผลกระทบน้อยที่สุดโดยมีแผนงานในการกู้คืนหรือย้อนกลับสู่สถานะตั้งต้นในกรณีที่การดำเนินการเปลี่ยน (Rollout) นั้นไม่สามารถดำเนินการสำเร็จหรือเกิดข้อผิดพลาดขึ้น

8.3 การจัดการขีดความสามารถ (Capacity Management)

8.3.1 เพื่อใช้เป็นมาตรฐานการตั้งค่าของระบบปฏิบัติการ ระบบฐานข้อมูลและอุปกรณ์เครือข่ายสื่อสารต่างๆ อย่างเป็นลายลักษณ์อักษร

8.3.2 มีการประเมินแนวโน้มการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศสอดคล้องกับการประมาณการ (Forecasting)ปริมาณธุรกรรมและปริมาณลูกค้าในภาวะปกติและภาวะวิกฤตที่อาจจะเกิดขึ้นทั้งในปัจจุบันและอนาคต เพื่อวางแผนรองรับการใช้งานในอนาคต (capacity planning)โดยครอบคลุมทั้งระบบหลักและระบบสำรอง

8.3.3 มีกระบวนการหรือแนวทางในการขยายขีดความสามารถของระบบและโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ ให้ทันต่อความต้องการใช้งาน และการรองรับการพร้อมทำงานโดยอัตโนมัติเมื่อเกิดเหตุฉุกเฉิน รวมทั้งมีกระบวนการหรือเครื่องมือในการติดตามประสิทธิภาพและความเพียงพอของการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศของระบบ

8.3.4 มีการกำหนดตัวชี้วัดการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ (threshold และ trigger) ในระดับต่างๆ เช่นตัวชี้วัดด้านความพร้อมใช้(Availability) ขีดความสามารถ (Capacity) ประสิทธิภาพการทำงาน (Performance) ของระบบและโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ เป็นต้นโดยครอบคลุมการเชื่อมต่อตั้งแต่ช่องทางการให้บริการจนถึงระบบประมวลผล รวมถึงผู้ให้บริการภายนอก (End-t-end)เพื่อให้มีการแจ้งเตือนผู้เกี่ยวข้องอย่างทันท่วงทีและสามารถวิเคราะห์ปัญหาและแนวทางการรับมือที่เหมาะสม รวมถึงการประสานงานกับหน่วยงานทั้งภายในและภายนอกกรณีเกิดเหตุขัดข้องo-end)เพื่อให้มีการแจ้งเตือนผู้เกี่ยวข้องอย่างทันท่วงทีและสามารถวิเคราะห์ปัญหาและแนวทางการรับมือที่เหมาะสม รวมถึงการประสานงานกับหน่วยงานทั้งภายในและภายนอกกรณีเกิดเหตุขัดข้อง

8.3.5 ผู้ดูแลระบบฯต้องเฝ้าติดตามสังเกตการใช้งานทรัพยากรเทคโนโลยีสารสนเทศ และมีการติดตามประเมินผลการติดตามสังเกตดังกล่าวอย่างสม่ำเสมอ โดยครอบคลุมทั้งระบบหลักและระบบสำรอง เพื่อวางแผนบริหารทรัพยากรเทคโนโลยีสารสนเทศ ให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม (Capacity Planning) อย่างน้องปีละ 1 ครั้ง

8.3.6 กำหนดกระบวนการดำเนินงาน เพื่อรับมือเหตุการณ์การใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศหรือการใช้ประสิทธิภาพของระบบงานเกินขีดจำกัดของตัวชี้วัดที่กำหนดไว้เช่นการจำกัดการให้บริการบางช่องทางหรือตัดการเชื่อมต่อกับผู้ให้บริการหรือบุคคลภายนอกที่มีผลกระทบต่อระบบ เช่นสถาบันการเงินผู้รับโอนเงินผู้ให้บริการ Bill Payment เป็นต้น

8.3.7 จัดทำรายงานความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศนำเสนอต่อคณะกรรมการที่ได้รับมอบหมายหรือผู้บริหารระดับสูงที่เกี่ยวข้องรับทราบอย่างสม่ำเสมอ เพื่อให้มีการกำกับดูแลความพร้อมและความเพียงพอของระบบในการรองรับการให้บริการทางธุรกิจได้อย่างต่อเนื่องรวมทั้งเพื่อพิจารณาแนวทางลดความเสี่ยงได้ทันการ

8.4 การบริหารจัดการการตั้งค่าระบบ (System Configuration)

8.4.1 กระบวนการในการควบคุมหรือแก้ไขเปลี่ยนแปลงการตั้งค่าของระบบที่ใช้งานจริง โดยจัดทำ minimum baseline standard เพื่อใช้เป็นมาตรฐานการตั้งค่าของระบบปฏิบัติการ ระบบฐานข้อมูลและอุปกรณ์เครือข่ายสื่อสารต่างๆ อย่างเป็นลายลักษณ์อักษร

8.4.2 การจัดเก็บการเปลี่ยนแปลงของการตั้งค่าระบบ (System Configuration Version Control)

8.4.3 การเปลี่ยนแปลงการตั้งค่าบนระบบที่ให้บริการจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงเพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

8.4.4 การสอบทานการตั้งค่าบนระบบที่ให้บริการจริงอย่างสม่ำเสมอ

8.4.5 การขออนุมัติยกเว้น (Exception) กรณีมีความจำเป็นต้องตั้งค่าที่ไม่เป็นไปตามเอกสารมาตรฐานการตั้งค่า

8.5 การบริหารจัดการ Patch (Patch Management)

8.5.1 กระบวนการควบคุมการติดตั้ง Patch ของระบบที่ใช้งานจริงทุกครั้งก่อนนำไปติดตั้งบนระบบที่ให้บริการจริง เพื่อให้สามารถติดตั้ง Patch ที่สำคัญในการรักษาความปลอดภัยได้ทันการณ์

8.5.2 การตรวจสอบความถูกต้องของ Patch และการประเมินความเสี่ยงและความจำเป็นในการติดตั้ง Patch

8.5.3 มีการทบทวนและปรับปรุงกระบวนการบริหารจัดการ patch อย่างสม่ำเสมอ

8.5.4 การจัดการเปลี่ยนแปลงของการติดตั้ง Patch (Patch Version Control) โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ

8.5.5 การทดสอบ Patch ก่อนนำไปติดตั้งบนระบบที่ให้บริการจริงและการอนุมัติเพื่อติดตั้ง Patch บนระบบที่ให้บริการจริง กรณีมีเหตุผู้ผลิตระบบงานหรืออุปกรณ์ยังไม่แจ้งการปรับปรุง security patch อย่างเป็นทางการเพื่อปิดช่องโหว่ใหม่ๆ ที่เพิ่งค้นพบ บริษัทต้องจัดให้มีการควบคุมอื่นทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีจากช่องโหว่นั้นๆ

8.6 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Control Against Malware)

8.6.1 เครื่องคอมพิวเตอร์ลูกขาย และเครื่องคอมพิวเตอร์แบบพกพาต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัสที่ได้รับการ อัพเดทข้อมูลจากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการป้องกันไวรัส และต้องเปิดใช้งานตลอดเวลาที่ใช้เครื่อง

8.6.2 เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริหารป้องกันไวรัส ต้องมีการอัพเดทข้อมูลล่าสุดอยู่สมอ

8.6.3 ผู้ใช้งานต้องตรวจสอบไฟล์แนบที่มากับจดหมายอิเล็กทรอนิกส์ (e-mail) หรือไฟล์ที่ได้รับมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

8.6.4 ห้ามผู้ใช้งานสร้าง เก็บ หรือเผยแพร่โปรแกรมไม่ประสงค์ดีเข้าสู่ระบบคอมพิวเตอร์ ขอบบริษัท

8.6.5 ห้ามผู้ใช้งานขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส

8.6.6 เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องให้ปิดฟังก์ชันการทำงานเชื่อมต่อกับอินเทอร์เน็ต ยกเว้นในกรณีที่จำเป็นต้องใช้เท่านั้น เพื่อเป็นการป้องกันไม่ให้โปรแกรมไม่ประสงค์ดีมีผลกระทบกับข้อมูลที่สำคัญบนเครื่องคอมพิวเตอร์แม่ข่ายเหล่านี้

8.7 กำหนดการควบคุมการรักษาความปลอดภัยในอุปกรณ์ด้านเทคโนโลยีสารสนเทศของบริษัทฯที่ใช้ปฏิบัติงาน (Endpoint)

8.7.1 กำหนดเอกสารมาตรฐานการตั้งค่า Security Baseline สำหรับอุปกรณ์ที่ใช้ปฏิบัติงานทั้งอุปกรณ์ดังกล่าวเพื่อป้องกันความเสี่ยงจากโปรแกรมไม่ประสงค์ดี (Malware) และการรั่วไหลของข้อมูล เช่น การติดตั้งโปรแกรมที่ได้รับอนุญาต

8.7.2 กำหนดการควบคุม เช่น การติดตั้งโปรแกรมป้องกันไวรัสหรือระบบตรวจจับการแฝงตัวของโปรแกรมไม่ประสงค์ดี (Malware) และอัพเดทโปรแกรมอย่างสม่ำเสมอมีกระบวนการหรือเครื่องมือในการตรวจจับ คัดกรองสกัดกั้น เพื่อป้องกันข้อมูลสำคัญรั่วไหล (Data Leakage Prevention: DLP) การควบคุมการใช้สื่อบันทึกข้อมูลพกพา (Removable Media) เป็นต้น

8.8 การนำอุปกรณ์ส่วนตัว (Bring Your Own Device: BYOD) มาใช้ในการปฏิบัติงานให้ฝ่ายเทคโนโลยีสารสนเทศกำหนดกระบวนการบริหารจัดการอุปกรณ์ส่วนตัว ตั้งแต่การลงทะเบียน การต่ออายุ และการยกเลิกใช้งาน และจัดให้มีการทบทวนปีละ 2 ครั้ง

8.9 การสำรองข้อมูล (Data Backup)

8.9.1 ผู้ดูแลระบบฯ ต้องจัดให้มีการสำรองและทดสอบการกู้คนข้อมูลอย่างน้องปีละ 1 ครั้ง

8.9.2 ผู้ดูแลระบบฯ ต้องจัดทำบันทึกการสำรองข้อมูล (Operation Logs)

8.9.3 ผู้ดูแลระบบฯ ต้องจัดทำรายงานข้อผิดพลาด (Fault Logging) ที่เกิดจากการสำรองข้อมูลรวมทั้งวิธีการแก้ไข

8.9.4 กำหนดชนิดและช่วงเวลาของการสำรองข้อมูล พร้อมทั้งสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมี 2 ชนิด คือ การสำรองข้อมูลแบบเต็ม และการสำรองข้อมูลแบบเพิ่มส่วนต่างในกรณีพบปัญหาทำให้ไม่สามารถสำรองข้อมูลได้อย่างครบถ้วนสมบูรณ์ให้ผู้ดูแล จัดการระบบงานดำเนินการแก้ไขปัญหา และสรุปผลให้ผู้บังคับบัญชาทราบ

8.9.5 ผู้ใช้งานต้องสำรองข้อมูลตามความจำเป็นและเหมาะสมไว้บนสื่อบันทึกอื่น ๆ เป็นประจำทุกเดือน

8.9.6 ผู้ใช้งานต้องรักษาสื่อบันทึกข้อมูลสำรอง ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และห้ามนำข้อมูลไปเปิดเผยต่อบุคคลภายนอกบริษัทฯ โดยตั้งใจ หรือไม่ตั้งใจ

หมายเหตุ : ผู้ดูแลระบบฯ ต้องจัดทำ Backup configuration baseline แต่ละ application เพื่อใช้ในการตรวจสอบและเป็นมาตรฐานในการปฏิบัติงาน

8.10 การสำรองข้อมูล (Information Backup)

8.10.1 ผู้ดูแลระบบฯและเจ้าของข้อมูลทำบัญชีรายชื่อข้อมูลที่มีความสำคัญและปรับปรุงบัญชีรายชื่อให้มีความทันสมัยอยู่เสมอ

8.10.2 ผู้ดูแลระบบฯกำหนดชนิดของข้อมูลที่มีความจำเป็นต้องสำรองข้อมูลไว้อย่างน้อยต้องประกอบด้วยข้อมูลในฐานข้อมูลของระบบเทคโนโลยีสารสนเทศ หรือไฟล์ข้อมูลที่เกี่ยวข้อง

8.10.3 ผู้ดูแลระบบฯ กำหนดความถี่ในการสำรอบข้อมูล

8.11 การจัดเก็บข้อมูลบันทึกเหตุการณ์และติดตาม (Logging and Monitoring)

8.11.1 ให้ฝ่ายเทคโนโลยีสารสนเทศ ดำเนินการจัดเก็บข้อมูลบันทึกเหตุการณ์และติดตาม (Event logging) ดังนี้ จัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging) ของเครื่องแม่ข่าย ระบบงาน ระบบปฏิบัติการ และอุปกรณ์เครือข่ายที่สำคัญ โดยครอบคลุมถึงการบันทึกการเข้าถึงระบบ (Access Log) และการบันทึกกิจกรรมการดำเนินการ (Activity Log) ที่สำคัญของผู้ใช้งาน รวมถึงกิจกรรมการดูแลระบบของผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศที่มีสิทธิ์สูง ไว้เป็นหลักฐาน เพื่อให้สามารถติดตาม และตรวจสอบการเข้าถึงและการใช้งานได้ และต้องกำหนดให้มีการตรวจสอบข้อมูล บันทึกเหตุการณ์ (Log Review) อย่างสม่ำเสมอ เพื่อวิเคราะห์และตรวจหาเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่างๆ รวมทั้งให้มีการวิเคราะห์ข้อมูล ล็อกดังกล่าวอย่างสม่ำเสมอ และจัดการแก้ไขข้อผิดพลาดอย่างเหมาะสม รวมถึงป้องกันการปฏิเสธการรับผิด

8.11.2 ควบคุมให้อุปกรณ์ในการบันทึกเหตุการณ์ และข้อมูลบันทึกเหตุการณ์ (Log) ได้รับการป้องกันจากการเข้าถึงหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต และมีรายละเอียดที่ครบถ้วนเพียงพอที่จะใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวบุคคลผู้กระทำได้และจัดเก็บย้อนหลังเป็นระยะเวลาอย่างน้อย 90 วัน หรือตามกฎหมายที่เกี่ยวข้องกำหนด

8.11.3 ตั้งค่าเวลาของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่ายสื่อสาร มีความสอดคล้องตรงกันกับเครื่องแม่ข่าย Network Time Protocol: NTP (clock synchronization) เพื่อให้ค่าบันทึกมีความถูกต้องเป็นแบบ real-time และตรงกับแหล่งเวลาอ้างอิงที่เชื่อถือได้

8.12 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (Security Monitoring)

8.12.1 จัดให้มีขั้นตอนการปฏิบัติงานในการติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม โดยกำหนดกระบวนการหรือใช้เครื่องมือในการตรวจจับเหตุการณ์ผิดปกติ (logging) หรือภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศที่สำคัญ ครอบคลุมระดับระบบปฏิบัติการระบบจัดการฐานข้อมูล ระบบงาน และระบบเครือข่าย เพื่อให้สามารถตรวจจับ ป้องกัน และรับมือเหตุการณ์ผิดปกติและภัยคุกคามได้อย่างทันท่วงทีและมีความต่อเนื่อง

8.12.2 กำหนดกระบวนการหรือใช้เครื่องมือในการรับข้อมูลจากแหล่งข้อมูลที่เชื่อถือได้ รวมถึงกำหนดผู้รับผิดชอบในการประสานงานแลกเปลี่ยนข้อมูลกับหน่วยงานที่เกี่ยวข้อง เพื่อวิเคราะห์และหาแนวทางจัดการข้อมูลภัยคุกคามที่อาจเกิดขึ้นอย่างต่อเนื่อง ครอบคลุมถึงลักษณะการโจมตี ความเป็นไปได้ที่จะ

เกิดเหตุการณ์ภัยคุกคาม รวมถึงวิธีการรับมือกับภัยคุกคามนั้น เพื่อนำมาใช้สนับสนุนการรับมือภัยคุกคามทางไซเบอร์

8.12.3 ในกรณีที่พบภัยคุกคามที่ส่งผลกระทบอย่างมีนัยสำคัญต่อบริษัทฯ ให้รายงานผู้บริหารระดับสูงที่ดูแลฝ่ายเทคโนโลยีสารสนเทศ ฝ่ายตรวจสอบภายในและบริหารความเสี่ยง และคณะกรรมการบริหาร และดำเนินการตรวจสอบสาเหตุหรือช่องโหว่ของระบบ และดำเนินการปิดช่องโหว่และป้องกันความเสี่ยงที่อาจเกิดขึ้นอีก

8.13 การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (Technical Vulnerability Management)

8.13.1 กำหนดขั้นตอนการปฏิบัติงานในการบริหารจัดการช่องโหว่ (Vulnerability Management) ของระบบเทคโนโลยีสารสนเทศตามระดับความเสี่ยงเพื่อให้ทราบถึงช่องโหว่และกำหนดแนวทางในการดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นโดยครอบคลุมถึงการประเมินช่องโหว่ของระบบเทคโนโลยีสารสนเทศที่สำคัญทุกระบบอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีระบบงานใหม่

8.13.2 การรายงานผลประเมินช่องโหว่ไปยังเจ้าหน้าที่ผู้รับผิดชอบรวมทั้งมีการติดตามการดำเนินการปรับปรุงแก้ไข และนำเสนอความคืบหน้าการดำเนินการต่อผู้บริหารระดับสูงที่ดูแลฝ่ายเทคโนโลยีสารสนเทศ ฝ่ายตรวจสอบภายในและบริหารความเสี่ยง และคณะกรรมการบริหารรับทราบ

8.14 กำหนดขั้นตอนการปฏิบัติงานในการทดสอบเจาะระบบ (penetration test)

8.14.1 การจัดให้มีผู้เชี่ยวชาญภายในหรือภายนอกที่มีความเป็นอิสระ ทำหน้าที่ทดสอบเจาะระบบ โดยเฉพาะระบบงานและระบบเครือข่ายที่มีการเชื่อมต่อกับระบบเครือข่ายสื่อสารสาธารณะ (Internet Facing) อย่างน้อย 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันท่วงที

8.14.2 การติดตามการดำเนินการปรับปรุงแก้ไขและนำเสนอความคืบหน้าการดำเนินการต่อผู้บริหารระดับสูงที่ดูแลฝ่ายเทคโนโลยีสารสนเทศ ฝ่ายตรวจสอบภายในและบริหารความเสี่ยง และคณะกรรมการบริหารรับทราบ

8.14.3 กำหนดกระบวนการรวบรวมและวิเคราะห์ช่องโหว่ทางด้านเทคนิคที่ตรวจพบเพื่อกำหนดมาตรการรักษาความปลอดภัยต่อไป

หมวดที่ 9 การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications Security)

9.1 การบริหารจัดการความมั่นคงปลอดภัยสำหรับเครือข่าย (Network Security Management)

9.1.1 พนักงานต้องใช้บริการระบบเครือข่ายตามที่ผู้ดูแลระบบเครือข่ายอนุญาตเท่านั้น

9.1.2 พนักงานต้องใช้ระบบเครือข่ายที่ไม่กระทบต่อประสิทธิภาพการใช้งานเครือข่ายโดยรวม เช่น การรับ-ส่งไฟล์ขนาดใหญ่ การดาวน์โหลดหรืออัพโหลดไฟล์ที่มีขนาดใหญ่ ฟังเพลงออนไลน์ ดูทีวี หรือวิดีโอออนไลน์ เล่นเกมออนไลน์ ในระหว่างเวลาปฏิบัติงาน เป็นต้น

9.1.3 ห้ามพนักงานนำอุปกรณ์เครือข่ายเชื่อมต่อกับระบบเครือข่ายของบริษัทฯ ก่อนได้รับอนุญาตจากผู้ดูแลระบบเครือข่าย

9.1.4 มีการแบ่งแยกเครือข่าย private network และ public network เพื่อจำกัดการเข้าถึง และความปลอดภัย โดยจะจัดให้มีอุปกรณ์รักษาความปลอดภัยเครือข่าย

9.1.5 ห้ามใช้เครือข่ายเพื่อกระทำสิ่งผิดกฎหมาย

9.1.6 ผู้ใช้งานต้องเข้าใช้ระบบเครือข่ายด้วยบัญชีผู้ใช้งานของตัวเองเท่านั้น ยกเว้นผู้ที่ได้รับการอนุญาตจากคณะกรรมการบริหาร

9.1.7 ห้ามเผยแพร่ข้อมูลของผู้อื่นหรือของบริษัทฯ โดยไม่ได้รับอนุญาต

9.2 การควบคุมระบบเครือข่าย (Network Controls)

9.2.1 ผู้ดูแลเครือข่ายต้องจำกัดการเข้าถึงระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ ที่เชื่อมต่ออยู่กับระบบเครือข่าย โดยกำหนดให้ผู้ใช้งานในเครือข่ายสามารถเข้าถึงระบบเทคโนโลยีสารสนเทศ ผ่านทางระบบเครือข่ายได้แต่เพียงบริการที่อนุญาตให้เข้าถึงเท่านั้น

9.2.2 ผู้ดูแลระบบเครือข่ายต้องทดสอบความปลอดภัยทุกครั้งที่จะเชื่อมต่อกับระบบเครือข่ายของบุคคลภายนอก เพื่อให้มั่นใจว่าไม่มีการเข้าถึงทรัพยากรของบริษัทฯ โดยไม่ได้รับอนุญาต

9.2.3 ผู้ดูแลระบบเครือข่ายต้องควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่ายโดยไม่ได้รับอนุญาต

9.2.4 การเข้าถึงอุปกรณ์เครือข่ายเพื่อการตรวจสอบและปรับแต่งระบบทั้งทางกายภาพและการเข้าถึงจากระยะไกล (remote access) ต้องมีการควบคุมและทำได้เพียงเฉพาะผู้ดูแลระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น และกระทำผ่านช่องทางที่มีความปลอดภัยเช่น SSH, VPN หรือ SSL/TLS เป็นต้น

9.2.5 ในกรณีที่ต้องกำหนดสิทธิการเข้าถึงแบบชั่วคราวแก่บุคคลภายนอก ผู้ดูแลระบบเครือข่ายต้องให้มีผู้ควบคุมตรวจสอบและยกเลิกสิทธิการเข้าถึงทันทีที่ปฏิบัติงานเสร็จ

9.2.6 ผู้ดูแลระบบเครือข่ายต้องกำหนดค่าเริ่มต้นพื้นฐานของทุกระบบเครือข่ายต้องเป็นอนุญาตบางส่วนและปฏิเสธทั้งหมด (Permit any & Deny all)

9.2.7 ผู้แลระบบเครือข่ายต้องตรวจสอบและปิดพอร์ตของอุปกรณ์เครือข่ายที่ไม่ได้งาน

9.2.8 การให้บริการทางเครือข่ายสำหรับเครื่องคอมพิวเตอร์แม่ข่าย ผู้ดูแลระบบเครือข่ายต้องอนุญาตเฉพาะพอร์ต (Port) การเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น

9.2.9 เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบเทคโนโลยีสารสนเทศ ต่างๆ ต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

9.2.10 ผู้ดูแลระบบเครือข่ายต้องตรวจสอบ Security Log เพื่อค้นหา Invalid Attempt Access ของผู้บุกรุกและตรวจสอบ Fault Alarm Log เพื่อการตรวจสอบปัญหาที่เกิดขึ้นประจำวัน

9.2.11 ผู้ดูแลระบบเครือข่ายต้อง Update Security Patch ของอุปกรณ์เครือข่าย อย่างสม่ำเสมอ

9.2.12 ผู้ดูแลระบบเครือข่ายต้องจัดทำบันทึกสรุปการเกิดปัญหากับระบบเครือข่ายและแนวทางแก้ไข

9.2.13 ผู้ดูแลระบบเครือข่ายต้องสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์เครือข่ายเป็นประจำหรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

9.2.14 ผู้ดูแลระบบเครือข่ายต้องจัดทำแผนผังเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในบริษัทฯ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

9.2.15 ผู้ดูแลระบบเครือข่ายต้องตั้งชื่ออุปกรณ์เครือข่ายให้เป็นไปตามมาตรฐานเทคโนโลยีสารสนเทศและการสื่อสารที่กำหนด

9.2.16 ผู้ดูแลระบบเครือข่ายต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องกับกฎหมาย

9.2.17 ให้มีการระบุอุปกรณ์ที่เชื่อมต่อเข้ากับระบบเทคโนโลยีสารสนเทศ โดยอัตโนมัติ (Automatic equipment identification) เพื่อตรวจสอบการเชื่อมต่อของอุปกรณ์ดังกล่าวว่ามาจากอุปกรณ์ดังกล่าวจริงหรือจากสถานที่ที่กำหนดไว้เท่านั้น ทั้งนี้ระบบเทคโนโลยีสารสนเทศจะรับการเชื่อมต่อจากเฉพาะอุปกรณ์ ที่ได้รับอนุญาตหรือมาจากเฉพาะสถานที่ที่ได้รับอนุญาตเท่านั้น

9.3 การแบ่งแยกระบบเครือข่าย (Segregation in Networks) กำหนดให้มีการแบ่งแยกระบบเครือข่ายตามกลุ่มบริการเทคโนโลยีสารสนเทศ ผู้ใช้งาน และระบบ ดังนี้เป็นอย่างน้อย

9.3.1 กลุ่มที่ให้บริการเทคโนโลยีสารสนเทศ เป็นระบบเครือข่ายที่สามารถเข้าถึงและใช้งานโดยผู้ใช้งาน เช่น ระบบอินทราเน็ต ระบบจดหมายอิเล็กทรอนิกส์ เป็นต้น

9.3.2 กลุ่มให้บริการระบบเทคโนโลยีสารสนเทศ เป็นระบบเครือข่ายที่เข้าถึงและใช้งานโดยระบบเทคโนโลยีสารสนเทศ ซึ่งต้องไม่ถูกเข้าถึงจากผู้ใช้งานโดยตรง เช่น ระบบฐานข้อมูล ระบบ Directory Service ระบบ Domain Name System (DNS) ระบบ Print Service เป็นต้น

9.3.3 กลุ่มที่ให้บริการผู้ใช้งานเป็นเครือข่ายที่สามารถเข้าถึงและใช้งานโดยเครื่องคอมพิวเตอร์ของผู้ใช้งาน

9.3.4 กลุ่มที่ให้บริการผู้ใช้งานแบบไร้สาย เป็นเครือข่ายสามารถเข้าถึงและใช้งานโดยเครื่องคอมพิวเตอร์พกพา แท็บเล็ต และสมาร์ทโฟนของผู้ใช้งาน

9.3.5 กลุ่มผู้ใช้งาน Guest สามารถ ใช้งาน เฉพาะ Internet เท่านั้น

9.4 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

9.4.1 วิธีการใดๆ ที่สามารถเข้าถึงข้อมูลหรือระบบเทคโนโลยีสารสนเทศ ได้จากระยะไกล ต้องกำหนดให้มีการพิสูจน์ตัวตนผู้ใช้งานก่อนเข้าใช้งาน

9.4.2 เจ้าของระบบเทคโนโลยีสารสนเทศ เป็นผู้ให้สิทธิแก่ผู้ใช้งานเข้าสู่ระบบจากระยะไกลตามความจำเป็นเท่านั้น

9.4.3 ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

9.4.4 ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องตรวจสอบความมั่นคงปลอดภัยการเข้าใช้งานระบบจากระยะไกลอย่างสม่ำเสมอ

9.4.5 ผู้ดูแลระบบ จัดให้มีการจัดเก็บข้อมูลการเข้าถึงข้อมูลหรือระบบเทคโนโลยีสารสนเทศ ได้จากระยะไกล เพื่อให้สามรถตรวจสอบได้

9.5 การตรวจสอบการโจมตีระบบ (Detection of attacks of system)

9.5.1 ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องจัดให้มีการใช้งานซอฟต์แวร์สำหรับการตรวจสอบการโจมตีระบบเทคโนโลยีสารสนเทศ (Network Intrusion Prevention/Detection System: NIDPS)

9.5.2 ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องจัดให้มีการเฝ้าระวังการโจมตีการทำงานของระบบเทคโนโลยีสารสนเทศอย่างต่อเนื่องผ่านระบบเครือข่ายตรวจจับแจ้งเตือน และสามารถยับยั้งการบุกรุกหรือตอบโต้การโจมตีได้โดยอัตโนมัติแบบต่อเนื่องบนระบบเครือข่ายให้เพียงพอเหมาะสมตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก เช่น โดยใช้เครื่องมือป้องกันการโจมตีเว็บไซต์(web application firewall :WAF) มาตรการป้องกันการโจมตีแบบ distributed denial of services (DDoS) และระบบป้องกันข้อมูลรั่วไหล (data leakage prevention systems : DLPS) และมีการตรวจจับไวรัสหรือโปรแกรมไม่ประสงค์ดีต่างๆ ที่อาจบุกรุกเข้าสู่เครือข่าย เป็นต้น

9.6 การถ่ายโอนข้อมูล (Information Transfer)

9.6.1 การรับ-ส่งข้อมูลหรือไฟล์อิเล็กทรอนิกส์ที่เป็นความลับระหว่างหน่วยงานภายในหรือภายนอกบริษัทฯ ต้องได้รับการเข้ารหัสข้อมูลตามนโยบายของบริษัทฯ

9.6.2 กำหนดและติดตั้งมาตรการควบคุมการรับส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) เช่น อีเมล หรือ Instant Messaging หรือ File Sharing หรือ ระบบเครือข่ายสังคมออนไลน์ เป็นต้น โดยข้อความทางอิเล็กทรอนิกส์ต้องได้รับการป้องกันอย่างเหมาะสม

9.6.3 การรักษาความลับหรือข้อตกลงการไม่เปิดเผยข้อมูล (Confidentiality or Non-Disclosure Agreements) โดยกำหนดให้มีข้อตกลงในการรักษาความลับหรือไม่เปิดเผยความลับอย่างเป็นลายลักษณ์อักษร (Non-Disclosure Agreement: NDA) กับผู้ให้บริการภายนอก

หมวดที่ 10 การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ (System Acquisition and Development and Maintenance)

10.1 การกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ (Security Requirements of Information Systems) เพื่อให้แน่ใจว่ามีการสร้างความปลอดภัยสารสนเทศให้กับระบบสารสนเทศ ตลอดวงจรการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านความปลอดภัยสารสนเทศที่ให้บริการผ่านเครือข่ายสารสนเทศ

10.1.1 การกำหนดความต้องการด้านความมั่นคงปลอดภัย (Information Security Requirements analysis and Specification)

(1) กำหนดให้มีเกณฑ์การตรวจรับ ระบบเทคโนโลยีสารสนเทศ ที่มีการปรับปรุง หรือที่มีเวอร์ชันใหม่หรือควรมีการทดสอบ ระบบเทคโนโลยีสารสนเทศ ก่อนการตรวจรับ

(2) กำหนดให้มีการระบุข้อกำหนดด้านการควบคุมความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ในการจัดทำข้อกำหนดขั้นต่อของระบบเทคโนโลยีสารสนเทศ ใหม่ หรือการปรับปรุงระบบเทคโนโลยีสารสนเทศ เดิม

(3) ข้อมูลเทคโนโลยีสารสนเทศ ที่มีการเผยแพร่ต่อสาธารณชน ให้มีการป้องกันมิให้มีการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต และเพื่อรักษาความถูกต้องครบถ้วนของข้อมูลเทคโนโลยีสารสนเทศ

(4) กำหนดให้มีข้อกำหนดขั้นต่ำสำหรับการรักษาความถูกต้องแท้จริง Authenticity และความถูกต้องครบถ้วน Integrity ของข้อมูลใน แอพพลิเคชั่น รวมทั้งมีการระบุและปฏิบัติตามวิธีการป้องกันที่เหมาะสม

(5) ต้องมีการดูแล ควบคุม ติดตามตรวจสอบการทำงานในการจ้างช่วงพัฒนาซอฟต์แวร์

10.1.2 ความมั่นคงปลอดภัยของบริการเทคโนโลยีสารสนเทศ บนเครือข่ายสาธารณะ (Securing application services on public networks)

(1) เทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการบริการเทคโนโลยีสารสนเทศ ที่มีการส่งผ่านเครือข่ายสาธารณะต้องได้รับการป้องกันและการเปิดเผย หรือเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

10.1.3 การป้องกันธุรกรรมของบริการเทคโนโลยีสารสนเทศ (Protecting application services transactions)

(1) เทคโนโลยีสารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการเทคโนโลยีสารสนเทศ ที่เกี่ยวข้องกับธุรกรรมของบริการเทคโนโลยีสารสนเทศ ต้องได้รับการป้องกันจากการรับส่งข้อมูลที่ไม่สมบูรณ์การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับ อนุญาต การส่งข้อมูลซ้ำโดยไม่ได้รับอนุญาตนโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย(Secure development policy) มีการแยกระบบเทคโนโลยีสารสนเทศ สำหรับการพัฒนาและใช้งานจริงออกจากกันเพื่อลดความเสี่ยงในการเข้าใช้งานหรือการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ โดยมิได้รับอนุญาต

10.2 ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ (Security in Development and Support Processes)เพื่อให้มั่นใจว่ากระบวนการพัฒนาระบบสารสนเทศมีความมั่นคงปลอดภัย ตลอดวงจรการพัฒนา (development lifecycle)

10.2.1 นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)

(1) มีการแยกระบบเทคโนโลยีสารสนเทศสำหรับการพัฒนาและใช้งานจริงออกจากกันเพื่อควบคุมความเสี่ยงในการเข้าถึงระบบหรือการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

10.2.2 กระบวนการในการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ (System Change Control Procedures)

(1) ผู้ดูแลระบบต้องแจ้งให้ผู้ที่เกี่ยวข้องทราบเกี่ยวกับการปรับปรุงหรือเปลี่ยนแปลงระบบเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการทดสอบ และทบทวนก่อนที่จะดำเนินการปรับปรุงหรือเปลี่ยนแปลงระบบ

(2) ผู้ดูแลระบบ ต้องวางแผนดำเนินการปรับปรุงหรือเปลี่ยนแปลงระบบ ก่อนเปลี่ยนไปใช้ระบบใหม่

(3) ผู้ดูแลระบบต้องควบคุมโปรแกรมระบบ (System Software) ที่มีความสำคัญ และประสิทธิภาพการใช้งานโดยทั่วไป หลังจากการแก้ไข หรือบำรุงรักษาระบบ

10.2.3 การตรวจสอบซอฟต์แวร์หลังจากการเปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications After Operating Platform Changes)

(1) เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลง ผู้พัฒนาระบบสารสนเทศต้องตรวจสอบและทดสอบซอฟต์แวร์ต่าง ๆ เพื่อยืนยันว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัย

10.2.4 การควบคุมการเปลี่ยนแปลงของซอฟต์แวร์สำเร็จรูป (Restrictions on Changes to Software Packages)

(1) เมื่อมีการใช้งานซอฟต์แวร์สำเร็จรูป ต้องมีการควบคุมการเปลี่ยนแปลงที่ทำจำเป็น และการเปลี่ยนแปลงทั้งหมดต้องถูกทดสอบและจัดทำเป็นเอกสารเพื่อให้สามารถนำไปใช้งานได้เมื่อมีการปรับปรุงซอฟต์แวร์ในอนาคต

10.2.5 หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles)

(1) เพื่อให้ความมั่นคงปลอดภัยทางด้านวิศวกรรมระบบ ต้องมีการกำหนดขั้นตอนที่เหมาะสมในการพัฒนา ปรับปรุง และดำเนินการระบบอย่างมีประสิทธิภาพและปลอดภัย

10.2.6 สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure development environment)

(1) ต้องมีการจัดทำหรือจัดหาสภาพแวดล้อมในการทำงานที่เหมาะสมและปลอดภัย รวมถึงการจัดทำและปรับปรุงระบบเพื่อให้มีความมั่นคงปลอดภัยในทุกขั้นตอนของการพัฒนาระบบ

10.2.7 การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing)

(1) โปรแกรมหรือระบบที่พัฒนาขึ้นมา ควรมีการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัย โดยต้องมีการทดสอบอยู่ในช่วงระหว่างการพัฒนา

10.2.8 การทดสอบเพื่อรับรองระบบ (System acceptance testing)

(1) มีการจัดทำแผนการทดสอบหรือเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ โดยต้องมีการจัดทำทั้งสำหรับระบบใหม่และระบบที่มีการปรับปรุง

(2) ต้องจัดทำเกณฑ์ในการยอมรับระบบใหม่ ระบบที่จัดซื้อเข้ามาใช้งาน หรือทรัพยากรสารสนเทศอื่น ๆ ก่อนการใช้งาน รวมทั้งต้องจัดทำเอกสาร Checklist หัวข้อที่ใช้ในการทดสอบระบบก่อนที่จะตรวจรับระบบนั้น และกำหนดให้มีการอนุมัติโดยผู้ที่ทำการทดสอบและผู้ส่งมอบ

10.3 ข้อมูลสำหรับการทดสอบ (Test data) เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

10.3.1 การป้องกันข้อมูลสำหรับการทดสอบ (Protection of Test Data)

(1) ข้อมูลสำหรับการทดสอบ (Test data) การป้องกันข้อมูลสำหรับการทดสอบ (Protection of Test Data) ข้อมูลจริงที่จะนำไปใช้ในการทดสอบระบบ จะต้องได้รับอนุญาตจากผู้รับผิดชอบในการรักษาข้อมูลนั้น ๆ ก่อน เมื่อใช้งานเสร็จจะต้องทำการลบข้อมูลจริงออกจากระบบทดสอบทันที และทำการบันทึกไว้เป็นหลักฐานว่าได้นำข้อมูลจริงไปใช้ในการทดสอบอะไรบ้าง รวมถึงวัน เวลา และหน่วยงานที่ทดสอบ แจ้งไปยังผู้รับผิดชอบในการรักษาข้อมูลนั้นอีกครั้ง

หมวดที่ 11 การบริหารจัดการสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security Incident Management)

การใช้งานระบบเทคโนโลยีสารสนเทศอาจเกิดปัญหาหรือเหตุขัดข้องของระบบเทคโนโลยีสารสนเทศขึ้นระหว่างการทำงาน บริษัทจึงจำเป็นต้องมีมาตรการสำหรับจัดการเหตุขัดข้องของระบบเทคโนโลยีสารสนเทศที่เกิดขึ้นเพื่อลดความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้นรวมถึงเป็นแนวทางปฏิบัติให้สอดคล้องกับระบบบริหาร

11.1 การรายงาน กรณีระบบเทคโนโลยีสารสนเทศ ได้รับความเสียหาย

11.1.1 ผู้ใช้งานระบบเทคโนโลยีสารสนเทศ ของบริษัทฯ มีหน้าที่ในการรายงานเหตุละเมิดหรือจุดอ่อน ด้านความมั่นคงใดๆ ที่พบเห็นหรือที่ต้องสงสัยต่อผู้บังคับบัญชาและ/หรือผู้ดูแลระบบฯ โดยทันทีเพื่อให้สามารถแก้ไขปัญหาได้อย่างรวดเร็ว ตัวอย่างของเหตุละเมิดความมั่นคงที่ต้องรายงาน ได้แก่

(1) การตรวจพบไวรัสหรือโปรแกรมไม่ประสงค์ดีต่างๆ

(2) การตรวจพบความพยายามเจาะระบบหรือเครื่องมือเจาะระบบ

(3) การเข้าถึงข้อมูลหรือระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

(4) การใช้งานข้อมูลหรือระบบเทคโนโลยีสารสนเทศอย่างไม่เหมาะสมการเข้าถึงข้อมูลหรือระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

(5) ช่องโหว่หรือจุดอ่อนของซอฟต์แวร์

(6) การละเมิดนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัย

(7) การกระทำที่ผิดกฎหมายหรือข้อบังคับของบริษัทฯ

11.2 การแก้ไขปัญหา และบันทึกเหตุการณ์ กรณีระบบเทคโนโลยีสารสนเทศ ได้รับความเสียหาย

11.2.1 ผู้ใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทฯ ซึ่งพบเห็นเหตุละเมิดหรือจุดอ่อนด้านความมั่นคง ต้องไม่บอกเล่าถึงเหตุที่ตนพบนั้นกับบุคคลอื่นใด ยกเว้นผู้บังคับบัญชาและผู้ดูแลระบบฯ ทั้งนี้ผู้ใช้งานต้องหลีกเลี่ยงการพิสูจน์หรือทดสอบจุดอ่อนด้านความมั่นคงที่ต้องสงสัยด้วยตนเอง

11.2.2 ผู้ดูแลระบบฯ มีหน้าที่รับผิดชอบต่อการรับมือเหตุละเมิดความมั่นคงปลอดภัยต้องดำเนินการตอบสนองต่อเหตุด้วยความรวดเร็ว มีสติรอบคอบ และต้องติดต่อประสานงานกับหน่อยงานต่างๆที่เกี่ยวข้องอย่างเหมาะสม รวมถึง บันทึกข้อมูล และจัดทำเอกสารเกี่ยวกับเหตุละเมิดความมั่นคงปลอดภัยโดยละเอียด

11.2.3 ข้อมูลและหลักฐานที่เกี่ยวข้องกับเหตุละเมิดความมั่นคงที่เกิดขึ้นทั้งหมดต้องได้รับการบันทึกและจัดเก็บอย่างปลอดภัยโดยผู้ดูแลระบบฯ เพื่อนำมาศึกษาและป้องกันไม่ให้เกิดเหตุซ้ำในอนาคต

11.2.4 ฝ่ายเทคโนโลยีสารสนเทศ ร่วมกับฝ่ายทรัพยากรบุคคลและ/หรือฝ่ายธุรกิจที่เกี่ยวข้องจัดทำสื่อเพื่อเสริมสร้างการตระหนักรู้และความเข้าใจเกี่ยวกับเหตุละเมิดความมั่นคง วิธีการรายงานเหตุ วิธีการรวบรวมข้อมูลที่เป็นประโยชน์ต่อการสืบสวนและการเก็บรักษาหลักฐานให้แก่ผู้ดูแลระบบฯ

11.2.5 บริษัทฯต้องจัดฝึกอบรมในหัวข้อที่เกี่ยวข้องกับการตอบสนอง/รับมือต่อเหตุละเมิดความมั่นคง โดยผู้เชี่ยวชาญจากหน่วยงานภายนอก ให้แก่ผู้ดูแลระบบฯที่มีหน้าที่รับผิดชอบในการรับมือเหตุละเมิดความมั่นคง

11.2.6 เครื่องคอมพิวเตอร์ของผู้ใช้งานที่ถูกปลดออก โอนย้าย และลดตำแหน่งจากการการกระทำผิดที่เกี่ยวกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ต้องถูกแยกออกจากเครือข่ายทั้งภายในและภายนอกโดยทันที และก่อนที่จะนำกลับมาใช้ใหม่ ต้องมีการสำรองข้อมูลจากฮาร์ดไดรฟ์เสียก่อน แล้วจึงทำการฟอร์แมตเครื่องคอมพิวเตอร์นั้น เพื่อป้องกันการแพร่กระจายของซอฟต์แวร์มุ่งร้าย เช่น backdoor ไวรัส โทรจัน หรือเพื่อกำจัดซอฟต์แวร์ที่ไม่ได้รับอนุญาต ซึ่งอาจถูกติดตั้งไว้ในระบบเครือข่าย

11.3 การรายงานปัญหาด้านเทคโนโลยีสารสนเทศ

11.3.1 ในกรณีที่เกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีสารสนเทศซึ่งส่งผลกระทบต่อการให้บริการ ระบบงาน หรือชื่อเสียง รวมถึงกรณีที่เทคโนโลยีสารสนเทศที่มีนัยสำคัญถูกโจมตีหรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ จะต้องแจ้งต่อผู้บริหารในตำแหน่งสูงสุด รวมถึงหน่วยงานที่เกี่ยวข้องและหน่วยงานกำกับดูแล เช่น ธนาคารแห่งประเทศไทย เป็นต้น

หมวดที่ 12 การบริหารการจัดการด้านการบริหารหรือดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง (Information Security Business Continuity Management)

12.1 การบริหารจัดการความต่อเนื่องของความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security Continuity)

12.1.1 การจัดทำแผนเตรียมความพร้อมกรณีเหตุฉุกเฉิน

12.1.2 ผู้ดูแลระบบฯ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน (Contingency Plan) เพื่อรับมือสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นได้ทั้งวิธีการทางอิเล็กทรอนิกส์และทางกายภาพโดยแผนเตรียมความพร้อมกรณีฉุกเฉินต้องมีรายละเอียดอย่างน้อยดังนี้

(1) การกำหนดหน้าที่และความรับผิดชอบของบุคคลที่เกี่ยวข้อง

(2) การกำหนดขั้นตอนการปฏิบัติในการกู้คืนระบบเทคโนโลยีสารสนเทศ

(3) การกำหนดขั้นตอนการปฏิบัติในการสำรองข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้

(4) กำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก

(5) ให้ปรับปรุงแผนเตรียมความพร้อมฉุกเฉินอย่างน้อยปีละ 1 ครั้ง โดยมุ่งเน้นที่ระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูง

(6) ให้ทำการทดสอบแผนเตรียมความพร้อมฉุกเฉินอย่างน้อยปีละ 1 ครั้ง หากมีปัญหาเกิดขึ้นในระหว่างการกู้คืน ให้ดำเนินการแก้ไขและบันทึกข้อมูลปัญหาเหล่านั้น พร้อมทั้งวิธีการแก้ไขอย่างเป็นลายลักษณ์อักษร

12.1.3 นโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรครอบคลุมอย่างน้อยดังนี้

- บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการ ผู้บริหารระดับสูงและผู้เกี่ยวข้อง
- การประเมินความเสี่ยง
- การวิเคราะห์ผลกระทบทางธุรกิจและกำหนดเป้าหมายในการกู้คืนระบบเทคโนโลยีสารสนเทศ
- การจัดระดับความสำคัญของระบบงาน
- การกำหนดกลยุทธ์แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
- การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
- การสื่อสารและการฝึกอบรมแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
- การทดสอบ การปรับปรุงและการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

12.2 ระบบปฏิบัติการสำรอง (Redundancies)

12.2.1 กำหนดให้ผู้ดูแลระบบฯประเมินและกำหนดระบบเทคโนโลยีสารสนเทศสำหรับระบบสำคัญรวมไปถึงจัดเตรียมอุปกรณ์ที่สามารถทำงานทดแทนได้อย่างเหมาะสม

12.2.2 กำหนดให้ผู้ดูแลระบบฯ กำหนดสถานที่และเตรียมพื้นที่ให้อยู่ในสภาพพร้อมใช้งานสำหรับระบบทำงานทดแทน

12.2.3 กำหนดให้ผู้ดูแลระบบฯ ทดสอบระบบปฏิบัติงานฯ ทดสอบระบบปฏิบัติงานสำรองอย่างสม่ำเสมอเพื่อมั่นใจได้ว่าจะสามารถทำงานท ดแทนระบบหลักได้เมื่อมีความจำเป็นต้องใช้งาน

หมวดที่ 13 การปฏิบัติตามกฎเกณฑ์ด้านเทคโนโลยีสารสนเทศ (Compliance with IT Regulations)

13.1 การปฏิบัติตามข้อกำหนดทางด้านกฎหมายและสัญญา (Compliance with Legal and Contractual Requirements)เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง พระราชบัญญัติระเบียบข้อบังคับ รวมทั้งสัญญาต่างๆ

13.2 การระบุข้อกำหนดและความต้องการในสัญญาจ้างในการใช้งานระบบเทคโนโลยีสารสนเทศ (Identification of Applicable Legislation and Contractual Requirements)

13.2.1 คณะกรรมการบริหาร ผู้บริหารระดับสูง ผู้บริหารฝ่าย และพนักงานบริษัทฯต้องรับทราบทำความเข้าใจและปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ รวมทั้ง กฎ ระเบียบข้อบังคับ กฎหมายที่เกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศที่กำหนดขึ้นอย่างเคร่งครัด

13.3 ทรัพย์สินทางปัญญา (Intellectual Property Rights)

13.3.1 ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานทรัพย์สินทางปัญญาที่บริษัทฯจัดหามาให้ใช้งาน

13.3.2 ผู้ดูแลระบบฯ ต้องมีการบริหารจัดการและควบคุมดูแลการใช้งานซอฟต์แวร์ให้เป็นไปตามลิขสิทธิ์ที่ได้รับ

13.3.3 ห้ามผู้ใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใดๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนเครื่องคอมพิวเตอร์ แท็ปเล็ต หรือสมาร์ทโฟนของบริษัทฯ โดยเด็ดขาด

13.3.4 กำหนดให้มีการตรวจสอบเครื่องคอมพิวเตอร์อย่างน้อยปีละ 2 ครั้ง เพื่อตรวจดูรายการของซอฟต์แวร์ในเครื่องคอมพิวเตอร์ ถ้าพบว่ามีซอฟต์แวร์ที่ไม่ได้รับอนุญาต ซอฟต์แวร์เหล่านั้นจะถูกลบทิ้ง และถ้าหากมีความจำเป็น จะมีการพิจารณาให้นำซอฟต์แวร์ที่มีใบอนุญาตอย่างถูกต้องอื่นมาใช้แทนซอฟต์แวร์ดังกล่าวได้

13.4 การป้องกันข้อมูล (Protection of Records)ผู้ดูแลระบบฯต้องป้องกันมิให้ข้อมูลที่สำคัญเกิดความเสียหายสูญหาย หรือถูกปลอมแปลง โดยให้สอดคล้องกับกฎหมาย ข้อกำหนดตามสัญญาต่างๆของบริษัทฯ และข้อกำหนดการให้บริการ

13.5 การคุ้มครองข้อมูลส่วนบุคล (Privacy and Protection of Personally Identifiable Information)

13.5.1 ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศขององค์กร ถือเป็นทรัพย์สินขององค์กร (ยกเว้น ข้อมูลที่เป็นทรัพย์สินของลูกค้า หรือบุคคลภายนอกรวมถึงซอฟต์แวร์ หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตร หรือลิขสิทธ์ของบุคคลภายนอก) สามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

13.6 การกำกับดูแลการปฏิบัติงานให้เป็นไปตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ

13.6.1 ให้ผู้บริหารระดับสูงและผู้บริหารฝ่ายเป็นผู้กำกับ ดูแล ให้ผู้ใต้บังคับบัญชาปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของบริษัทฯอย่างเคร่งครัด

13.6.2 ในกรณีที่มีการฝ่าฝืนหรือละเลยการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ ให้ผู้บังคับบัญชาดำเนินการเพื่อยับยั้งเหตุการณ์ฝ่าฝืนหรือ ละเลยการปฏิบัติดังกล่าวตามสมควร และรายงานตามสายบังคับบัญชาไปยังผู้บริหารระดับสูงและ/หรือคณะกรรมการบริหาร เพื่อพิจารณาดำเนินการ่อไป

13.6.3 หากบุคคลใดจงใจฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ ฉบับนี้จะถือว่าเป็นความผิดทางวินัยและให้ดำเนินการตามข้อบังคับเกี่ยวกับพนักงาน ทั้งนี้หากการกระทำนั้นเป็นเหตุให้บริษัทฯ ได้รับความเสียหาย บริษัทฯจะพิจารณาดำเนินคดีตามกฎหมายอีกทางหนึ่งด้วย

6. การยกเว้นนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ในกรณีที่พนักงานหรือสำนักงานในบริษัทฯไม่สามารถปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้และจำเป็นต้องยกเว้นการบังคับใช้ในบางข้อ ให้จัดทำเอกสารข้อยกเว้น และนำเสนอ ต่อผู้บริหารระดับสูงที่ดูแลฝ่ายเทคโนโลยีสารสนเทศ เพื่อพิจารณากลั่นกรองก่อน เพื่อนำเสนอต่อคณะกรรมการบริหารเพื่อขออนุมัติ นอกจากนี้ผู้บริหารระดับสูงที่ดูแลฝ่ายเทคโนโลยีสารสนเทศ และฝ่ายเทคโนโลยีสารสนเทศ ต้องตรวจทานและประเมินข้อยกเว้นนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง และนำเสนอต่อคณะกรรมการบริหารเพื่อทราบ

7. การสื่อสารนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ให้ฝ่ายเทคโนโลยีสารสนเทศ และฝ่ายงานธุรกิจที่เกี่ยวข้องสื่อสารและเผยแพร่นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง ให้แก่ คณะกรรมการ ผู้บริหาร พนักงานของบริษัทฯ และผู้ให้บริการภายนอกที่เกี่ยวข้องให้มีความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและสร้างความตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและแนวทางการบริหารจัดการการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและสามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพ

8. การทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ให้ฝ่ายเทคโนโลยีสารสนเทศ ทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญเพื่อมั่นใจได้ว่าเนื้อหาของนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ยังคงไว้ซึ่งความสมบูรณ์ มีประสิทธิภาพและสามารถนำไปใช้งานได้อย่างเหมาะสม โดยให้นำเสนอ ผู้บริหารระดับสูงที่ดูแลฝ่ายเทคโนโลยีสารสนเทศ กลั่นกรองก่อนนำเสนอคณะกรรมการบริหารเพื่ออนุมัติ ทั้งนี้ฝ่ายเทคโนโลยีสารสนเทศ และฝ่ายงานที่เกี่ยวข้องต้องปรับปรุงเอกสารแนวปฏิบัติ ขั้นตอนการปฏิบัติงาน และเอกสารสนับสนุนต่างๆที่เกี่ยวข้องให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีการเปลี่ยนแปลง

9. **บทลงโทษ**

การละเมิด ฝ่าฝืน ละเลย หรือไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตลอดจนแนวปฏิบัติและขั้นตอนการปฏิบัติงานที่เกี่ยวข้องถือเป็นความผิดทางวินัย ซึ่งต้องถูกพิจารณาลงโทษทางวินัยตามข้อบังคับของบริษัทฯ และหากละเมิด ฝ่าฝืน ละเลยการปฏิบัตินั้นเข้าข่ายการกระทำที่ผิดกฎหมาย ผู้ละเมิดก็ต้องได้รับการดำเนินคดีตามที่กฎหมายระบุไว้

10. **เอกสารอ้างอิง**

ระบบบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ISO/IEC 27001:2013

ทั้งนี้ ให้มีผลบังคับใช้ ตั้งแต่ วันที่ 21 กุมภาพันธ์ 2568 เป็นต้น

(นายไกรทิพย์ ไกรฤกษ์)
ประธานคณะกรรมการบริษัท
บริษัท เมเจอร์ ซีนีเพล็กซ์ กรุ๊ป จำกัด (มหาชน)

Appendix 1

รายการซอฟต์แวร์มาตรฐานที่อนุญาตให้ติดตั้ง และใช้งานภายในบริษัทฯ: สำหรับผู้ใช้ทั่วไป

หมวด	ชื่อซอฟต์แวร์	ราคา/ License	หมายเหตุ
ระบบปฏิบัติการ (Operation Software: OS)			
	Microsoft Windows 7 Professional		64 bit
	Microsoft Windows 8 Professional		64 bit
	Microsoft Windows 10 Professional		64 bit
	OS X		เฉพาะเครื่อง Apple, Macintosh
ชุดโปรแกรมสำนักงาน (Office Suite)			
	Microsoft Office O365 Business		ใช้ได้แต่ Word, Excel, Power Point, One Drive บนเครื่อง Desktop
	Microsoft Office O365 Business Premium		ใช้ได้แต่ Word, Excel, Power Point, One Drive บนเครื่อง Desktop
	Microsoft Office O365 Business Pro		ใช้ได้แต่ Word, Excel, Power Point, One Drive บนเครื่อง Desktop
	Microsoft Office 2013		Word, Excel, Power Point, Outlook, Access, OneNote, Publisher
	Microsoft Visio		เฉพาะผู้ที่ได้รับการอนุมัติเท่านั้น
	Microsoft Visio O365		เฉพาะผู้ที่ได้รับการอนุมัติเท่านั้น
	Microsoft Project		เฉพาะผู้ที่ได้รับการอนุมัติเท่านั้น
	Microsoft Visual Studio		เฉพาะผู้ที่ได้รับการอนุมัติเท่านั้น
	Microsoft Office for Mac		เฉพาะเครื่อง Apple, Macintosh
ชุดโปรแกรมเฉพาะทาง (Specific Software)			
	Adobe Creative Cloud		เฉพาะผู้ที่ได้รับการอนุมัติเท่านั้น
	Adobe Photoshop CS5		เฉพาะผู้ที่ได้รับการอนุมัติเท่านั้น
	Adobe Illustrator CS5		เฉพาะผู้ที่ได้รับการอนุมัติเท่านั้น
	Adobe Premiere Pro		เฉพาะผู้ที่ได้รับการอนุมัติเท่านั้น
	Adobe After Effects		เฉพาะผู้ที่ได้รับการอนุมัติเท่านั้น
	AutoCAD		เฉพาะผู้ที่ได้รับการอนุมัติเท่านั้น
	Adobe Acrobat Pro		เฉพาะผู้ที่ได้รับการอนุมัติเท่านั้น
	SketchUp Pro 2020		เฉพาะผู้ที่ได้รับการอนุมัติเท่านั้น

หมวด	ชื่อซอฟต์แวร์	ราคา/ License	หมายเหตุ
	Camtasia		เฉพาะผู้ที่ได้รับการอนุมัติเท่านั้น
	SolidWorks		เฉพาะผู้ที่ได้รับการอนุมัติเท่านั้น
โปรแกรมอรรถประโยชน์ (Utilization Software)			
	ESET Nod32 antivirus		โปรแกรมป้องกัน Virus
	Bit Defender		
	Izarc		ใช้แทน Winzip, WinRar
	Adobe Acrobat Reader		ใช้สำหรับเปิดไฟล์ PDF
	Microsoft Picture Manager		ใช้แทน ACDsee Pro4
	PDFCreator		ใช้แทน Adobe Acrobat Pro
	CDBurnerXP		ใช้แทน Nero Burner
	GIMP		ใช้แทน Photoshop
	Foxit reader		ใช้สำหรับ Print PDF
	Window Media Player		ใช้แทน Power DVD
	Note++		ใช้แทน Edit Plus
	DownThemAll		ใช้แทน Internet Download Manager
โปรแกรมเครือข่ายสังคมออนไลน์ (Social Network Program)			
	Facebook		อนุญาตให้ใช้ตามเวลาที่กำหนด
	Line		อนุญาตให้ใช้ตามเวลาที่กำหนด
	MS Team		
	Instagram		อนุญาตให้ใช้ตามเวลาที่กำหนด
อื่นๆ			
	Internet Explorer		
	Fire Fox		
	Google Chrome		
	Flash Player		ใช้ร่วมกับ Browser
	JAVA		ใช้ร่วมกับ Browser