นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์
(Cybersecurity Policy)
บริษัท จัสมิน เทคโนโลยี โซลูชั่น จำกัด (มหาชน)

รหัสเอกสาร	:	PC-IT-001
ผู้รับผิดชอบ/จัดทำ	:	Software Development Team
ผู้ตรวจทาน	:	คณะกรรมการตรวจสอบและธรรมาภิบาล
ผู้อนุมัติเอกสาร	:	คณะกรรมการบริษัท
วันที่มีผลบังคับใช้	:	01 มิถุนายน 2565
วันที่ทบทวนครั้งล่าสุด	:	24 มีนาคม 2569

บริษัท จัสมิน เทคโนโลยี โซลูชั่น จำกัด (มหาชน) 200 ชั้น 9 หมู่ 4 ถนนแจ้งวัฒนะ ตำบลปากเกร็ด อำเภอปากเกร็ด จังหวัดนนทบุรี 11120
JTSmine Technology Solution Public Company Limited 200, 9th Floor, Moo 4, Chaengwatana Road, Pakkred Sub-district, Pakkred District, Nonthaburi 11120 Tel : +66 (0) 2 100 8300 Fax : +66 (0) 962 2523, URL : http://www.jts.co.th, Registration No. 0107547000109

รายละเอียดการจัดทำเอกสาร

การรับรองเอกสาร

บทบาท	ผู้รับผิดชอบ	ลายมือชื่อ
ผู้รับผิดชอบ/จัดทำ	Software Development Team	
ผู้ตรวจทาน	มติที่ประชุมคณะกรรมการตรวจสอบและธรรมาภิบาล	
ผู้อนุมัติเอกสาร	มติที่ประชุมคณะกรรมการบริษัท	

ประวัติการแก้ไขปรับปรุง

เวอร์ชัน	คำอธิบายและเหตุผลในการแก้ไข	ผู้ขอแก้ไข	วันที่ประกาศใช้
1.0	**เอกสารเผยแพร่ฉบับแรก**	สมเจตน์ แซ่จัง	01 มิถุนายน 2565
2.0	แก้ไขใหม่ทั้งฉบับ เพื่อให้สอดคล้อง และเป็นตามแนวทางของ มาตรฐาน ISO/IEC 27001:2022 รวมทั้งข้อบังคับเกี่ยวกับการใช้งานแพลตฟอร์มปัญญาประดิษฐ์ (หน้า 10) ความมั่นคงปลอดภัยสารสนเทศในการบริหารโครงการ (หน้า 12) ความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคราวด์ (หน้า 20)	Software Development Team	20 ธันวาคม 2567
3.0	เพิ่มเอกสารอ้างอิง แก้ไขแนวทางเรื่อง AI Security สอดรับกับ "แนวทางการประยุกต์ใช้ปัญญาประดิษฐ์อย่างมีธรรมาภิบาลสำหรับผู้บริหารองค์กร" (AI Governance Guideline) จัดทำโดย ETDA และ "แนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย (AI Security Guidelines)" ของ สกมช. (NCSA) (หน้า 11 , 22) แก้ไข เพื่อให้สอดคล้อง และเป็นตามแนวทางของ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568 (การปฏิบัติงานจากระยะไกลและการควบคุมการเข้าถึง หน้า 28) (ข้อตกลงกับผู้ให้บริการภายนอก หน้า 41)	Software Development Team	24 มีนาคม 2569

<u>เอกสารอ้างอิง</u>

1. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
2. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565
3. นโยบายคุ้มครองข้อมูลส่วนบุคคล JTS Group (PC-DPO-001)
4. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560

5. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566
6. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567
7. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568
8. แนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย (AI Security Guidelines) โดย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)
9. คู่มือแนวทางการประยุกต์ใช้ Generative AI อย่างมีธรรมาภิบาลสำหรับองค์กร (Generative AI Governance Guideline for Organizations)

สารบัญ

นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Policy)

1. บทนำ

1.1 วัตถุประสงค์

นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์จัดทำขึ้นโดยมีวัตถุประสงค์หลัก 5 ประการ ดังนี้

1) เพื่อปกป้องข้อมูลสารสนเทศ ไม่ให้สูญหาย เสียหาย ถูกทำลาย ถูกแก้ไข หรือเปิดเผยโดยไม่ได้รับอนุญาต ข้อมูลสารสนเทศอันหมายถึงข้อมูลทั้งหมดที่มีความสำคัญต่อองค์กร ไม่ว่าจะเป็นข้อมูลทางธุรกิจ ข้อมูลส่วนบุคคล ข้อมูลทางการเงิน ข้อมูลทางเทคนิค ฯลฯ
2) เพื่อสร้างความมั่นใจในการให้บริการแก่ผู้ใช้บริการ ว่าข้อมูลสารสนเทศที่ได้มอบให้กับองค์กรจะได้รับการปกป้องและรักษาให้มีความปลอดภัยอย่างเหมาะสม
3) เพื่อปฏิบัติตามข้อกำหนดทางกฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง เช่น พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)
4) เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศมีประสิทธิภาพ เหมาะสม เพียงพอและบรรลุตามวัตถุประสงค์ที่ตั้งเป้าหมายไว้ของบริษัท จัสมิน เทคโนโลยี โซลูชั่น จำกัด (มหาชน), บริษัท จัสเทล เน็ทเวิร์ค จำกัด (JasTel), บริษัท คลาวด์ คอมพิวติ้ง โซลูชั่นส์ จำกัด (CCS) และบริษัทในเครือ
5) ส่งเสริมธรรมาภิบาล AI กำหนดแนวทางการใช้งานปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย (AI Security Governance) ตามแนวทางของ สกมช.

วัตถุประสงค์ทั้ง 5 ประการดังที่ได้กล่าวในข้างต้นมีความสำคัญต่อองค์กรเป็นอย่างมาก เนื่องจากข้อมูลสารสนเทศถือเป็นสินทรัพย์ที่สำคัญขององค์กร หากข้อมูลสารสนเทศสูญหาย เสียหาย หรือถูกโจรกรรม อาจส่งผลกระทบต่อการดำเนินธุรกิจขององค์กรได้ เช่น ก่อให้เกิดความเสียหายต่อชื่อเสียง สูญเสียรายได้ สูญเสียลูกค้า หรือถูกลงโทษตามกฎหมาย นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ จึงถือเป็นแนวทางปฏิบัติที่สำคัญที่องค์กรควรกำหนดขึ้นเพื่อปกป้องข้อมูลสารสนเทศและสร้างความมั่นใจในการให้บริการแก่ผู้ใช้บริการ นอกจากวัตถุประสงค์หลักทั้ง 5 ประการแล้ว นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์อาจกำหนดวัตถุประสงค์เพิ่มเติมอื่น ๆ ขึ้นตามความเหมาะสมขององค์กร เช่น

- เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์
- เพื่อปรับปรุงประสิทธิภาพของระบบสารสนเทศ
- เพื่อพัฒนาความรู้และความสามารถของบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศ

องค์กรต้องพิจารณาวัตถุประสงค์ของนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างรอบคอบ เพื่อให้นโยบายดังกล่าวบรรลุตามวัตถุประสงค์ที่ตั้งเป้าหมายไว้ได้อย่างมีประสิทธิภาพ

1.2 ขอบเขตของเอกสาร

นโยบายฉบับนี้ใช้กับบริษัท จัสมิน เทคโนโลยี โซลูชั่น จำกัด (มหาชน), บริษัท จัสเทล เน็ทเวิร์ค จำกัด (JasTel), บริษัท คลาวด์ คอมพิวติ้ง โซลูชั่นส์ จำกัด (CCS) และบริษัทในเครือ ทั้งนี้ ให้ครอบคลุมถึงบุคคลภายนอกที่ได้รับอนุญาตให้ใช้ระบบเครือข่าย คอมพิวเตอร์แม่ข่าย ระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์ทั้งแบบตั้งโต๊ะและแบบพกพา หรืออุปกรณ์สื่อสารโทรคมนาคมเพื่อเข้าถึงระบบสารสนเทศของกลุ่มบริษัทฯ โดยให้ยกเลิกประกาศฉบับเดิม เรื่อง นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

1.3 ระยะเวลาทบทวน

บริษัทฯ กำหนดให้มีการปรับปรุงและทบทวนนโยบายในการรักษาความมั่นคงปลอดภัยของข้อมูล (Review of the policies for information security) อย่างสม่ำเสมอ เพื่อให้การรักษาความมั่นคงปลอดภัยสารสนเทศคงความถูกต้อง สมบูรณ์ และมีความพร้อมใช้งาน โดยสอดคล้องเหมาะสมกับการเปลี่ยนแปลงและความต้องการทางธุรกิจของบริษัทฯ ให้เป็นปัจจุบัน อย่างน้อยปีละ 1 ครั้ง

2. กลยุทธ์การป้องกันความปลอดภัยของข้อมูล (Information Security Protection Strategy)

2.1 การรักษาความมั่นคงปลอดภัยของข้อมูล (Security Principle)

การรักษาความมั่นคงปลอดภัยของข้อมูล มีหลักการเพื่อให้บรรลุผลตามวัตถุประสงค์ดังต่อไปนี้

- **ความลับ (Confidentiality)** คือ การปกป้องความลับของข้อมูล โดยป้องกันการเข้าถึงและการเปิดเผยข้อมูลจาก ผู้ที่ไม่ได้รับอนุญาต รวมไปถึงข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นกรรมสิทธิ์ของกลุ่มบริษัทฯ
- **ความถูกต้องสมบูรณ์ (Integrity)** คือ การทำให้มั่นใจว่าข้อมูลสารสนเทศมีความถูกต้อง ครบถ้วนสมบูรณ์ตามที่ผู้ใช้ข้อมูลต้องการ ต้องไม่มีการแก้ไข ดัดแปลง หรือโดนทำลายโดยผู้ที่ไม่ได้รับอนุญาต
- **ความพร้อมใช้งาน (Availability)** คือ การทำให้มั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลและบริการได้อย่างรวดเร็วและเชื่อถือได้
- **ความรับผิดชอบ (Accountability)** คือ การระบุหน้าที่ความรับผิดชอบของแต่ละบุคคล รวมถึงการรับผิดและรับชอบในผลของการกระทำตามบทบาทหน้าที่นั้นๆ
- **การพิสูจน์ตัวตน (Authentication)** คือ การทำให้มั่นใจว่าสิทธิการเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศต้องผ่านกระบวนการยืนยันตัวตนที่สมบูรณ์แล้วเท่านั้น
- **การกำหนดสิทธิ (Authorization)** คือ การทำให้มั่นใจว่าการให้สิทธิเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศเป็นไปตามความจำเป็น (Least Privilege) และสอดคล้องกับความต้องการพื้นฐาน (Need to Know Basis) ตามที่ได้รับอนุญาต

2.2 การบริหารจัดการความเสี่ยงด้านปลอดภัยสารสนเทศ (Information Security Risk Management)

การบริหารความเสี่ยงเป็นความรับผิดชอบร่วมกันของผู้บริหารและพนักงานทุกระดับ และต้องมีการปฏิบัติอย่างต่อเนื่อง โดยกระบวนการบริหารความเสี่ยงประกอบด้วยขั้นตอนหลัก ดังนี้

- การระบุความเสี่ยงที่อาจเกิดขึ้นและมีผลกระทบต่อการรักษาความปลอดภัยข้อมูล (Risk Identification)
- การวิเคราะห์ความเสี่ยง (Risk Analysis)
- การประเมินความเสี่ยง (Risk Assessment)
- การจัดการความเสี่ยง (Risk Mitigation or Risk Treatment)
- การสื่อสารให้ความรู้และการให้คำปรึกษาแนะนำ (Risk Communication and Consultation) เกี่ยวกับการบริหารความเสี่ยงองค์กร
- การติดตามความเสี่ยงและการรายงาน (Risk Monitoring and Report)

2.3 การบริหารจัดการความมั่นคงปลอดภัยระบบปัญญาประดิษฐ์ (AI Security Governance)

เพื่อให้การประมวลผลข้อมูลบนแพลตฟอร์ม AI ดำเนินการอย่างถูกต้องและปลอดภัย ต้องปฏิบัติดังต่อไปนี้

- **การพัฒนา AI** ในการพัฒนา AI ต้องเป็นไปตามหลักการ Secure by Design และ Defense-in-Depth
    - **ห้าม** พัฒนาหรือใช้งานระบบที่มีลักษณะครอบงำจิตใจเพื่อจำกัดการตัดสินใจ หรือระบบ Social Scoring โดยเด็ดขาด
    - ทีมพัฒนาที่เกี่ยวข้อง ต้องมีการวิเคราะห์และประเมินผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ใน 3 ด้านหลัก (CIA Triad) จากภัยคุกคาม AI ได้แก่ ความลับ (C), ความถูกต้อง (I) และความพร้อมใช้ (A) ประเมินผลกระทบต่อ CIA
    - วงจรชีวิตการทำ AI (AI Life Cycle) ทีมพัฒนาต้องดูแลความปลอดภัย โดยแบ่งออกเป็นระยะต่าง ๆ ดังนี้
        - **การออกแบบ (Concept & Secure Design)** กำหนดความต้องการและประเมินความเสี่ยงเบื้องต้น
        - **การพัฒนา (Secure Development)** คัดกรองและป้องกันข้อมูลที่นำมาใช้ฝึกสอน (Train) โมเดล AI ไม่ให้มีใครแอบนำข้อมูลที่เป็นพิษมาใส่ (Data Poisoning) หรือซ่อนคำสั่งอันตรายไว้
        - **การทบทวนและทดสอบ (Secure Verification)** ก่อนนำไปใช้จริง ต้องทดสอบจำลองการโจมตี เพื่อดูว่า AI จะหลงกลหรือทำงานผิดพลาดหรือไม่
        - **การนำไปใช้งาน (Secure Deployment)** การตั้งค่าสภาพแวดล้อมของระบบให้ปลอดภัย แข็งแกร่ง และปกป้องข้อมูลระหว่างการใช้งานจริง
        - **การดำเนินงานและบำรุงรักษา (Secure Operation & Maintenance)** การเฝ้าระวัง (Monitor) พฤติกรรมที่ผิดปกติของ AI อย่างต่อเนื่อง และคอยอัปเดตอุดช่องโหว่
        - **การกำจัดและทำลาย (Disposal)** เมื่อเลิกใช้งาน AI แล้ว ต้องมีกระบวนการลบทำลายข้อมูล และไฟล์โมเดลอย่างปลอดภัย เพื่อไม่ให้มีข้อมูลสำคัญรั่วไหลหลงเหลืออยู่

- **การควบคุมข้อมูล** ห้ามนำข้อมูลลับขององค์กร ข้อมูลลูกค้า ข้อมูลพนักงาน หรือข้อมูลส่วนบุคคลไปประมวลผลในแพลตฟอร์ม AI สาธารณะ (เช่น ChatGPT, Gemini) ที่อยู่นอกเหนือการควบคุมขององค์กรโดยไม่ได้รับอนุมัติเด็ดขาด
- **การปกปิดข้อมูล** ก่อนนำข้อมูลไปวิเคราะห์ในระบบ AI ควรใช้วิธีการทำข้อมูลให้เป็นนิรนาม (Anonymization) หรือการทำข้อมูลให้เป็นข้อมูลที่ไม่สามารถระบุตัวตนได้ (Data Masking/Pseudonymization) เพื่อลดความเสี่ยงข้อมูลรั่วไหล
- **ความโปร่งใสและจริยธรรม** การจัดการข้อมูลส่วนบุคคลต้องเป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) และนโยบายคุ้มครองข้อมูลส่วนบุคคลของบริษัท ซึ่งกำหนดให้มีการขอความยินยอมจากเจ้าของข้อมูลก่อนที่จะนำข้อมูลไปใช้ในระบบ AI หรือการวิเคราะห์ข้อมูลอื่น ๆ และต้องระบุชัดเจนว่าข้อมูลส่วนบุคคลจะไม่ถูกนำไปใช้เกินกว่าขอบเขตของวัตถุประสงค์ที่ได้รับความยินยอม
- **การระวังภัยคุกคามใหม่** สร้างความตระหนักรู้แก่พนักงานเกี่ยวกับภัยคุกคามจาก AI เช่น การหลอกลวงด้วย Deepfake, การป้อนคำสั่งมุ่งร้าย (Prompt Injection) หรือข้อมูลที่ถูกวางยา (Data Poisoning)

3. การบังคับใช้นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์

3.1 การบังคับใช้นโยบาย

การประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมีการประกาศและสื่อสารไปยังผู้ที่เกี่ยวข้องทราบเพื่อปฏิบัติได้อย่างเหมาะสม โดยผู้บังคับบัญชาตามสายงานตั้งแต่ระดับฝ่ายขึ้นไป มีหน้าที่รับผิดชอบในการจัดทำมาตรการควบคุมที่เหมาะสมเพื่อให้สอดคล้องกับนโยบายด้านความปลอดภัยสารสนเทศ ภายใต้ขอบเขตความรับผิดชอบของตน และให้มีการตรวจสอบมาตรการควบคุมด้านความปลอดภัยสารสนเทศโดยผู้ตรวจสอบอิสระหรือผู้ตรวจติดตามคุณภาพภายใน

3.2 การจัดการมาตรการที่ได้รับการยกเว้น (Handling of Policy Deviation)

หากมีความจำเป็นที่ต้องใช้บางมาตรการควบคุมที่ไม่เป็นไปตามนโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศ ผู้บังคับบัญชาตามสายงานที่เกี่ยวข้องกับมาตรการควบคุมที่ได้รับการยกเว้นนั้น ต้องทบทวนและพิจารณาความเสี่ยงในการใช้มาตรการควบคุมดังกล่าวเป็นประจำทุกปี

4. บทลงโทษทางวินัย

การละเมิด ฝ่าฝืน หรือไม่ปฏิบัติตามนโยบาย รวมวิธีปฏิบัติงาน และเอกสารที่เกี่ยวข้อง ไม่ว่าโดยเจตนาหรือไม่เจตนา ถือเป็นความผิดซึ่งต้องถูกลงโทษทางวินัยตามความเหมาะสม หากการละเมิด ฝ่าฝืน หรือไม่ปฏิบัติตามเข้าข่ายการกระทำความผิดต่อ พ.ร.บ. ไซเบอร์ฯ หรือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ (PDPA) ผู้ละเมิดต้องได้รับการดำเนินคดีทางกฎหมายตามที่กฎหมายระบุ บทลงโทษทางวินัยนั้นจะอิงตามบทลงโทษของพนักงานที่ฝ่าย HR กำหนดไว้

5. มาตรการควบคุมด้านองค์กร (Organization controls)

5.1 นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ (Policies for information security)

นโยบายความมั่นคงปลอดภัยสารสนเทศและนโยบายอื่นที่เกี่ยวข้อง จะถูกกำหนด และอนุมัติโดยผู้บริหารระดับสูง พร้อมเผยแพร่ สื่อสาร แก่บุคลากรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องให้รับทราบ และกำหนดให้มีการทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงกฎหมายสำคัญเกิดขึ้น

5.2 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities)

ผู้บริหารระดับสูงสุดของแต่ละบริษัทฯ มีการกำหนดหน้าที่ความรับผิดชอบที่ชัดเจนพร้อมทั้งสื่อสารภายในองค์กร และคณะทำงานที่เกี่ยวข้องกับระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ และอาจกำหนดหน่วยงานหรือบุคคลต่าง ๆ ที่มีส่วนเกี่ยวข้องในการดำเนินงานภายใต้ขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ร่วมกันผลักดันเป้าหมายให้บรรลุผล

5.3 การแบ่งแยกงานและหน้าที่ความรับผิดชอบ (Segregations of duties)

เป็นการแบ่งแยกหน้าที่ในระบบหรือกระบวนการต่าง ๆ หรือพื้นที่ทับซ้อนภายในองค์กร เพื่อไม่ให้มีบุคคลใดบุคคลหนึ่งหรือหน่วยงานใดหน่วยงานหนึ่ง สามารถทำกิจกรรมทั้งหมดในกระบวนการทางธุรกิจ เพื่อลดความเสี่ยงในการดำเนินธุรกิจ ทั้งลดความเสี่ยงที่เกี่ยวข้องกับความผิดพลาด, การทุจริต, หรือการก่อปัญหาทางธุรกิจอื่น ๆ ที่อาจเกิดขึ้นจากความผิดพลาดหรือการประพฤติปฏิบัติที่ไม่เหมาะสมของบุคคลใด ๆ

5.4 หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities)

ผู้บริหารทุกระดับของบริษัท มีหน้าที่กำกับดูแล และเสริมสร้างค่านิยม ให้กับพนักงานและหน่วยงานภายนอกให้มีการปฏิบัติตามแนวปฏิบัติและกระบวนการความมั่นคงปลอดภัยด้านสารสนเทศ ในด้านต่าง ๆ ดังนี้

(1) มีการสื่อสารให้กับพนักงานและหน่วยงานภายนอกให้รับทราบถึงหน้าที่และความรับผิดชอบความมั่นคงปลอดภัยของตนเอง และบทลงโทษหากพบการกระทำผิด

(2) มีการสื่อสารหรืออบรมให้กับพนักงานและหน่วยงานภายนอกที่เกี่ยวข้อง มีความตระหนักรู้ และปฏิบัติงานโดยคำนึงถึงการรักษาความมั่งคงปลอดภัยของข้อมูล

(3) ให้ทิศทางกำกับดูแลและการสนับสนุนให้เกิดความมั่นคงปลอดภัยสารสนเทศภายในบริษัทฯ

5.5 การติดต่อหน่วยงานผู้มีอำนาจ (Contact with authorities)

จัดทำรายชื่อหน่วยงานผู้มีอำนาจ และทำการสื่อสารอย่างมีประสิทธิภาพกับหน่วยงานที่มีอำนาจในการบังคับใช้กฎหมาย หน่วยงานที่กำกับดูแลบริษัทฯ และผู้ให้บริการทางด้านโทรคมนาคม/คณะทำงานเมื่อเกิดเหตุฉุกเฉินด้านระบบสารสนเทศ รวมถึงหน่วยงานราชการที่ต้องทำการติดต่อเมื่อเกิดเหตุการณ์ต่าง ๆ โดยจะต้องมีการทบทวนและปรับปรุงข้อมูลที่จะสื่อสารให้ทันสมัยอยู่เสมอ

5.6 การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษ (Contact with special interest groups)

ได้รับข้อมูลต่าง ๆ ด้านความมั่นคงปลอดภัยสารสนเทศ จากผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย หรือได้รับข้อมูลเทคโนโลยีใหม่ ๆ, ข้อมูลเกี่ยวกับวิธีปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ, ข้อมูลด้านการเตือนล่วงหน้า, คำปรึกษา และการติดตั้งแพตช์ (Patch) เกี่ยวกับการโจมตีและช่องโหว่ต่าง ๆ, คำแนะนำด้านความมั่นคงปลอดภัยจากผู้ขายผลิตภัณฑ์ และการแลกเปลี่ยนข้อมูลกับองค์กรอื่น ๆ เพื่อลดความเสี่ยงจากการถูกคุกคามจากช่องโหว่ด้านความปลอดภัยสารสนเทศและเพื่อให้ผู้ได้รับผลกระทบพิจารณาและดำเนินการทันทีภายใต้กรอบเวลาที่กำหนดไว้

5.7 ข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม (Threat intelligence)

ต้องมีวิธีการจัดการเกี่ยวกับข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ

(1) กำหนดแหล่งที่มาของข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคามที่จำเป็นต่อบริษัทฯ

(2) กำหนดวิธีการวิเคราะห์ข้อมูลภัยคุกคาม และเกณฑ์การประเมินหรือใช้ software จากแหล่งที่เชื่อถือได้ทำการประเมิน

(3) กำหนดมาตรการควบคุมเพื่อป้องกันข้อมูลภัยคุกคาม

(4) กำหนดวิธีการจัดเก็บข้อมูลภัยคุกคาม

5.8 ความมั่นคงปลอดภัยสารสนเทศในการบริหารโครงการ (Information security in project management)

โครงการใด ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ จะต้องมีการระบุขอบเขตและวัตถุประสงค์ของโครงการ และการเข้าถึงซึ่งระบบสารสนเทศทั้งหมด เพื่อจะได้นำมาประเมินด้านความมั่นคงปลอดภัยสารสนเทศทั้งหมด โดยให้มีข้อตกลงการรักษาความลับของข้อมูลและข้อกำหนดในการปฏิบัติงานครอบคลุมถึงความมั่นคงปลอดภัยสารสนเทศกับผู้ที่เกี่ยวข้องในการปฏิบัติงานโครงการนั้น ๆ

5.9 บัญชีทะเบียนข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ (Inventory of information and other associated assets)

(1) รายการทรัพย์สิน (Inventory of Assets)

ทรัพย์สินทั้งหมดที่เกี่ยวข้องกับการดำเนินงานจะต้องได้รับการบันทึกในรายการทรัพย์สิน โดยครอบคลุมถึงทรัพย์สินประเภทต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศของบริษัท และต้องทำการทบทวนบัญชีรายการทรัพย์สินเป็นประจำ อย่างน้อยปีละ 1 ครั้ง

(2) ความเป็นเจ้าของทรัพย์สิน (Ownership of Assets)

ทรัพย์สินทั้งหมดจะต้องมีผู้ดูแลและมีการกำหนดชื่อผู้ที่ครอบครองอาจจะเป็นบุคคลหรือหน่วยงานก็ได้ ในกรณีที่กำหนดให้ทรัพย์สินใด ๆ เป็นของหน่วยงานในบริษัท ทรัพย์สินนั้นจะอยู่ในความรับผิดชอบหัวหน้าหน่วยงานนั้น ๆ

5.10 การใช้งานข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ (Acceptable use of information and other associated assets)

หน่วยงานใดที่เป็นผู้รับผิดชอบทรัพย์สินและข้อมูลสารสนเทศ จะต้องจัดทำเอกสารหลักเกณฑ์ ข้อกำหนดการใช้งานอย่างเหมาะสม และ/หรือขั้นตอนปฏิบัติสำหรับการจัดการทรัพย์สินและข้อมูลสารสนเทศนั้นได้อย่างถูกต้องเหมาะสม หากทรัพย์สินและข้อมูลสารสนเทศนั้นจะถูกนำไปใช้ที่หน่วยงานอื่น

5.11 การคืนทรัพย์สิน (Return of assets)

พนักงานและลูกจ้างของหน่วยงานทั้งหมด ต้องคืนทรัพย์สินของบริษัททั้งหมดที่ตนถือครอง เมื่อมีการเปลี่ยนแปลงสภาพการจ้าง หรือโอนย้าย หรือสิ้นสุดการจ้างงาน หรือหมดสัญญา หรือสิ้นสุดข้อตกลงการจ้างต่อหัวหน้างานหรือผู้รับผิดชอบโครงการ

(1) ผู้ดูแลระบบสารสนเทศ ต้องถอดถอนสิทธิการเข้าถึงข้อมูล พื้นที่ ระบบเทคโนโลยีสารสนเทศทันทีที่มีการสิ้นสุดหรือเปลี่ยนแปลงการจ้าง

(2) สำหรับสื่อบันทึกข้อมูล และคอมพิวเตอร์ ผู้รับผิดชอบต้องล้าง, ลบ, ทำลายข้อมูล ด้วยวิธีการที่เหมาะสมก่อนนำไปจัดเก็บเป็นเครื่องสำรอง หากพบว่าอุปกรณ์หรือสื่อบันทึกใด ๆ เสี่ยงหรือเป็นอันตรายต่อระบบสารสนเทศ ให้เสนอขออนุมัติทุบทำลาย

5.12 การจัดหมวดหมู่ของสารสนเทศ (Classification of information)

ต้องทำการจัดประเภทข้อมูลสารสนเทศ ลำดับความสำคัญหรือระดับชั้นความลับของข้อมูล รวมถึงระดับชั้นการเข้าถึง เวลาที่อนุญาตให้เข้าถึง และเจ้าของข้อมูลเป็นผู้กำหนดระดับชั้นความลับของข้อมูล ข้อมูลทั้งหมดที่อยู่ภายในขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศจะต้องได้รับการจัดระดับชั้นความลับ โดยมีแนวปฏิบัติดังนี้

(1) การแบ่งประเภท การจัดระดับชั้นและช่องทางการเข้าถึงข้อมูลเป็นไปตามเอกสารแนวปฏิบัติการจัดระดับชั้นความลับ การติดป้าย และการจัดการข้อมูล (Information Classification, Labelling and Handling Guideline)

(2) การใช้งานหรือการเข้าถึงข้อมูลให้อยู่ภายในเวลาทำการ หรือให้สอดคล้องกับประเภทข้อมูลและการปฏิบัติงานของผู้ดูแลข้อมูล

(3) เจ้าของข้อมูลจะต้องเป็นผู้กำหนดระดับชั้นความลับของข้อมูลที่ตนเป็นเจ้าของ และกำหนดให้มีการทบทวนระดับชั้นความลับอย่างสม่ำเสมอ

5.13 การจำแนกข้อมูลสารสนเทศ (Labelling of information)

ข้อมูลสารสนเทศกำหนดให้มีการจำแนกประเภทข้อมูลโดยการติดป้าย เพื่อการจัดการข้อมูลที่อยู่ในขั้นตอนการจัดเก็บ การขนส่ง การประมวลผล และการทำลายทิ้ง ให้สอดคล้องตามประเภทข้อมูล โดยมีแนวปฏิบัติดังนี้

(1) การติดป้ายและการจัดการข้อมูลเป็นไปตามแนวปฏิบัติการจัดระดับชั้นความลับ การติดป้าย และการจัดการข้อมูล (Information Classification, Labelling and Handling Guideline)

(2) เจ้าของข้อมูลจะต้องกำหนดมาตรการในการจัดการข้อมูลให้สอดคล้องตามระดับชั้นความลับ และมีการทบทวนประสิทธิภาพของมาตรการอย่างสม่ำเสมอ

(3) ข้อมูลที่ไม่สามารถติดป้ายได้ เช่น ไฟล์อิเล็กทรอนิกส์ในเครื่องคอมพิวเตอร์ จะต้องมีวิธีปฏิบัติให้สอดคล้องกับระดับชั้นความลับสูงสุดที่มีในเครื่อง โดยไม่จำเป็นต้องติดป้าย

5.14 การโอนถ่ายข้อมูล (Information transfer)

5.14.1 แนวปฏิบัติและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนข้อมูลสารสนเทศ (Information Transfer Policies and Procedures)

เพื่อให้การแลกเปลี่ยนข้อมูลสารสนเทศทั้งภายในและภายนอกบริษัท มีความมั่นคงปลอดภัยเป็นไปตามระดับชั้นความลับของข้อมูล จึงได้จัดทำข้อกำหนดในการแลกเปลี่ยนข้อมูลสารสนเทศ ดังนี้

1) การแลกเปลี่ยนข้อมูลสารสนเทศภายในบริษัท

การแลกเปลี่ยนข้อมูลสารสนเทศภายในบริษัทจะต้องปฏิบัติตามเอกสารแนวปฏิบัติการจัดระดับชั้นความลับ การติดป้าย และการจัดการข้อมูล (Information Classification, Labelling and Handling Guideline)

2) การแลกเปลี่ยนข้อมูลสารสนเทศระหว่างองค์กร

ต้องจัดหา กำหนดมาตรการ และการใช้งานระบบสารสนเทศทางธุรกิจที่มีความเชื่อมโยงกัน โดยให้บริษัทที่อยู่ในเครือทั้งหมดมีแนวปฏิบัติ ดังนี้

A. วิเคราะห์ความเสี่ยงและกำหนดมาตรการจัดการความเสี่ยงที่เกิดจากการใช้งานระบบสารสนเทศที่เชื่อมโยงกันระหว่างหน่วยงาน โดยการประเมินความเสี่ยงของการเข้าถึงข้อมูลจากหน่วยงานภายนอก โดยพิจารณาประเด็นต่าง ๆ ดังต่อไปนี้

i. รูปแบบของการเข้าถึงข้อมูลสารสนเทศ
ii. ประเภทของข้อมูลสารสนเทศที่ต้องการใช้ในการแลกเปลี่ยน
iii. มาตรฐานทางเทคนิคในการบันทึกและอ่านข้อมูลสารเทศ ตลอดจนซอฟต์แวร์ที่เกี่ยวข้อง
iv. ข้อมูลหรือซอฟต์แวร์ที่ต้องการจะส่ง หรือมาตรการ/ กระบวนการในการแลกเปลี่ยนสื่อบันทึกข้อมูล
v. มาตรการอื่น ๆ ที่จำเป็นในการป้องกันข้อมูลที่สำคัญ เช่น การใช้กุญแจในการเข้ารหัสข้อมูล เป็นต้น
vi. ทบทวนมาตรการ (Controls) ตามที่ได้กำหนดไว้สำหรับการเข้าออกสถานที่ตลอดจนการเข้าถึงระบบ หากมีความจำเป็นอาจเพิ่มมาตรการเพื่อลดความเสี่ยงที่มีแนวโน้มว่าจะเกิดขึ้น ทั้งนี้มาตรการทั้งหมดต้องได้รับการวางแผนและนำมาใช้อย่างเป็นทางการต่อไป

B. กำหนดให้มีการเผยแพร่ข้อมูลที่เกี่ยวข้องผ่านทางระบบเทคโนโลยีสารสนเทศ เช่น อีเมล ปฏิทินส่วนกลาง (Public Calendar) อินทราเน็ต ฯลฯ ตามความจำเป็น

C. ให้ปฏิบัติตามระเบียบ แนวปฏิบัติ และข้อกำหนดของบริษัทฯ ในการใช้งานระบบเทคโนโลยีสารสนเทศ

D. แบ่งแยกระบบที่มีข้อมูลสำคัญออกจากโซนการใช้งานทั่วไป หรือจำกัดสิทธิการเข้าถึงเฉพาะพนักงานที่มีความจำเป็นเท่านั้น

E. ต้องมีสัญญาหรือข้อตกลงเพื่อระบุความรับผิดชอบของฝ่ายที่รับข้อมูล รวมทั้งระบุมาตรฐานในการบรรจุเอกสารหรือข้อมูล และการส่งอย่างชัดเจน

F. ห้ามนำข้อมูลลับขององค์กร เช่น ข้อมูลทางการเงิน ข้อมูลลูกค้า ข้อมูลพนักงาน ไปใช้งานกับระบบ AI ใด ๆ โปรดแจ้งหัวหน้างานทันทีหากพบเห็นพนักงานฝ่าฝืน ผู้ฝ่าฝืนอาจถูกพิจารณาโทษทางวินัย

3) การเผยแพร่ข้อมูลสู่สาธารณะ

จัดให้เว็บไซต์ที่ใช้เผยแพร่ข้อมูลสู่สาธารณะ มีแนวปฏิบัติในการบริหารจัดการ ดังนี้

A. มีการดูแลข้อมูลทะเบียนโดเมนเทียบเท่ากับทรัพย์สินมีค่าอื่น ๆ

B. เนื้อหาแต่ละส่วนที่อยู่ในเว็บไซต์จะต้องได้รับการอนุมัติโดยผู้บริหารที่เกี่ยวข้องก่อนที่จะมีการเผยแพร่ออกสู่สาธารณะ

C. จัดเก็บบันทึกการทบทวนเนื้อหาและข้อมูลอนุมัติการเผยแพร่ข้อมูลออกสู่สาธารณะอย่างเป็นทางการ

D. มีการเฝ้าระวังเนื้อหาในเว็บไซต์เพื่อให้มั่นใจได้ว่า ข้อมูลที่เผยแพร่เป็นข้อมูลที่เกี่ยวข้อง เป็นประโยชน์ และถูกต้อง

E. มีการเฝ้าระวังและตรวจสอบความถูกต้องของข้อมูลไม่ให้มีการเปลี่ยนแปลง แก้ไข โดยไม่ได้รับอนุญาต

5.14.2 ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreement on Information Transfer)

การถ่ายโอนสารสนเทศระหว่างบริษัทกับหน่วยงานภายนอกทั้งหมด จะต้องมีการร่วมลงนามในสัญญาว่าด้วยข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศในการแลกเปลี่ยนข้อมูลสารสนเทศ รวมถึงการจัดส่งข้อมูล และ/หรือ ซอฟต์แวร์ และการจัดการแลกเปลี่ยนสื่อบันทึกข้อมูล

5.14.3 การใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Electronic Messaging)

(1) ผู้บริหาร พนักงานทุกคนต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) ของบริษัท เพื่อวัตถุประสงค์ในการทำงานตามภารกิจหน้าที่ความรับผิดชอบของตนเอง และใช้ในการติดต่อกับหน่วยงานทั้งภายในและภายนอก

(2) ห้ามส่งข้อมูลลับไปยังหน่วยงานอื่น ทั้งภายในและภายนอกหากไม่ได้รับอนุญาตอย่างเป็นทางการ และข้อมูลต้องได้รับการป้องกันตามแนวทางการจัดการตามระดับชั้นสูงสุดของข้อมูลนั้น

(3) อีเมลทั้งหมดควรมีการบันทึกถึงข้อตกลงการรักษาความลับ และระบุข้อความการปฏิเสธความรับผิดชอบหากมีการนำอีเมลไปใช้งานโดยไม่ได้รับอนุญาต

(4) ไม่อนุญาตให้ทำการปลอมแปลงต้นทางของการสื่อสารอิเล็กทรอนิกส์ การเปลี่ยนแปลงข้อมูลของระบบที่ใช้ในการระบุที่มาของข้อความ หรือปิดบังต้นทางของการสื่อสาร

(5) ห้ามมิให้เข้าถึงระบบเพื่อพยายามในการเฝ้าติดตาม อ่าน คัดลอก ลบ หรือเจาะเข้าไปในการสื่อสารทางอิเล็กทรอนิกส์ของบุคคลอื่นโดยไม่ได้รับความยินยอมจากบุคคลนั้น (ยกเว้นบุคลากรระบบเครือข่ายที่ได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร)

(6) ไม่ควรใช้ระบบอีเมลเก็บข้อมูลสะสมไว้เป็นเวลานาน

(7) ห้ามส่งต่อ E-Mail ที่เกี่ยวกับการล่วงละเมิดหรือข่มขู่ หรือมีเนื้อหาข้อความที่ขัดต่อกฎหมายและศีลธรรมอันเป็นเหตุให้เสียชื่อเสียงของบริษัทได้ และใช้ E-Mail เป็นเครื่องมือในการกระจายข่าวสาร เว้นแต่เป็นการประกาศที่เหมาะสม

5.14.4 การใช้งานระบบอินเทอร์เน็ตและเครือข่ายออนไลน์อย่างปลอดภัย

(1) ผู้ใช้งานจะต้องใช้อินเทอร์เน็ต และการส่งข้อความแชต เพื่อวัตถุประสงค์ในการปฏิบัติงานเท่านั้น

(2) เฉพาะเจ้าหน้าที่ที่ได้รับอนุญาตเท่านั้นที่สามารถเป็นตัวแทนบริษัท เพื่อการสื่อสารบนเครือข่ายออนไลน์ได้

(3) ผู้ใช้งานจะต้องปฏิบัติตามกฎหมายลิขสิทธิ์และอ้างอิงแหล่งที่มาอย่างเหมาะสม เมื่อโพสต์เนื้อหาในโซเชียลมีเดีย

(4) ผู้ใช้งานจะต้องไม่เผยแพร่ โพสต์หรือปล่อยข้อมูลใด ๆ ที่ถือว่าเป็นความลับของบริษัทฯหรือของผู้อื่น หรือที่ไม่ต้องการเปิดเผยต่อสาธารณะ

(5) ห้ามใช้โลโก้และเครื่องหมายการค้าของบริษัท โดยไม่ได้รับความยินยอมเป็นลายลักษณ์อักษร

(6) การโพสต์ข้อความใด ๆ ที่เกี่ยวข้องกับบริษัทจะต้องได้รับอนุญาตอย่างเป็นทางการก่อน

(7) ห้ามเผยแพร่ข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากเจ้าของข้อมูลอย่างถูกต้อง

(8) ผู้ใช้งานที่เยี่ยมชมเว็บไซต์ลามกอนาจาร อาจจะถูกลงโทษทางวินัยและอาจถูกเลิกจ้าง

(9) ผู้ใช้งานควรใช้งานระบบ Internet, Intranet และ E-Mail ด้วยความรอบคอบและมีวิจารณญาณ โดยให้ระลึกเสมอว่าพนักงานคือตัวแทนของบริษัทในการทำธุรกิจ

5.15 การควบคุมการเข้าถึง (Access control)

มีการใช้แนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

5.15.1 การเข้าถึงระบบสารสนเทศทั้งในส่วนของพนักงานและบุคคลภายนอก ต้องสอดคล้องตามมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศและคำนึงถึงการรักษาความปลอดภัยของข้อมูลอยู่เสมอ

5.15.2 ระดับการเข้าถึงสอดคล้องกับระดับชั้นความลับของข้อมูลที่สามารถเข้าถึงได้

5.15.3 การอนุญาตให้เข้าถึง ให้ใช้เกณฑ์พิจารณาดังต่อไปนี้

(1) การเข้าถึงสถานที่ทางกายภาพ ขึ้นอยู่กับความจำเป็นในการเข้าถึง (Need-to-access)

(2) สิทธิการเข้าถึงระบบสารสนเทศและระบบเครือข่าย ขึ้นอยู่กับความจำเป็นที่ต้องใช้งาน (Need-to-use)

(3) สิทธิการเข้าถึงข้อมูลสารสนเทศที่อยู่ในระบบสารสนเทศและอุปกรณ์เครือข่าย ควรจำกัดไว้เฉพาะข้อมูลที่จำเป็นต้องทราบ (Need-to-know)

5.15.4 การกำหนดหลักเกณฑ์ในการอนุญาตการเข้าถึง

(1) การกำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้องต้องกำหนดสิทธิที่สามารถใช้งานในขอบเขตขั้นต่ำดังนี้

a. อ่านอย่างเดียว

b. สร้างข้อมูล

c. แก้ไข

d. ประมวลผล

e. ไม่มีสิทธิ

(2) การกำหนดเกณฑ์การระงับสิทธิ มอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งานที่กำหนดไว้

(3) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูงหรือผู้ดูแลระบบที่ได้รับมอบหมาย

5.15.5 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับของข้อมูลที่สามารถเข้าถึงได้

(1) ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับของข้อมูล

(2) เจ้าของข้อมูล จะต้องมีการตรวจสอบความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

(3) วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบ ต้องกำหนดรายชื่อผู้ใช้งานและรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละระดับชั้นความลับของข้อมูล

5.16 การบริหารจัดการด้านเอกลักษณ์ (Identity management)

มีขั้นตอนการลงทะเบียนผู้ใช้งาน การโยกย้าย และการสิ้นสุดความจำเป็นต้องใช้งาน โดยมีแนวปฏิบัติดังนี้

5.16.1 การลงทะเบียนผู้ใช้งาน

(1) ปฏิบัติตามเอกสารกระบวนการลงทะเบียนและการเพิกถอนสิทธิผู้ใช้งาน (User Registration/ De-registration Procedure)

(2) บัญชีของผู้ใช้แต่ละคนจะต้องไม่ซ้ำกันและสามารถอ้างอิงกลับไปยังผู้ที่เป็นเจ้าของได้ ในกรณีที่ไม่สามารถหลีกเลี่ยงการใช้บัญชีผู้ใช้ซ้ำ ให้ระบุชื่อผู้ที่ใช้งานร่วมกันและมีการทบทวนรายชื่อผู้ใช้อย่างสม่ำเสมอ

(3) การให้สิทธิสอดคล้องกับแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศของบริษัท

(4) ไม่กำหนดชื่อบัญชีผู้ใช้ที่สื่อถึงหน้าที่ความรับผิดชอบในการปฏิบัติงาน

5.16.2 การบริหารจัดการรหัสผ่านของผู้ใช้งาน

(1) แจ้งรหัสผ่านให้กับผู้ใช้งานโดยตรงโดยไม่มีบุคคลที่สามรับทราบ

(2) กำชับให้ผู้ใช้เปลี่ยนแปลงรหัสผ่านทันที หรือเปลี่ยนครั้งแรกที่มีการใช้งาน

(3) กำหนดให้ผู้ดูแลระบบสอบถามข้อมูลเพื่อยืนยันตัวบุคคลผู้ใช้ทุกครั้งที่ได้รับการร้องขอให้เปลี่ยน/รีเซตรหัสผ่าน ตัวอย่างคำถามของข้อมูลเพื่อยืนยันตัวบุคคล ได้แก่ หมายเลขโทรศัพท์ภายใน รหัสประจำตัวพนักงาน ฯลฯ

(4) รหัสผ่านจะถูกเปลี่ยนอย่างเหมาะสมหรือเมื่อใดก็ตามที่มีข้อบ่งชี้ว่าอาจมีการรั่วไหลของข้อมูล หรือใช้ระบบ MFA (Multi Factor Authentication)

(5) รหัสผ่านที่ใช้ร่วมกัน (Share Password) จะต้องได้รับการดูแลอย่างเหมาะสม

(6) รหัสผ่านจะต้องไม่ถูกเก็บไว้ในระบบประมวลผลข้อมูลหรือสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ใด ๆ โดยไม่มีการเข้ารหัสข้อมูลไว้

(7) รหัสผ่านจะไม่ถูกบันทึกไว้ เว้นแต่จะสามารถจัดเก็บได้อย่างปลอดภัย

(8) ผู้ใช้งานจะต้องรับผิดชอบต่อบัญชีผู้ใช้งานและรหัสผ่านของตน และจะไม่เปิดเผยต่อผู้ใด ไม่ว่าด้วยเหตุผลใดก็ตาม

(9) ผู้ใช้งานจะต้องเปลี่ยนรหัสผ่านทันทีที่เข้าใช้งานครั้งแรก และการกำหนดรหัสผ่านต้องเป็นรหัสผ่านที่มั่นคงปลอดภัย มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีประสิทธิภาพได้

(10) รหัสผ่านต้องมีความยาวอย่างน้อยแปด (8) ตัวอักษรและประกอบด้วยคุณสมบัติอย่างน้อยสาม (3) ลักษณะดังต่อไปนี้:

a. อักขระตัวเลขอย่างน้อยหนึ่งตัว (0 - 9)
b. อักขระตัวพิมพ์เล็กอย่างน้อยหนึ่งตัว (a - z)
c. อักขระตัวพิมพ์ใหญ่อย่างน้อยหนึ่งตัว (A - Z)
d. อักขระพิเศษอย่างน้อยหนึ่งตัว (~! @ # $% ^ & * - +?) สำหรับระบบที่รองรับอักขระพิเศษ

(11) ผู้ใช้งานจะต้องพิจารณาสิ่งต่อไปนี้ เมื่อสร้างรหัสผ่านเพื่อเพิ่มความคาดเดายากของรหัสผ่าน:

a. ห้ามใช้คำในภาษาสแลง ภาษาถิ่น ฯลฯ
b. ห้ามใช้ข้อมูลส่วนบุคคล เช่น ชื่อ (ชื่อของญาติ ชื่อของสัตว์เลี้ยง ฯลฯ) หรือวันที่เช่นวันเกิดวันหยุดและวันครบรอบ (เช่น“09Aug2009”)
c. ห้ามใช้คำวลีหรือตัวย่อที่เกี่ยวข้องกับองค์กร (เช่น“JTSiTgroup”)
d. ห้ามใช้ข้อกำหนดคำสั่งเว็บไซต์ชื่อคอมพิวเตอร์หรือแอปพลิเคชันซอฟต์แวร์ (เช่น “winipcfg”, “ yahoodotcom”)
e. ห้ามใช้คำหรือรูปแบบตัวเลข (เช่น“12345678”,“ abcdefgh”)
f. ไม่ควรเพิ่มรหัสผ่านด้วยการเติม/ต่อท้ายอักขระด้วยลำดับเลขที่ (เช่น “oldpassword1”, “ 1oldpassword”)

5.17 ข้อมูลในการพิสูจน์ตัวตน (Authentication information)

ผู้ดูแลระบบ จัดสรรและจัดการข้อมูลในการพิสูจน์ตัวตน โดยมีแนวปฏิบัติดังนี้

(1) ระบุประเภทของข้อมูลที่ต้องพิสูจน์ตัวตนที่อนุญาตให้ใช้เพื่อเข้าถึงระบบและข้อมูลสารสนเทศ

(2) กำหนดวิธีการจัดเก็บข้อมูลในการพิสูจน์ตัวตน

(3) ข้อมูลในการพิสูจน์ตัวตนทั้งหมดจะต้องได้รับการเข้ารหัสและจัดเก็บอย่างปลอดภัย

5.18 สิทธิ์การเข้าถึง (Access rights)

ผู้บริหารระดับสูงหรือผู้รับมอบอำนาจ พิจารณาและกำหนดสิทธิ์การเข้าถึงข้อมูลและทรัพย์สินที่เกี่ยวข้อง โดยมีแนวปฏิบัติดังนี้

(1) กำหนดตารางระดับของสิทธิ์การเข้าถึงสำหรับผู้ใช้

(2) กำหนดวิธีการมอบหมายสิทธิ์การเข้าถึงให้กับผู้ใช้

(3) กำหนดวิธีการถอนสิทธิ์การเข้าถึงจากผู้ใช้

(4) ทบทวนสิทธิอย่างน้อยปีละ 1 ครั้ง ทั้งนี้อาจกำหนดความถี่ให้มากขึ้นสำหรับระบบที่มีความสำคัญสูง

5.19 ความมั่นคงปลอดภัยสารสนเทศในความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)

ต้องคำนึงถึงและนำมาตรการด้านความมั่นคงปลอดภัยมากำกับหรือควบคุมในการให้บริการของผู้ให้บริการภายนอก ดังนี้

(1) ในระยะการวางแผน บริษัทควรระบุความต้องการจัดจ้างคนภายนอก, ความเสี่ยงที่จะเกิดขึ้นในการจ้างคนภายนอก และปัจจัยที่สามารถเป็นไปได้ในการลดการจัดจ้างคนภายนอก รายละเอียดเหล่านี้จะต้องทำเป็นลายลักษณ์อักษรในส่วนของการบริหารจัดการโครงการ

(2) ข้อผูกพัน บริษัทควรจะเลือกและประเมินหาผู้ให้บริการเพื่อที่จะรักษาความมั่นคงปลอดภัยสารสนเทศให้เป็นไปตามทัศนะของบริษัท โดยที่มีการระบุการจัดการด้านความมั่นคงปลอดภัยอย่างละเอียดในสัญญา รวมถึงการลงนามข้อตกลงการไม่เปิดเผยข้อมูลด้วย (Non-Disclosure Agreement) และปฏิบัติตามแนวปฏิบัติฉบับนี้

(3) การนำไปปฏิบัติ บริษัทต้องพัฒนาการรักษาความมั่นคงปลอดภัยสารสนเทศ และตารางสมรรถนะโดยอ้างอิงตามสัญญาและเงื่อนไขที่กำหนดไว้ ตารางนั้นจะต้องมีการเฝ้าระวังและทบทวนเป็นประจำ

(4) การแก้ไข/เปลี่ยนแปลง บริษัทอาจพิจารณาให้มีการเพิ่มเติมข้อกำหนดหรือวิธีการปกป้องใด ๆ ในเอกสารสัญญาการบริการ เพื่อรักษาด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งนี้ขึ้นอยู่กับลักษณะงานที่ทำการว่าจ้างและผลการประเมินความเสี่ยง

(5) ผู้ให้บริการ (Third-Party) ที่มีการจ้างช่วงงานต่อ ให้ผู้ให้บริการช่วง (Subcontractor) ต้องแจ้งให้ผู้ว่าจ้างรับทราบทุกครั้งและต้องดำเนินการให้ ผู้ให้บริการช่วง ลงนามในข้อตกลงการไม่เปิดเผยข้อมูลด้วย (Non-Disclosure Agreement) และปฏิบัติตามแนวปฏิบัติฉบับนี้อย่างเคร่งครัด โดยผู้ให้บริการมีหน้าที่กำกับดูแลและรับผิดชอบต่อผลงานและการกระทำทั้งหลายของผู้ให้บริการช่วง (Subcontractor)

(6) เมื่อสิ้นสุดการให้บริการ บริษัทต้องเตรียมให้ผู้ให้บริการส่งหน้าที่ความรับผิดชอบกลับมายังบริษัทหรือผู้ให้บริการรายใหม่ บริษัทต้องมั่นใจได้ว่าข้อมูลของบริษัททั้งหมดต้องได้กลับคืนจากผู้ให้บริการรายเดิม รายละเอียดเหล่านี้จะต้องทำเป็นลายลักษณ์อักษรในส่วนของการบริหารจัดการโครงการ

(7) เมื่อผู้ให้บริการหรือหน่วยงานภายนอกส่งมอบงานเสร็จสิ้น ข้อมูลการพัฒนาระบบ โปรแกรม และคู่มือต่าง ๆ ถือเป็นลิขสิทธิ์หรือทรัพย์สินของบริษัท ห้ามเปิดเผยหรือนำไปใช้โดยไม่ได้อนุญาต

5.20 การระบุความมั่นคงปลอดภัยสารสนเทศในข้อตกลงของผู้ให้บริการภายนอก (Addressing information security within supplier agreements)

ข้อตกลงกับหน่วยงานภายนอกจะต้องระบุถึงการให้ความสำคัญกับความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องดังต่อไปนี้

(1) การจัดหมวดหมู่ข้อมูลและการจัดการกับข้อมูลสารสนเทศ

(2) ระดับเป้าหมายของการให้บริการที่ยอมรับได้

(3) ความรับผิดของทั้งสองฝ่าย

(4) การป้องกันสิทธิในทรัพย์สินทางปัญญา (Intellectual Property Rights - IPR) และลิขสิทธิ์ของงานที่ทำร่วมกัน

(5) การควบคุมการเข้าใช้งานทั้งแบบเข้าถึงตัวเครื่องและแบบผ่านทางระบบเครือข่าย

(6) สิทธิในการตรวจสอบความรับผิดชอบตามสัญญาหรือการตรวจสอบที่ดำเนินการโดยบุคคลที่สาม

(7) การเกี่ยวข้องของหน่วยงานภายนอกโดยกับผู้รับจ้างช่วงอื่น

(8) ข้อกำหนดในการเก็บรักษาไว้ซึ่งรายชื่อของผู้ที่ได้รับอนุญาตใช้บริการ และสิทธิอื่น ๆ

(9) สิทธิในการเฝ้าระวังและยกเลิกกิจกรรมของผู้ใช้งาน

(10) ข้อกำหนดในการทำสำเนา และเปิดเผยข้อมูลบริษัท

(11) การเรียกคืน หรือการทำลายข้อมูลต่าง ๆ เมื่อสัญญาเสร็จสิ้น

(12) ข้อกำหนดในการป้องกันซอฟต์แวร์ประสงค์ร้าย

5.21 การจัดการด้านความมั่นคงปลอดภัยสารสนเทศในห่วงโซ่อุปทานเทคโนโลยีสารสนเทศและการสื่อสาร (Managing information security in the information and communication technology (ICT) supply chain)

ต้องมีการกำหนดกระบวนการและขั้นตอนเพื่อเตรียมความพร้อมด้านเทคโนโลยีสารสนเทศและการสื่อสารต่อเนื่องทางธุรกิจ

(1) ระบุและประเมินความเสี่ยงที่อาจส่งผลต่อความพร้อมใช้งานของระบบ ICT

(2) จัดทำแผนสำรองข้อมูล (Backup and Recovery Plan)

(3) จัดทำแผนรับมือภัยพิบัติ (Disaster Recovery Plan)

(4) จัดทำแผนการจัดการเหตุการณ์ฉุกเฉิน (Incident Response Plan)

(5) ทดสอบแผนความพร้อมใช้งานอย่างสม่ำเสมอ และจัดฝึกอบรมให้ผู้ใช้เกี่ยวกับแนวทางปฏิบัติ

(6) ตรวจสอบประสิทธิภาพของระบบ ICT และการปฏิบัติตามนโยบาย

(7) ทบทวนและปรับปรุงอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับความต้องการทางธุรกิจและเทคโนโลยีที่เปลี่ยนแปลง

5.22 การติดตาม การทบทวน และการเปลี่ยนแปลงการจัดการบริการของผู้ให้บริการภายนอก (Monitoring, review and change management of supplier services)

5.22.1 การติดตามและทบทวนบริการของผู้ให้บริการภายนอก

(1) การส่งมอบบริการโดยบุคคลที่สามจากภายนอกควรจะมีการตกลงทำสัญญารักษาความปลอดภัย คำนิยามของบริการ และระดับของการส่งมอบบริการรวมอยู่ในสัญญาส่งมอบบริการจากหน่วยงานภายนอก

(2) ควรจัดให้มีการตรวจสอบติดตามและประเมินผลการบริการจากหน่วยงานภายนอกเป็นประจำ เพื่อให้มั่นใจว่าได้มีการปฏิบัติตามข้อตกลงในการรักษาความมั่นคงปลอดภัยของข้อมูล และเพื่อให้ได้มีการจัดการกับปัญหาทางด้านความปลอดภัยอย่างเหมาะสม

(3) สร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยด้านไซเบอร์เท่าที่จำเป็นต่อผู้ปฏิบัติงานที่เกี่ยวข้อง

(4) สื่อสารกระบวนการและขั้นตอนในการจัดการเหตุการณ์ละเมิดความปลอดภัยหรือเหตุการณ์ฉุกเฉินด้านความมั่นคงปลอดภัยของข้อมูลสานสนเทศและความปลอดภัยด้านไซเบอร์

(5) ติดตาม/เฝ้าระวังผู้ให้บริการภายนอกให้ปฏิบัติตามแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยทางไซเบอร์

5.22.2 การบริหารการเปลี่ยนแปลงในบริการจากผู้ให้บริการภายนอก

(1) บริษัทจะปรับปรุงเงื่อนไขในสัญญาการให้บริการเมื่อมีการเปลี่ยนแปลงข้อกำหนดในการให้บริการ ซึ่งรวมถึงการดูแลและปรับปรุงแนวปฏิบัติ ขั้นตอนปฏิบัติ และการควบคุมด้านความมั่นคงปลอดภัยของข้อมูลที่มีอยู่เดิม

(2) ระหว่างทำการเปลี่ยนแปลงการให้บริการ ต้องมีการบริหารความเสี่ยงที่อาจเกิดขึ้นจากการเปลี่ยนแปลงการให้บริการ

5.23 ความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์ (Information security for use of cloud service)

ต้องกำหนดกระบวนการที่ชัดเจนสำหรับการจัดหา การใช้ การจัดการ และการยกเลิกการใช้บริการคลาวด์ เพื่อให้แน่ใจว่าความมั่นคงปลอดภัยสารสนเทศได้รับการรักษาไว้ตลอดวงจรการใช้งาน

5.23.1 การจัดหา คัดเลือกผู้ให้บริการคลาวด์

a. เลือกใช้ผู้ให้บริการระบบคลาวด์ที่มีความน่าเชื่อถือและเป็นผู้ที่ได้รับรองมาตรฐาน ISO 27001, SOC 2 หรือมาตรฐานที่เทียบเท่า

b. ระบุประเภทของข้อมูลที่จะจัดเก็บในระบบคลาวด์

c. กำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการระบบคลาวด์

d. กำหนดกระบวนการสำหรับการเจรจาสัญญาและข้อตกลงระดับบริการ (SLA)

5.23.2 การใช้บริการคลาวด์

a. กำหนดสิทธิ์การเข้าถึงข้อมูลบนระบบคลาวด์ โดยพิจารณาจากบทบาทและหน้าที่ของผู้ใช้งาน

b. ใช้การยืนยันตัวตนแบบหลายชั้น (MFA) เพื่อเพิ่มความปลอดภัยในการเข้าถึงข้อมูล

c. ตรวจสอบและบันทึกกิจกรรมการเข้าถึงข้อมูลบนระบบคลาวด์อย่างสม่ำเสมอ

d. มีการสำรองข้อมูลบนระบบคลาวด์อย่างสม่ำเสมอ

e. จัดฝึกอบรมให้แก่ผู้ใช้งานเกี่ยวกับนโยบายความมั่นคงปลอดภัยทางไซเบอร์สำหรับการใช้บริการคลาวด์

5.23.3 การจัดการบริการคลาวด์

a. ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับการใช้บริการระบบคลาวด์

b. กำหนดกระบวนการสำหรับการรายงานและแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัย

5.23.4 การยกเลิกบริการคลาวด์

a. กำหนดกระบวนการสำหรับการยกเลิกการใช้งานบริการระบบคลาวด์

b. กำหนดวิธีการลบข้อมูลออกจากการใช้บริการระบบคลาวด์

c. กำหนดวิธีการเก็บหลักฐานการลบข้อมูล

5.24 การวางแผนและการเตรียมการ การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information security incident management planning and preparation)

5.24.1 ต้องมีการกำหนดขั้นตอนการจัดการเหตุการณ์และจุดอ่อนด้านความปลอดภัยข้อมูล เพื่อจัดการเหตุการณ์ในหลาย ๆ ลักษณะที่เกิดขึ้น เช่น

a. ระบบข้อมูลขัดข้อง และใช้บริการไม่ได้
b. โปรแกรมประสงค์ร้ายต่อระบบ
c. การถูกโจมตีที่ทำให้เครื่องเป้าหมายไม่สามารถให้บริการได้
d. ความผิดพลาดอันเป็นผลจากข้อมูลทางธุรกิจที่ไม่สมบูรณ์หรือไม่ถูกต้อง
e. การล่วงละเมิดความลับและความครบถ้วนสมบูรณ์ของข้อมูล
f. การใช้ระบบข้อมูลโดยมิชอบ

5.24.2 ผู้รับผิดชอบมีหน้าที่สื่อสารกระบวนการบริหารจัดการเหตุการณ์ด้านความปลอดภัยสารสนเทศและบทบาทหน้าที่ให้ผู้เกี่ยวข้องทราบ

5.24.3 ผู้ใช้งานจะต้องรายงานเหตุการณ์และ/หรือจุดอ่อนด้านความมั่นคงปลอดภัยไปยังเจ้าหน้าที่ที่เกี่ยวข้องในการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยทันที ตามแนวปฏิบัติในการรายงานเหตุละเมิดด้านความมั่นคงปลอดภัย

5.25 การประเมินและการตัดสินใจต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Assessment and decision on information security events)

ต้องมีการกำหนดแนวทางสำหรับการประเมินและตัดสินใจต่อเหตุการณ์ด้านความมั่นคง ควรดำเนินการดังนี้

(1) รวบรวมและวิเคราะห์ข้อมูลเพื่อตรวจหาเหตุการณ์ละเมิดความปลอดภัย
(2) จัดแบ่งประเภทและลำดับเหตุการณ์เพื่อพิจารณาว่าเหตุการณ์นั้นควรส่งต่อทีมอื่นในการดำเนินการหรือไม่
(3) วิเคราะห์ข้อมูลที่เกี่ยวข้องกับเหตุการณ์ กำหนดกลยุทธ์การตอบสนองและแก้ไข
(4) ตัดสินใจเกี่ยวกับวิธีการตอบสนองต่อเหตุการณ์ด้านความมั่นคงสารสนเทศ ประสานงานหรือสื่อสารข้อมูลที่เหมาะสมไปยังบุคคลที่เกี่ยวข้อง

5.26 การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)

(1) การตอบสนองต่อเหตุละเมิดด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยทางไซเบอร์ ตามขั้นตอนการตอบสนอง และแผนการตอบสนอง
(2) ห้ามผู้ใช้งานตอบคำถามที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยและความผิดพลาดของระบบกับสื่อใด ๆ เองโดยเด็ดขาด การสื่อสารข้อมูลกับหน่วยงานภายนอกทั้งหมดเป็นหน้าที่ของคณะทำงานที่ได้รับมอบหมายในการสื่อสารเท่านั้น

5.27 การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents)

ความรู้ที่ได้รับจากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ต้องมีการนำไปใช้ในการทบทวนเหตุการณ์จุดอ่อนทางด้านความปลอดภัยสารสนเทศและความปลอดภัยทางไซเบอร์ เพื่อทบทวนความเสี่ยงและมาตรการการ

ป้องกันให้เหมาะสม รวมถึงการปรับปรุงการบริหารจัดการเหตุการณ์ต่าง ๆ ให้มีประสิทธิภาพมากขึ้น เพื่อป้องกันการเกิดเหตุการณ์ละเมิดความปลอดภัยในอนาคต

5.28 การเก็บรวบรวมหลักฐาน (Collection of evidence)

ต้องมีการเก็บรักษาหลักฐานสนับสนุนอื่น ๆ อาทิ อีเมล ผู้ดูแล การเข้าถึง ข้อยกเว้น ไฟร์วอลล์ และระบบตรวจจับการบุกรุก และที่เกี่ยวข้องอื่น ๆ โดยวิธีการเก็บรวบรวมหลักฐานควรจะสอดคล้องกับแนวปฏิบัติการจัดเก็บและจัดการสารสนเทศที่ใช้เป็นหลักฐาน

5.29 ความมั่นคงปลอดภัยสารสนเทศระหว่างการหยุดชะงัก (Information security during disruption)

5.29.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อพัฒนาและรักษาความต่อเนื่องของธุรกิจทั่วทั้งบริษัท ประกอบด้วยเทคโนโลยีสารสนเทศ การบริหารจัดการ และด้านอื่น ๆ ของฝ่ายต่าง ๆ

(1) การประเมินต้องคำนึงถึงกระบวนการทางธุรกิจทั้งหมด และไม่จำกัดอยู่เพียงระบบประมวลผลเท่านั้น

(2) ควรทำการวิเคราะห์ผลกระทบทางธุรกิจเพื่อระบุเหตุการณ์ที่สามารถทำให้กระบวนการทางธุรกิจหยุดชะงักลงได้

5.29.2 การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

(1) ต้องมีการปฏิบัติตามแผนความต่อเนื่องทางธุรกิจ หากเกิดเหตุภัยพิบัติ การให้บริการทางธุรกิจที่สำคัญของบริษัทจะสามารถดำเนินการได้ภายใต้กรอบเวลาที่กำหนดไว้

(2) ข้อพิจารณาของข้อกำหนดทางความมั่นคงปลอดภัยสารสนเทศ

(3) สภาพแวดล้อมทางกายภาพของระบบคอมพิวเตอร์สำรองฉุกเฉินจะต้องปฏิบัติตามความมั่นคงปลอดภัยขั้นต่ำ คือ การกำหนดความรับผิดชอบในการเข้าถึงระบบคอมพิวเตอร์สำรองฉุกเฉิน

(4) การเตรียมระบบคอมพิวเตอร์สำรองฉุกเฉินต้องมีสถาปัตยกรรมเครือข่ายเช่นเดียวกับสภาพแวดล้อมปกติ โดยที่ความสามารถในการทำงานซ้ำซ้อนอาจลดลงได้

(5) การเตรียมระบบสารสนเทศต้องมีความปลอดภัยตามแนวทางการดำเนินการของบริษัท

(6) ต้องมีการจัดการข้อมูลตลอดเวลาโดยผู้ควบคุมที่ถูกกำหนดไว้และผู้ใช้

(7) ต้องมีการจัดการสื่อบันทึกโดยผู้ได้รับอนุญาต และทำการจัดเก็บในตู้ที่ถูกล็อกอย่างดี

(8) ในกรณีที่มีการให้บริการจากหน่วยงานภายนอก ต้องมีเอกสารรายชื่อบุคคลผู้มีอำนาจเพื่อที่จะสามารถเริ่มและยุติการให้บริการ

5.29.3 การพัฒนาและจัดทำแผนการบริหารความต่อเนื่องของธุรกิจรวมทั้งความมั่นคงปลอดภัยของข้อมูลสารสนเทศโดยแผนการบริหารความต่อเนื่องของธุรกิจควรประกอบด้วยสิ่งต่อไปนี้

(1) การระบุกระบวนการทางธุรกิจที่มีความสำคัญ และการใช้งานร่วมกันหรือความต่อเนื่องกันของ

(2) กระบวนการเหล่านี้

(3) ลำดับความสำคัญของกระบวนการต่าง ๆ ที่ต้องกู้กลับมา

(4) การระบุความรับผิดชอบทั้งหมดและการเตรียมการสำหรับกรณีฉุกเฉิน

(5) เอกสารเกี่ยวกับวิธีการกู้กระบวนการคืน เช่น Hot Site, Cold Site และทรัพยากรที่ใช้ เป็นต้น

(6) เอกสารเกี่ยวกับขั้นตอนต่าง ๆ ที่ได้ตกลงกันแล้ว

(7) แผนการบริหารความต่อเนื่องของธุรกิจต้องครอบคลุมถึงความต่อเนื่องของกระบวนการทางธุรกิจและบริการที่มีความสำคัญ ข้อกำหนดการดำเนินงาน และการกู้บริการด้านคอมพิวเตอร์คืนจากภัยพิบัติ

(8) พนักงานควรได้รับการฝึกอบรมเกี่ยวกับขั้นตอนการกู้ระบบคืนตามที่ตกลงกัน และจะต้องทำการทดสอบเป็นประจำเพื่อให้มั่นใจว่าพนักงานรู้ว่าต้องตอบสนองอย่างไรเพื่อคงความต่อเนื่องของธุรกิจต่อไป

5.30 ความพร้อมด้าน ICT เพื่อความต่อเนื่องทางธุรกิจ (ICT readiness for business continuity)

การทดสอบ และการประเมินแผนการบริหารความต่อเนื่องของธุรกิจ ควรประกอบด้วยสิ่งต่อไปนี้

(1) ต้องมีการวางแผนการทดสอบด้านความต่อเนื่องทางธุรกิจ

(2) ต้องมีการทดสอบด้านความต่อเนื่องของธุรกิจตามแผนที่กำหนด

(3) ต้องติดตามข้อบกพร่องที่ระบุได้ในระหว่างการทดสอบความต่อเนื่องของธุรกิจ เพื่อนำไปสู่การปรับปรุงแก้ไข

5.31 กฎหมาย ข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และข้อผูกพันตามสัญญา (Legal, statutory, regulatory and contractual requirements)

ต้องระบุ และติดตามกฎหมาย กฎระเบียบ ข้อบังคับ และข้อผูกพันธ์ทางสัญญา ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศให้เป็นปัจจุบัน รวมถึงต้องมีการประเมินความสอดคล้องของกฎหมาย พร้อมนำไปปฏิบัติให้สอดคล้อง

5.32 สิทธิในทรัพย์สินทางปัญญา (Intellectual property rights)

ต้องมีการควบคุมและมีขั้นตอนปฏิบัติที่เหมาะสม สอดคล้องกับกฎหมาย ระเบียบข้อบังคับ ในการใช้งานผลิตภัณฑ์ซอฟต์แวร์ที่มีกรรมสิทธิ์ที่ถูกต้อง

5.33 การป้องกันบันทึก (Protection of records)

บันทึกต่าง ๆ ที่มีความสำคัญของบริษัทต้องได้รับการป้องกันจากการสูญหาย การทำลาย และการปลอมแปลง การเข้าถึง และการเผยแพร่ออกไปโดยไม่ได้รับอนุญาต บันทึกที่มีความสำคัญสูงต้องป้องด้วยวิธีการที่เหมาะสม

5.34 ความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคล (Privacy and protection of personal identifiable information PII)

ข้อมูลที่เป็นข้อมูลส่วนบุคคลที่บริษัทจัดเก็บหรือดูแลไว้ ต้องมีการดำเนินการเกี่ยวกับการรักษาความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมาย ระเบียบข้อบังคับ และข้อกำหนดตามสัญญาที่เกี่ยวข้อง

5.35 การทบทวนด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ (Independent review of information security)

(1) จะต้องมีการตรวจสอบความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงบุคลากร กระบวนการ และเทคโนโลยี อย่างน้อยปีละ1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ ตามช่วงเวลาที่วางแผนไว้ เพื่อหาจุดที่ไม่เป็นไปตามมาตรฐาน

(2) ผู้ตรวจสอบที่ได้รับมอบหมายให้ทำการตรวจสอบความมั่นคงปลอดภัยสารสนเทศจะต้องไม่เป็นผู้ตรวจสอบงานของตนเอง

5.36 การปฏิบัติตามนโยบาย กฎระเบียบ และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ (Compliance with policies, rules and standards for information security)

(1) ผู้บังคับบัญชาต้องมีความรับผิดชอบในการกำกับดูแลการทำงานของพนักงานในทีมเพื่อให้เป็นไปตามแนวปฏิบัติ ขั้นตอน และมาตรฐานด้านความปลอดภัยที่เกี่ยวข้อง ในกรณีที่พบเหตุละเมิดด้านความมั่นคงปลอดภัยจากการปฏิบัติงานของทีมงาน ต้องดำเนินการร้องขอให้ทำการสอบสวน เพื่อเข้าสู่ขั้นตอนของกระบวนการแก้ไขปัญหา

(2) ผู้บังคับบัญชาต้องมีหน้าที่รับผิดชอบในการปฏิบัติตามแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศ

(3) ผู้บริหาร และผู้จัดการฝ่าย ร่วมกันทบทวนแนวทางการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร นโยบายเฉพาะ กฎระเบียบ และมาตรฐานที่เกี่ยวข้อง อย่างสม่ำเสมอ

5.37 เอกสารขั้นตอนการปฏิบัติงาน (Documented operating procedures)

ต้องจัดทำขั้นตอนการปฏิบัติงานสำหรับสิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศ ที่ใช้ในการปฏิบัติงานทั้งหมดเป็นเอกสารและมีพร้อมใช้แก่ผู้ใช้งานทุกคนที่จำเป็นต้องใช้ เพื่อให้มั่นใจว่าจะมีการใช้งานอย่างเหมาะสมและปลอดภัย ขั้นตอนการปฏิบัติงานควรระบุถึงหัวข้อต่าง ๆ ที่เกี่ยวข้อง ดังต่อไปนี้

(1) ขั้นตอนการปฏิบัติงานในการเปิดเครื่องและปิดเครื่อง พร้อมทั้งระบุหน้าที่รับผิดชอบ

(2) กำหนดขั้นตอนการปฏิบัติงาน ควรแสดงรอบระยะเวลา/เกณฑ์ที่ต้องมีการดำเนินการ และ/หรือวิธีการจัดการข้อผิดพลาดที่พบ รวมถึงระบุความเชื่อมโยงหรือความเกี่ยวข้องกับระบบอื่น ๆ ที่สำคัญ

(3) โครงสร้างพื้นฐานของเทคโนโลยีสารสนเทศต้องมีการตั้งค่าอย่างปลอดภัยตามแนวทางความปลอดภัยเบื้องต้น (Hardening Guideline) ก่อนนำไปใช้ในสภาพแวดล้อมการปฏิบัติจริง

(4) มีการควบคุมและลงทะเบียนเอกสาร รวมถึงมีการทบทวนเอกสารให้เป็นปัจจุบันอยู่เสมอ

6. มาตรการควบคุมด้านบุคคล (People control)

6.1 การคัดกรอง (Screening)

จัดให้มีการคัดสรรพนักงานและหน่วยงานภายนอกโดยจะต้องตรวจสอบประวัติของผู้สมัครในด้านต่าง ๆ ก่อนเข้าร่วมงานกับองค์กรและดำเนินการอย่างต่อเนื่องโดยให้สอดคล้องตามกฎหมาย ระเบียบข้อบังคับและจริยธรรมที่เกี่ยวข้องและเหมาะสมต่อข้อกำหนดทางธุรกิจ ชั้นความลับข้อมูลที่จะเข้าถึงและความเสี่ยงที่เกี่ยวข้อง (ทั้งนี้ต้องตกลงกับผู้ถูกคัดเลือก เพื่อขอความเห็นชอบ (Consent) จากพนักงานก่อน) เพื่อให้มั่นใจว่ามีคุณสมบัติครบถ้วนถูกต้อง และสอดคล้องกับหน้าที่ที่ได้รับ

6.2 ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and conditions of employment)

จัดให้มีการลงลายมือชื่อในสัญญาจ้างรับทราบบทบาทหน้าที่ความรับผิดชอบ เงื่อนไขและเกณฑ์การจ้างให้กับพนักงานและ/หรือหน่วยงานภายนอก รวมถึงรับทราบข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ และข้อตกลงการรักษาความลับ รวมถึงความรับผิดชอบต่ออุปกรณ์คอมพิวเตอร์และข้อมูลสารสนเทศที่ตนเองดูแล

6.3 ความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัย (Information security awareness, education and training)

จัดให้มีการอบรมเพื่อสร้างความตระหนักและความรู้ ด้านความมั่นคงปลอดภัยสารสนเทศ นโยบายขององค์กร นโยบายเฉพาะ และขั้นตอนปฏิบัติ ให้กับพนักงาน ลูกจ้าง หรือหน่วยงานภายนอกที่ปฏิบัติงานเกี่ยวข้องกับระบบ

สารสนเทศของบริษัทอย่างน้อยปีละ 1 ครั้ง โดยมีการทดสอบเพื่อวัดผลความสำเร็จในการฝึกอบรมดังกล่าว และติดตามผลหลังการฝึกอบรม

6.4 กระบวนการทางวินัย (Disciplinary process)

ต้องมีการกำหนดมาตรการหรือกระบวนการลงโทษทางวินัยของบริษัท เกี่ยวกับการฝ่าฝืน การละเมิดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ อย่างเป็นทางการและสื่อสารให้ทราบโดยทั่วกัน

6.5 ความรับผิดชอบหลังการสิ้นสุดสภาพหรือการเปลี่ยนแปลงการจ้างงาน (Responsibilities after termination or change of employment)

ต้องกำหนดขั้นตอน บังคับใช้ และสื่อสารให้ทุกหน่วยงานทราบ เกี่ยวกับการสิ้นสุดสภาพหรือเปลี่ยนแปลงการจ้างของพนักงานหรือหน่วยงานภายนอก ผู้รับผิดชอบหรือหัวหน้างานต้องทบทวนบทบาทและหน้าที่ความรับผิดชอบที่ได้รับ เพื่อการบริหารจัดการทรัพย์สินและสิทธิการเข้าถึงระบบสารสนเทศที่เหมาะสม รวมถึงให้มีการส่งถ่ายความรู้ในการทำงานอย่างเป็นทางการ และมีประสิทธิภาพให้กับบุคคลที่ได้รับมอบหมาย ก่อนสิ้นสุดหรือเปลี่ยนแปลงสัญญาจ้างงาน พนักงานต้องรักษาความลับขององค์กร ไม่นำข้อมูลที่เป็นความลับไปใช้ประโยชน์หรือเผยแพร่เด็ดขาด

6.6 ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or non-disclosure agreements)

ให้ผู้บริหาร พนักงานทุกคน รวมถึงพนักงานจากหน่วยงานทั้งภายในและภายนอกบริษัทที่ใช้ระบบสารสนเทศ ต้องทำข้อตกลงการรักษาความลับของข้อมูล โดยให้มีข้อความระบุไม่ให้เปิดเผยความลับไปยังผู้ที่ไม่เกี่ยวข้องและให้ลงลายมือชื่อรับทราบ โดยข้อความควรประกอบด้วยหัวข้อ ดังนี้

(1) ห้ามเปิดเผยความลับไปยังผู้ที่ไม่เกี่ยวข้อง รวมถึงบทลงโทษหรือสิ่งที่จะดำเนินการหากพบว่ามีการละเมิด

(2) ปฏิบัติตามแนวปฏิบัติความมั่นคงปลอดภัยที่เกี่ยวข้องในการไม่เปิดเผยความลับ เพื่อป้องกันไม่ให้ข้อมูลมีการรั่วไหลไปยังผู้ที่ไม่เกี่ยวข้อง

(3) การให้ความร่วมมือในการตรวจสอบกิจกรรมหากพบข้อสงสัยหรือข้อร้องเรียน

6.7 การปฏิบัติงานจากระยะไกลและการควบคุมการเข้าถึง (Remote Work & Zero-Trust Mindset)

การปฏิบัติงานจากระยะไกล(Remote Access) มีแนวทางปฏิบัติดังนี้

(1) **สิทธิ์ขั้นต่ำที่จำเป็น (Least Privilege)** ให้สิทธิ์การเข้าถึงระบบและข้อมูลบนพื้นฐานของความจำเป็นต้องทราบ (Need-to-know) และสอดคล้องกับหน้าที่ความรับผิดชอบ

(2) **การเชื่อมต่อระยะไกล (Remote Access)** การปฏิบัติงานจากระยะไกลต้องผ่านช่องทางที่ปลอดภัย ได้รับการอนุมัติอย่างเป็นทางการ และหากเป็นผู้ให้บริการภายนอก (Third Party) ต้องมีการควบคุมหรือตรวจสอบการเข้าถึงอย่างใกล้ชิดและใช้บัญชีผู้ใช้งานแยกต่างหาก

(3) **ความปลอดภัยของอุปกรณ์** อุปกรณ์พกพาจะต้องมีการล็อกรหัสผ่าน เข้ารหัสข้อมูลระดับดิสก์ (Disk Encryption) สำหรับข้อมูลความลับ และติดตั้งโปรแกรมป้องกันมัลแวร์ที่อัปเดตเสมอ

6.8 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information security event reporting)

ต้องกำหนดกลไกและช่องทางที่ใช้รายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information security event reporting) และแจ้งให้ผู้ใช้งานทุกคนทราบ ผู้ใช้งานต้องไม่พยายามแก้ไขความผิดปกติที่ต้องสงสัย แต่ให้รายงานตามกระบวนการที่กำหนด เพื่อประโยชน์ในการตรวจสอบจากผู้ดูแลหรือผู้เชี่ยวชาญเว้นแต่จะได้รับอนุญาต

7. มาตรการควบคุมด้านกายภาพ (Physical controls)

7.1 อาณาเขตความมั่นคงปลอดภัยทางกายภาพ (Physical security perimeters)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงมอบหมายให้ผู้ดูแลอาคารและพนักงานรักษาความปลอดภัยสอดส่องดูแลการเข้าถึงพื้นที่และเหตุการณ์ผิดปกติเพื่อให้ทรัพย์สินที่อยู่ภายในมีความมั่นคงปลอดภัย โดยมีการแบ่งพื้นที่ด้านความมั่นคงปลอดภัย ได้แก่ พื้นที่ที่ต้องมีการควบคุมการเข้าถึง โดยมีการจำกัดการเข้าถึงพื้นที่ตามความจำเป็น (Need-to-Access) โดยแบ่งระดับพื้นที่เป็น 2 ระดับ ได้แก่

(1) พื้นที่หวงห้าม คือ พื้นที่ที่มีระดับความสำคัญสูงสุด โดยเป็นพื้นที่ที่เก็บอุปกรณ์สำคัญ พื้นที่ในส่วนนี้ได้แก่ พื้นที่ศูนย์คอมพิวเตอร์ ห้องจ่ายกระแสไฟฟ้า เป็นต้น

(2) พื้นที่ปฏิบัติงาน คือ พื้นที่ที่มีความสำคัญระดับรองลงมา โดยพื้นที่ส่วนนี้มีการควบคุมการเข้า-ออกเฉพาะผู้ที่เกี่ยวข้อง ได้แก่ พื้นที่ห้องปฏิบัติงาน (Office Area) ห้องสำนักงาน ห้องประชุม เป็นต้น

7.2 การเข้า-ออกพื้นที่ (Physical entry)

ให้มีการควบคุมการเข้า-ออกพื้นที่ โดยมีแนวปฏิบัติดังนี้

(1) พนักงานที่ได้รับสิทธิในการเข้า-ออกพื้นที่ที่มีการติดตั้งอุปกรณ์อ่านบัตรหรือลายนิ้วมือ จะต้องเข้ากระบวนการลงทะเบียนและเพิกถอนสิทธิผู้ใช้งาน (User Registration/De-registration Procedure)

(2) งดการออกบัตรหรือการใช้ข้อมูลอัตลักษณ์ (Biometric Data) ในการเข้าถึงระบบสารสนเทศให้กับหน่วยงานภายนอกที่เข้าออกพื้นที่ชั่วคราว ยกเว้นมีเหตุจำเป็นโดยต้องได้รับการอนุมัติอย่างเป็นทางการ

(3) กำหนดให้หน่วยงานภายนอกที่เข้าถึงพื้นที่ของฝ่ายเทคโนโลยีสารสนเทศจะต้องติดบัตรผู้มาติดต่อในตำแหน่งที่เห็นได้ง่าย

(4) พนักงานที่อยู่ต่างฝ่าย และหน่วยงานภายนอกที่มีความประสงค์เข้าพื้นที่หวงห้ามจะต้องแจ้งความประสงค์ล่วงหน้า และมีผู้ติดตามระหว่างเข้าถึงพื้นที่ตลอดเวลา โดยบันทึกการเข้า-ออกทุกครั้ง

7.3 ความมั่นคงปลอดภัยของสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวก (Securing offices, rooms and facilities)

ห้องปฏิบัติงาน ห้องที่มีทรัพย์สินและอุปกรณ์ ต้องมีความมั่นคงปลอดภัย โดยครอบคลุมประเด็นสำคัญ ดังนี้

(1) อาคารหรือพื้นที่ที่มีความสำคัญ เช่น ศูนย์คอมพิวเตอร์ ฯลฯ มีความแข็งแรงและปลอดภัย ไม่สามารถรุกล้ำเข้าไปได้โดยง่าย

(2) หลีกเลี่ยงการวางอุปกรณ์เทคโนโลยีสารสนเทศที่สำคัญไว้บริเวณพื้นที่ส่วนกลาง, ล็อกหน้าจอคอมพิวเตอร์ทุกครั้ง, ไม่เขียนรหัส User/Password ติดไว้ที่อุปกรณ์เข้ารหัสต่าง ๆ

(3) สำนักงาน ห้องทำงาน สิ่งอำนวยความสะดวก และสภาพแวดล้อมของการปฏิบัติงานจะต้องมีความปลอดภัย

7.4 การเฝ้าติดตามความมั่นคงปลอดภัยทางกายภาพ (Physical security monitoring)

กำหนดวิธีการเฝ้าติดตามความมั่นคงปลอดภัยทางกายภาพ

(1) จัดทำแผนผังที่ตั้งอาคารที่ใช้เป็นพื้นที่ในการปฏิบัติการ และแสดงระดับความสำคัญของพื้นที่

(2) ประตูและหน้าต่างที่อยู่ในพื้นที่ด้านความมั่นคงปลอดภัยจะต้องทำจากวัสดุที่แข็งแรง และต้องปิดล็อกทุกบาน เพื่อป้องกันการบุกรุกจากภายนอก

(3) กำหนดให้พนักงานรักษาความปลอดภัยแลกบัตรของผู้มาติดต่อจากหน่วยงานภายนอก และจดบันทึกเพื่อใช้ในการตรวจสอบย้อนหลัง

(4) จัดให้มีการติดตั้ง CCTV ให้ครอบคลุมพื้นที่หวงห้ามเด็ดขาดและทางเข้า-ออกบริเวณพื้นที่หวงห้าม โดยสามารถเรียกดูภาพบันทึกภาพย้อนหลังได้

7.5 การป้องกันภัยคุกคามทางกายภาพและสิ่งแวดล้อม (Protecting against physical and environmental threats)

ต้องกำหนดแผนป้องกันภัยคุกคามทางกายภาพและสภาพแวดล้อม เพื่อใช้เป็นมาตรการในการเตรียมพร้อมรับเหตุอันที่อาจเกิดขึ้นได้ตลอดเวลา และไม่กระทบต่อการให้บริการของบริษัทฯ โดย

(1) ประเมินภัยคุกคามทั้งหมดที่อาจเกิดขึ้นได้ ทั้งจากทางกายภาพและสิ่งแวดล้อม

(2) จัดทำแผนหรือมาตรการรองรับ

(3) อาจมีการทบทวนเป็นประจำ อย่างน้อยปีละ 1 ครั้ง และมีการฝึกซ้อมตามความเหมาะสม

(4) ประเมินและปรับปรุงแผนหรือแนวทางการปฏิบัติหลังจากการฝึกซ้อมให้เหมาะสมขึ้น

7.6 การปฏิบัติงานในบริเวณที่ต้องรักษาความมั่นคงปลอดภัย (Working in secure areas)

ให้พื้นที่ของการปฏิบัติงานด้านเทคโนโลยีสารสนเทศมีการออกแบบให้มีความมั่นคงปลอดภัย โดยมีแนวปฏิบัติดังนี้

(1) ห้ามพนักงานที่ไม่มีหน้าที่ในการปฏิบัติงานในพื้นที่ และหน่วยงานภายนอกเข้าพื้นที่หวงห้าม เพื่อป้องกันการดำเนินการใด ๆ ที่ไม่ได้รับอนุญาต

(2) ต้องปิดล็อกประตูห้องที่ไม่มีการใช้งาน ปิดประตูและหน้าต่างทุกครั้งที่เลิกงาน หรือเมื่อไม่มีผู้ดูแล

(3) ไม่อนุญาตให้นำอุปกรณ์ถ่ายภาพ วิดีโอ เสียง หรืออุปกรณ์บันทึกอื่น ๆ เข้ามาภายในศูนย์คอมพิวเตอร์ เว้นแต่จะได้รับอนุญาต

(4) ไม่อนุญาตให้นำหรือรับประทานอาหารและเครื่องดื่มในศูนย์คอมพิวเตอร์

7.7 การจัดการเก็บโต๊ะทำงาน และจัดการหน้าจอ (Clear desk and clear screen)

(1) ข้อมูลที่จัดเก็บในสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ จะต้องได้รับการป้องกันจำแนกตามประเภทของข้อมูลที่กำหนดไว้ ในแนวปฏิบัติการจัดระดับชั้นความลับ การติดป้ายและการจัดเก็บข้อมูล

(2) ผู้ใช้งานไม่ควรวางเอกสารสำคัญไว้บนโต๊ะทำงาน และตั้งค่าตามแนวปฏิบัติป้องกันหน้าจอคอมพิวเตอร์ เพื่อป้องกันการเข้าถึงข้อมูลทางกายภาพต่อเอกสารและข้อมูลสำคัญของบริษัท

(3) เมื่อไม่อยู่ที่โต๊ะทำงาน ต้องกดล็อกหน้าจอทันที ก่อนออกไปจากโต๊ะทำงาน

(4) ควรจัดเก็บเอกสารข้อมูลที่สำคัญของบริษัทไว้ในที่มิดชิด รวมถึงสื่อบันทึกข้อมูลควรมีการเข้ารหัสป้องกันโดยเอกสารและสื่อที่เก็บข้อมูลควรเก็บไว้ในที่มิดชิด หรือใส่ตู้ที่มีกุญแจล็อก

(5) จะต้องไม่ติด Username/Password ไว้ที่หน้าจอ

(6) ตรวจสอบทุกครั้งว่าไม่มีเอกสารใด ๆ ตกค้างอยู่ที่เครื่องถ่ายเอกสาร หรือเครื่องส่งแฟกซ์ หลังจากถ่ายสำเนา หรือส่งแฟกซ์เสร็จแล้ว

(7) ไม่ปล่อยให้เอกสารสำคัญ หรือ เอกสารลับ ตกค้างที่เครื่องถ่ายสำเนา หรือ เครื่องส่งแฟกซ์

(8) โทรศัพท์มือถือ(ที่เป็นของบริษัท) ควรตั้งรหัสผ่านหน้าจอ

(9) อุปกรณ์ที่สำคัญอื่น ๆ เช่น USB thump drive/External HDD/ etc. ไม่ควรวางทิ้งไว้บนโต๊ะ

(10) กรณีใช้ notebook หลังเลิกงาน ควรเก็บไว้ในลิ้นชัก ถ้าไม่เก็บ ให้พับหน้าจอและมีสายล็อกเครื่องไว้

7.8 การจัดวางและการป้องกันอุปกรณ์ (Equipment siting and protection)

การวางอุปกรณ์ภายในศูนย์คอมพิวเตอร์จะต้องปฏิบัติตามข้อกำหนดดังต่อไปนี้

(1) ต้องใช้ชั้นวางอุปกรณ์ (Server Rack) สำหรับวางเซิร์ฟเวอร์และอุปกรณ์เครือข่ายที่สำคัญ
(2) ต้องปิดล็อกประตูชั้นวางทุกครั้งเมื่อสิ้นสุดการใช้งาน และกำหนดบุคลากรผู้มีสิทธิเปิดประตู
(3) ต้องติดตั้ง CCTV หน้าชั้นวางอุปกรณ์สำคัญเพื่อใช้ตรวจสอบผู้ใช้งานอุปกรณ์ในชั้นวาง
(4) ต้องเฝ้าระวังอุณหภูมิและความชื้นภายในพื้นที่หวงห้าม
(5) อุปกรณ์เครือข่ายหรืออุปกรณ์จัดเก็บข้อมูลที่สำคัญ ต้องมีการติดตั้งเครื่องปรับเสถียรไฟฟ้า (Stabilizer) เพื่อป้องกันไฟฟ้ากระชาก หรือกระแสไฟที่ไม่เสถียรจนทำให้อุปกรณ์ดังกล่าวชำรุดเสียหาย

7.9 ความมั่นคงปลอดภัยของทรัพย์สินที่ใช้งานนอกสำนักงาน (Security of assets off-premises)

การนำอุปกรณ์ออกนอกสำนักงานจะต้องได้รับอนุมัติจากเจ้าของอุปกรณ์ ผู้จัดการฝ่ายหรือผู้มีอำนาจในการอนุมัติเมื่อมีความประสงค์ในการนำอุปกรณ์ออกนอกสำนักงาน โดยมีข้อกำหนด ดังนี้

(1) นำอุปกรณ์ติดตัวอยู่ตลอดเวลา และไม่ทิ้งอุปกรณ์ไว้โดยไม่มีผู้ดูแล
(2) กำหนดกระบวนการจัดการข้อมูลที่มีความสำคัญที่อยู่ในอุปกรณ์ หากอุปกรณ์ชำรุดหรือสูญหาย
(3) มีการดูแลรักษาอุปกรณ์ตามคำแนะนำของผู้ผลิต หรือผู้ดูแลหลัก
(4) การจัดการข้อมูล ต้องเป็นไปตามมาตรฐานการจัดการข้อมูลตามระดับชั้นสูงสุดที่มีอยู่ภายในอุปกรณ์นั้น เช่น การทำ disk encryption หากเป็นข้อมูลระดับลับขึ้นไป

7.10 สื่อบันทึกข้อมูล (Storage media)

การบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยกหรือพกพาได้ โดยมีข้อกำหนด ดังนี้

(1) ต้องมีการจัดการข้อมูลสารสนเทศที่อยู่ในสื่อบันทึกนั้น ๆ โดยปฏิบัติตามแนวปฏิบัติการจัดระดับชั้นความลับ การติดป้าย และการจัดการข้อมูล (Information Classification, Labelling and Handling Guideline)
(2) สื่อบันทึกข้อมูลที่ล้าสมัยและไม่ใช้งานแล้วจะต้องถูกทำลายทิ้งตามมาตรฐานในการกำจัดสื่อบันทึกข้อมูลที่ได้กำหนดไว้
(3) การนำสื่อบันทึกข้อมูลที่นำออกไปใช้ภายนอกบริษัท ต้องได้รับการป้องกันอย่างเหมาะสม และผู้นำส่งสื่อบันทึกข้อมูล ต้องเป็นบุคคลหรือหน่วยงานที่ได้รับการรับรองและเชื่อถือได้
(4) สื่อบันทึกข้อมูล ที่จัดหาต้องเป็นไปตามมาตรฐานตามที่กำหนด จำหน่ายและขนส่งโดยบริษัทที่น่าเชื่อถือ

7.11 ระบบสาธารณูปโภคสนับสนุน (Supporting utilities)

จัดให้มีการติดตั้งอุปกรณ์สนับสนุน ระบบปรับอากาศ ระบายอากาศ ระบบแสงสว่าง และระบบดับเพลิงให้กับอุปกรณ์ในพื้นที่หวงห้าม รวมถึงประสานงานกับฝ่ายอาคารในการสนับสนุนและจัดหาให้มีการติดตั้งและสนับสนุนระบบไฟฟ้าให้กับอุปกรณ์ในพื้นที่ ดังนี้

(1) ต้องใช้ระบบสำรองกระแสไฟฟ้าต่อเนื่อง (UPS) เพื่อให้กระแสไฟฟ้ามีความเสถียร และป้องกันอุปกรณ์เสียหายจากเหตุไฟตก/ไฟกระชาก
(2) ต้องติดตั้งระบบปรับอากาศเพื่อสร้างสภาพแวดล้อมที่เหมาะสมให้กับอุปกรณ์

(3) ต้องติดตั้งไฟฉุกเฉินเพื่อให้บริการแสงสว่าง

(4) ต้องติดตั้งระบบแจ้งเตือน (Tele-Alarm) เพื่อแจ้งเตือนผู้ปฏิบัติงานเมื่อตรวจพบเหตุผิดปกติ

(5) ต้องติดตั้งระบบกำเนิดไฟฟ้าสำรองเพื่อให้กระแสไฟฟ้ามีความเสถียร

(6) ต้องมีระบบดับเพลิงหรืออุปกรณ์ดับเพลิงที่เหมาะสม และพร้อมใช้งานอยู่ตลอดเวลา และให้มีการตรวจเช็คตามรอบ

7.12 ความมั่นคงปลอดภัยของการเดินสาย (Cabling security)

ในการติดตั้งสายเคเบิลภายในพื้นที่หวงห้ามจะต้องปฏิบัติตามข้อกำหนดดังต่อไปนี้

(1) สายเคเบิลที่ใช้ในการสื่อสารข้อมูลอยู่ในท่อหรือราง

(2) มีการแยกสายไฟและสายเคเบิลเครือข่ายออกจากกันเพื่อป้องกันสัญญาณรบกวน การขัดขวางการทำงาน การแทรกแซงสัญญาณ หรือการทำให้เสียหาย

(3) จุดเชื่อมต่อเครือข่าย (Network Termination Point) จะต้องมีการป้องกันทางกายภาพเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(4) ต้องติดป้ายเพื่อระบุต้นทางและปลายทางของสายเคเบิลที่ใช้เชื่อมต่อเข้ากับอุปกรณ์เทคโนโลยีสารสนเทศ

7.13 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

จัดให้มีการบำรุงรักษาอุปกรณ์ที่หน่วยงานเป็นผู้ดูแลอย่างสม่ำเสมอ โดยมีหัวข้อสำคัญดังนี้

(1) มีการบำรุงรักษาระบบอุปกรณ์และระบบสนับสนุนการทำงานของอุปกรณ์ตามคำแนะนำของผู้ผลิต

(2) อนุญาตเฉพาะบุคลากรที่ผ่านการฝึกอบรมและได้รับการมอบหมายให้ทำการซ่อมบำรุงรักษา

(3) ในกรณีที่ใช้บริการซ่อมบำรุงจากหน่วยงานภายนอกจะต้องกำหนดเงื่อนไข และรอบระยะเวลาในการบำรุงรักษาอย่างละเอียด

7.14 การจำหน่ายหรือนำอุปกรณ์มาใช้ซ้ำอย่างมั่นคงปลอดภัย (Secure disposal or re-use of equipment)

เมื่อใช้งานอุปกรณ์เสร็จหรือต้องการนำอุปกรณ์กลับมาใช้ใหม่ให้ปฏิบัติดังนี้

(1) อุปกรณ์ที่มีสื่อบันทึกข้อมูลต้องได้รับการตรวจสอบ เพื่อให้มั่นใจว่าข้อมูลที่ละเอียดอ่อนและซอฟต์แวร์ลิขสิทธิ์ที่ติดตั้งอยู่ได้ถูกลบออก หรือเขียนทับอย่างมั่นคงปลอดภัย ก่อนนำไปจำหน่าย หรือนำไปใช้ซ้ำ

(2) ตรวจสอบลิขสิทธิ์ซอฟต์แวร์โดยมีการถอดถอนหรือยกเลิกการลงทะเบียนเพื่อให้สามารถนำซอฟต์แวร์ไปติดตั้งที่เครื่องอื่นได้

(3) เมื่อไม่ต้องการใช้ข้อมูลที่จัดเก็บอยู่ในอุปกรณ์ให้ทำการลบเพื่อป้องกันไม่ให้มีการเข้าถึง และสามารถนำข้อมูลมาใช้โดยไม่ได้รับอนุญาต โดยทำการลบ เขียนซ้ำ หรือทำลายข้อมูลอย่างถาวร

8. มาตรการควบคุมด้านเทคโนโลยี (Technological controls)

8.1 อุปกรณ์ระดับผู้ใช้งาน (User end point devices)

การรักษาความมั่นคงปลอดภัยของอุปกรณ์คอมพิวเตอร์แบบพกพา มีขอบเขตครอบคลุมถึงอุปกรณ์พกพา หรืออุปกรณ์เคลื่อนที่ใด ๆ ของบริษัทที่ใช้ในการเก็บข้อมูลหรือประมวลผลข้อมูลของบริษัท โดยมีแนวทางปฏิบัติดังนี้

(1) ควบคุมการติดตั้งซอฟต์แวร์บนอุปกรณ์ระดับผู้ใช้งาน โปรแกรมที่ไม่ได้รับอนุญาต กำหนดมาตรการการเข้าใช้งานจากที่อื่น

(2) ต้องมีการป้องกันหรือการล็อกอุปกรณ์พกพา และคอมพิวเตอร์พกพาอย่างเหมาะสม เมื่อไม่ได้ใช้งานภายในสำนักงาน

(3) ต้องติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ (Antivirus) บนคอมพิวเตอร์แบบพกพา และทำการปรับปรุงข้อมูลไวรัส (Virus Pattern) ให้ทันสมัยอยู่เสมอ

(4) คอมพิวเตอร์แบบพกพาต้องได้รับการป้องกันทางกายภาพอย่างเหมาะสมจากการเข้าถึงโดยไม่ได้รับอนุญาต เช่น การปิด USB Port

(5) ห้ามใช้ทรัพยากรของบริษัท เพื่อหรือสนับสนุนวัตถุประสงค์ที่ผิดกฎหมายตามที่กฎหมายได้บัญญัติไว้โดยเด็ดขาด

(6) ห้ามใช้ทรัพยากรของบริษัททำกิจกรรมทางการเมืองภายในบริษัทโดยเด็ดขาด

(7) การใช้งานทรัพยากรของบริษัทจะทำได้เฉพาะพนักงานหรือผู้ที่ได้รับอนุญาตเท่านั้น และใช้เพื่อวัตถุประสงค์ในการทำงานเท่านั้น

(8) ควรปฏิบัติตามคำแนะนำของผู้ผลิตในการปกป้องอุปกรณ์ตลอดเวลา เช่น การป้องกันการสัมผัสกับสนามแม่เหล็กไฟฟ้าที่มีศักย์สูง การป้องกันแสงแดดโดยตรง ฯลฯ

(9) ต้องไม่วางอุปกรณ์ไว้ในที่สาธารณะโดยที่ไม่มีคนดูแล ผู้ดูแลทรัพย์สินนั้นมีหน้าที่รับผิดชอบในการดูแลและป้องกันอุปกรณ์ต่าง ๆ นั้น หากอุปกรณ์เสียหาย สูญหาย หรือเกิดการลักขโมย จะต้องแจ้งผู้บังคับบัญชาและผู้ดูแลระบบให้ทราบทันทีเพื่อให้มีการติดตามและมีวิธีการจัดการกับเหตุการณ์ได้อย่างมีประสิทธิภาพ

(10) พนักงานและผู้จัดการส่วนหรือเทียบเท่าขึ้นไปของบริษัทมีหน้าที่จะต้องดูแลให้เครื่องคอมพิวเตอร์ที่ใช้งานในความรับผิดชอบ ได้รับการติดตั้งโปรแกรมใช้งานโดยถูกต้องตามนโยบายของบริษัท

(11) การจัดการข้อมูล ต้องเป็นไปตามมาตรฐานการจัดการข้อมูลตามระดับชั้นสูงสุดที่มีอยู่ภายในอุปกรณ์นั้น

(12) ใช้เครื่องหูฟังเพื่อรักษาความเป็นส่วนตัวและไม่รบกวนคนรอบข้าง

(13) พนักงานต้องดูแลรักษาความสะอาดของอุปกรณ์คอมพิวเตอร์พกพาที่ตนเองรับผิดชอบอยู่เสมอ

(14) ห้ามพนักงานใช้งานอุปกรณ์คอมพิวเตอร์ของบริษัทในการขุดเหรียญคริปโตเคอเรนซี่และห้ามใช้อุปกรณ์คอมพิวเตอร์ของบริษัทในการหาประโยชน์ส่วนตน เล่นการพนัน หรือเข้าเว็บลามกอนาจารเด็ดขาด

8.2 สิทธิพิเศษในการเข้าถึง (Privileged access rights)

กำหนดสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศตามความจำเป็นที่ต้องใช้งาน โดยมีแนวปฏิบัติดังนี้

(1) สิทธิที่ให้กับพนักงานและหน่วยงานภายนอกไม่ทำให้ความมั่นคงปลอดภัยด้านสารสนเทศลดลง

(2) ต้องกำหนดสิทธิให้ตรงตามหน้าที่การใช้งานอย่างชัดเจน แบ่งแยกสิทธิผู้ใช้งาน (User) กับสิทธิผู้ดูแล (Administrator) ออกจากกัน

(3) จำกัดบุคคลที่มีสิทธิผู้ดูแล (Administrator) ซึ่งหากมีความจำเป็นชั่วคราวที่ต้องใช้สิทธิดังกล่าว ให้กำหนดระยะเวลาที่อนุญาตและมีการทบทวนการให้สิทธิอย่างสม่ำเสมอ

(4) ต้องบันทึกสิทธิที่ให้ในแต่ละบัญชีผู้ใช้งานและมีการทบทวนความเหมาะสมของสิทธิที่ได้อย่างสม่ำเสมอ

8.3 การจำกัดการเข้าถึงข้อมูล (Information access restriction)

กำหนดให้มีแนวปฏิบัติในการเข้าถึงข้อมูลและโปรแกรม ดังนี้

(1) การเข้าถึงสารสนเทศสอดคล้องกับระดับชั้นความลับของข้อมูล

(2) กำหนดสิทธิของผู้ใช้งานในโปรแกรม สำหรับสิทธิในการอ่าน เขียน ลบ ฯลฯ ข้อมูลที่อยู่ภายใน ตามหน้าที่ความรับผิดชอบ

(3) เมนู/ฟังก์ชันในการใช้งานโปรแกรมสอดคล้องกับสิทธิที่ได้รับ

(4) มาตรการควบคุมการเข้าถึงของผู้ใช้บริการ (Outsource) ต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่กำหนดให้เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนอื่น ก็ต้องมีการควบคุมหรือตรวจสอบการเข้าถึงของผู้ให้บริการ โดยให้ผู้ดูแลระบบควบคุมดูแลการทำงานของผู้ให้บริการอย่างใกล้ชิดในกรณีที่ผู้ให้บริการมาปฏิบัติหน้าที่ ที่บริษัท และให้ผู้ดูแลระบบตรวจสอบการทำงานของผู้ให้บริการอย่างละเอียดในกรณีที่เป็นการให้บริการในลักษณะ Remote Access และปิด Modem ทันทีที่การให้บริการเสร็จสิ้น

(5) กำหนดให้ผู้บริการ (Outsource) ลงนามในสัญญารักษาความลับ

8.4 การเข้าถึงซอร์สโค้ด (Access to source code)

ต้องกำหนดให้ควบคุมการเข้าถึงซอร์สโค้ดตามแนวปฏิบัติ ดังนี้

(1) อนุญาตให้มีการเข้าถึงซอร์สโค้ดเฉพาะผู้มีสิทธิเท่านั้น โดยจัดทำบัญชีรายชื่อผู้ที่มีสิทธิการเข้าถึงอย่างเป็นลายลักษณ์อักษร

(2) มีการควบคุมเวอร์ชั่นของซอร์สโค้ด

(3) มีการเปิดบันทึกเหตุการณ์การเข้าถึงซอร์สโค้ด

8.5 การพิสูจน์ตัวตนอย่างมั่นคงปลอดภัย (Secure authentication)

กำหนดให้มีการบริหารจัดบัญชีผู้ใช้งาน โดยมีแนวปฏิบัติดังนี้

(1) กำหนดให้มีการพิสูจน์ตัวตนในระบบที่อนุญาตให้มีผู้ใช้หลายคน (Multi-user Application) โดยการใช้ Multi Factor Authentication ของผู้ใช้งานทุกครั้งในการเข้าสู่ระบบ

(2) ผู้ใช้งานแต่ละคนจะต้องมีบัญชีผู้ใช้ไม่ซ้ำกัน ไม่สามารถใช้ร่วมกัน หรือโอนให้กันได้

(3) ในกรณีที่จำเป็นต้องสร้างบัญชีผู้ใช้กลุ่มเพื่อใช้งานร่วมกันจะต้องได้รับการอนุมัติอย่างเป็นทางการจากผู้บังคับบัญชาของผู้ร้องขอ และจากผู้จัดการฝ่ายที่เกี่ยวข้องที่ดูแลระบบนั้น ๆ และมีการควบคุมการใช้งานอย่างเคร่งครัด เช่น กำหนดและบันทึกช่วงเวลาที่ใช้งาน

8.6 การบริหารจัดการขีดความสามารถของทรัพยากร (Capacity Management)

ต้องจัดให้มีการบริหารทรัพยากรสารสนเทศให้เพียงพอกับความต้องการใช้งานของระบบ

(1) ควรมีการวางแผนเฝ้าระวัง/ทบทวน ระดับความต้องการทรัพยากรของระบบอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าทรัพยากรของระบบที่ใช้งานอยู่เพียงพอที่จะรองรับปริมาณการใช้งานที่เพิ่มขึ้น

(2) ควรกำหนดระดับการเตือนและระดับแจ้งเตือนเพื่อใช้เป็นจุดอ้างอิงในการปรับแต่งระบบต่อไป

8.7 การป้องกันจากโปรแกรมไม่พึงประสงค์ (Protection against malware)

กำหนดให้มีแนวปฏิบัติดังนี้

(1) พนักงานทุกคนจะต้องได้รับความรู้และคำแนะนำเกี่ยวกับการป้องกันและจัดการไวรัส

(2) ผู้ใช้จะต้องติดตั้งซอฟต์แวร์ที่ได้รับการอนุมัติแล้วเท่านั้น หากซอฟต์แวร์นั้น ไม่อยู่ในเอกสารรายชื่อซอฟต์แวร์ที่ได้รับการอนุมัติ ผู้ติดตั้งต้องดำเนินการขออนุญาตต่อผู้บริหารก่อนทำการติดตั้ง

(3) ผู้ใช้งานจะต้องตรวจสอบให้แน่ใจว่าไฟล์อัปเดตโปรแกรมแอนตี้ไวรัสเป็นข้อมูลล่าสุดก่อนที่จะดาวน์โหลดไฟล์ภายนอกหรือเชื่อมต่อบริการอินเทอร์เน็ต

(4) ผู้ใช้งานจะต้องไม่พยายามเปิดไฟล์ที่ไม่ได้ร้องขอหรือน่าสงสัย ผ่านอีเมลอิเล็กทรอนิกส์ การส่งข้อความแชต หรือระบบเครือข่ายสังคมอื่น ๆ ต้องขอคำชี้แจงเกี่ยวกับวัตถุประสงค์ของไฟล์กับผู้ส่งก่อนที่จะทำการเปิด

(5) ผู้ใช้งานจะต้องสแกนสื่อบันทึกข้อมูลภายนอก ซึ่งเคยเชื่อมต่อกับระบบสารสนเทศอื่นที่ไม่ใช่ของบริษัท เพื่อตรวจสอบไวรัส

(6) หากอุปกรณ์คอมพิวเตอร์ที่ผู้ใช้งานดูแลติดไวรัสและไม่สามารถจัดการได้ด้วยตนเองให้ดำเนินการ ดังนี้

a. ตัดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์และระบบเครือข่าย
b. ติดต่อผู้ดูแลระบบให้เร็วที่สุด
c. ไม่พยายามลบหรือแก้ไขไฟล์ระบบ (System Files) ด้วยตนเอง
d. ให้ความร่วมมือผู้ดูแลระบบในการแก้ไขปัญหาจนกว่าผู้ดูแลระบบจะตรวจสอบว่าไวรัสทั้งหมดถูกลบออกแล้ว
e. หากการดูแลระบบไม่สามารถลบไวรัสทั้งหมดในระบบที่ติดไวรัส ซอฟต์แวร์และไฟล์ทั้งหมดในคอมพิวเตอร์ จะต้องถูกลบรวมถึงข้อมูลการบูตเครื่องหากจำเป็น และซอฟต์แวร์จะได้รับการติดตั้งใหม่และสแกนหาไวรัสอีกครั้ง

8.8 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)

(1) มีการระบุบทบาทและหน้าที่ความรับผิดชอบ รวมไปถึงการเฝ้าระวังช่องโหว่ การประเมินความเสี่ยง การปิดช่องโหว่ การติดตามทรัพย์สิน และการประสานงานอื่น ๆ ที่จำเป็น

(2) กำหนดขั้นตอนหรือมาตรการเพื่อการปรับปรุงประสิทธิภาพด้านความปลอดภัยของระบบปฏิบัติ

8.9 การจัดการการตั้งค่า (Configuration management)

Configuration ของฮาร์ดแวร์ ซอฟต์แวร์ บริการ และเครือข่าย มุ่งเน้นรักษาความมั่นคงปลอดภัย โดยมีแนวทางดังนี้

(1) จัดเก็บ Configuration เริ่มต้น กรณีที่มีการเปลี่ยนแปลง Configuration ต้องจัดเก็บ Version เก่าอย่างน้อย 1 Revision ใช้เพื่อกู้คืนระบบและอุปกรณ์ในกรณีที่เกิดความผิดพลาด

(2) กรณีที่ต้องการเปลี่ยนแปลง Configuration ต้องผ่านกระบวนการบริหารการจัดการการเปลี่ยนแปลง (Change Management)

(3) ต้องได้รับการสำรองข้อมูลและจัดเก็บไว้ในสถานที่ที่ปลอดภัย

(4) ต้องมีการทบทวนความถูกต้องของค่า Configuration อย่างน้อยปีละ 1 ครั้ง

8.10 การลบข้อมูล (Information deletion)

ข้อมูลที่ละเอียดอ่อน เช่น ข้อมูลส่วนบุคคล ข้อมูลทางการเงิน ข้อมูลลับทางธุรกิจ ที่จัดเก็บไว้ในระบบสารสนเทศ อุปกรณ์ หรือสื่อบันทึกข้อมูล ต้องถูกลบออก เมื่อไม่มีความจำเป็นต้องใช้งานข้อมูลนั้นอีก และให้สอดคล้องกับกฎหมายที่กำหนด

(1) ระบุประเภทและระยะเวลาของข้อมูลที่ต้องถูกลบ และการขออนุมัติและผู้ที่มีสิทธิ์อนุมัติของข้อมูลแต่ละประเภท

(2) กำหนดวิธีการลบ / เครื่องมือที่ใช้ลบข้อมูล พร้อมเก็บหลักฐานการลบข้อมูล

8.11 การซ่อนข้อมูล (Data masking)

ข้อมูลที่ละเอียดอ่อน เช่น ข้อมูลส่วนบุคคล ข้อมูลทางการเงิน ที่จัดเก็บไว้ในระบบสารสนเทศ อุปกรณ์ หรือสื่อบันทึกข้อมูล ต้องถูกซ่อน บดบังหรือแปลงข้อมูลบางส่วน เพื่อป้องกันการโจรกรรมข้อมูลส่วนตัวหรือการละเมิดความเป็นส่วนตัว

(1) ระบุประเภทของข้อมูลที่ต้องถูกซ่อน บดบังหรือแปลงข้อมูล

(2) กำหนดวิธีการซ่อน บดบังหรือแปลงข้อมูล / เครื่องมือที่ใช้ซ่อน บดบังหรือแปลงข้อมูล

(3) กำหนดรอบในการทดสอบว่าข้อมูลที่ถูกซ่อน บดบังหรือแปลงข้อมูลนั้น สามารถกลับคืนค่าต้นฉบับได้หรือไม่

(4) กำหนดกระบวนการหรือช่องทางการร้องขอข้อมูลที่ละเอียดอ่อน และวัตถุประสงค์การนำไปใช้ต้องชัดเจน และได้รับการอนุมัติจากผู้ดูแลข้อมูลนั้น อาจจะให้ข้อมูลเท่าที่จำเป็น

8.12 การป้องกันข้อมูลรั่วไหล (Data leakage prevention)

มาตรการป้องกันข้อมูลรั่วไหล ต้องนำมาใช้สำหรับ ระบบ เครือข่าย และอุปกรณ์ ที่ใช้ประมวลผล จัดเก็บ หรือมีการส่งข้อมูลที่ละเอียดอ่อน

(1) ระบุประเภทของข้อมูลที่เข้าข่ายมาตรการป้องกันข้อมูลรั่วไหล

(2) กำหนดวิธีการป้องกัน / เครื่องมือที่ใช้ป้องกันข้อมูลรั่วไหล พร้อมทั้งวิธีการแจ้งเตือนว่ามีข้อมูลรั่วไหลไปภายนอก

(3) หากจำเป็น อาจกำหนดการสุ่มตรวจสอบการรั่วไหลของข้อมูลเท่าที่สามารถทำได้

8.13 การสำรองข้อมูล (Information backup)

การสำรองข้อมูลสารสนเทศ, ซอฟแวร์และระบบ ต้องได้รับการบำรุงรักษาและทดสอบอย่างสม่ำเสมอ โดยดำเนินการดังนี้

(1) กำหนดประเภทของข้อมูลที่ต้องสำรอง

(2) กำหนดความถี่ในการสำรองข้อมูล และควรมีช่วงเวลาแนะนำในการเก็บรักษาข้อมูลที่เป็นไปตามข้อกำหนดทางธุรกิจ

(3) กำหนดสถานที่จัดเก็บข้อมูลสำรองและขั้นตอนในการสำรองข้อมูลที่จะนำมาใช้งาน

(4) กำหนดมาตรการรักษาความปลอดภัยสำหรับข้อมูลสำรอง เช่น ข้อมูลด้านสุขภาพ ต้องมีการเข้ารหัสข้อมูล การควบคุมการเข้าถึง

(5) ข้อมูลที่เก็บบนระบบสารสนเทศและข้อมูลที่เก็บบนสื่อบันทึกสำรองต้องเป็นไปตาม หรือมากกว่าที่ระบุไว้ในช่วงเวลาการเก็บรักษาข้อมูล

(6) กลยุทธ์การสำรองข้อมูลต้องเป็นไปตามความพร้อมใช้งาน และข้อกำหนดด้านความต่อเนื่องทางธุรกิจในส่วนของความเร็วในการกู้คืน และจำนวนข้อมูลที่ยอมให้สูญเสียได้มากที่สุด หากเกิดเหตุการณ์วิกฤติ ((RPO: Recovery Point Objective)

(7) ทดสอบการสำรองข้อมูล เพื่อให้แน่ใจว่าสามารถกู้คืนข้อมูลได้สำเร็จ

8.14 ระบบทดแทน (Redundancy of information processing facilities)

สิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศ ต้องดำเนินการสำรองไว้อย่างเพียงพอ เพื่อให้เป็นไปตามข้อกำหนดด้านความพร้อมใช้งาน

(1) สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ

- ต้องปฏิบัติตามกฎหมาย ข้อบังคับ และข้อผูกพันตามสัญญากับลูกค้า
- มีระดับการวิเคราะห์ผลกระทบทางธุรกิจสูง
- ระบบที่พึ่งพาระบบอื่นที่มีระดับการวิเคราะห์ผลกระทบทางธุรกิจสูง

(2) ตามข้อจำกัดทางภูมิศาสตร์ ความต้องการทางธุรกิจ และช่องโหว่ทางธุรกิจมีที่อยู่ การทำงานชุดสำรองควรพิจารณาถึงสิ่งเหล่านี้

- ความพร้อมในการบริหารจัดการพลังงาน
- ความพร้อมในการเชื่อมโยงเครือข่ายสู่สภาพแวดล้อมภายนอก
- ความพร้อมในการเชื่อมโยงเครือข่ายภายใน
- ความพร้อมในการเปิดระบบ
- ความพร้อมในการเก็บรักษาอุปกรณ์

8.15 บันทึกกิจกรรม (Logging)

ล็อกที่บันทึกกิจกรรม ข้อยกเว้น ข้อผิดพลาด และเหตุการณ์ที่เกี่ยวข้องอื่น ๆ จะต้องมีการจัดทำขึ้น จัดเก็บ ป้องกัน และวิเคราะห์

(1) การติดตามตรวจสอบการใช้งานของผู้ใช้งานระบบ

ฝ่ายเทคโนโลยีสารสนเทศ และเจ้าของระบบ กำหนดให้ผู้ดูแลระบบสารสนเทศและระบบเครือข่ายมีการตรวจสอบการใช้งานระบบอย่างสม่ำเสมอ โดยกำหนดให้ใช้เกณฑ์ในการติดตาม ดังนี้

- ความพยายามเข้าใช้งานที่ไม่สำเร็จ
- การแก้ไขการตั้งค่าโดยไม่ได้รับอนุญาต
- การเข้าถึงโดยไม่ได้รับอนุญาต
- ทรัพยากรที่มีการเข้าถึงโดยไม่ได้รับอนุญาต
- IP ที่ไม่รู้ที่มาหรือไม่ได้ลงทะเบียน
- การเข้าถึงในช่วงเวลาผิดปกติ
- เหตุผิดปกติหรือเหตุต้องสงสัยอื่น ๆ

หากพบว่ามีเหตุผิดปกติหรือเหตุต้องสงสัย ผู้ดูแลระบบจะต้องดำเนินการวิเคราะห์ ตรวจสอบ ดำเนินการแก้ไข รวมถึงรายงานไปยังผู้เกี่ยวข้องทันที

(2) การบันทึกข้อมูลผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

ในการตรวจสอบผู้ใช้งานระบบ จะต้องมีการเปิดบันทึกข้อมูลผู้ใช้งาน(logs) ซึ่งแบ่งออกเป็นระดับระบบปฏิบัติการและระดับแอปพลิเคชัน โดยจะต้องประกอบไปด้วยข้อมูลอย่างน้อยดังต่อไปนี้

- รหัสประจำตัวผู้ใช้
- วันที่และช่วงเวลาที่เข้าใช้งานและออกจากการใช้งาน
- เครื่องหรือตำแหน่งที่ใช้ในการเข้าใช้งาน หากสามารถระบุได้
- บันทึกการพยายามเข้าใช้งานระบบทั้งที่ประสบความสำเร็จและที่ถูกปฏิเสธ
- บันทึกการพยายามเข้าใช้งานแอปพลิเคชันทั้งที่ประสบความสำเร็จและที่ถูกปฏิเสธ หากสามารถทำได้
- บันทึกการพยายามเข้าใช้งานข้อมูลและทรัพยากรอื่น ๆ ทั้งที่ประสบความสำเร็จและที่ถูกปฏิเสธ
- การเปิดบันทึกจะต้องสามารถตรวจสอบกิจกรรมที่เกิดขึ้นจากผู้ใช้แต่ละคนได้ ซึ่งรวมไปถึงเจ้าหน้าที่ดูแลระบบที่มีหน้าที่ดูแลจัดการเครื่องแม่ข่าย
- ต้องมีการบันทึกการดำเนินการของผู้ดูแลระบบและผู้ใช้งาน
- ต้องมีการบันทึกการใช้งานผ่านสิทธิพิเศษของผู้ดูแลระบบ
- ต้องมีการบันทึก (logs) ผู้ใช้งานจัดทำโดยผู้ดูแลระบบ
- ควรมีการตั้งเวลาของระบบทั้งหมดให้ตรงกันเพื่อช่วยในการวิเคราะห์ลำดับการเกิดขึ้นของเหตุการณ์
- ต้องมีการป้องกันบันทึกข้อมูลการใช้งาน (logs) จากการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต และมีการจัดเก็บบันทึกการเข้าใช้งาน (logs) ไว้อย่างน้อย 90 วัน

8.16 การเฝ้าติดตามกิจกรรม (Monitoring activities)

เครือข่าย ระบบ และแอปพลิเคชัน ต้องได้รับการเฝ้าติดตามพฤติกรรมที่ผิดปกติและการดำเนินการที่ไม่เหมาะสม เพื่อประเมินเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่อาจเกิดขึ้น

(1) กำหนดประเภทของกิจกรรมที่ต้องถูกเฝ้าติดตาม เช่น การเข้าสู่ระบบ การเข้าถึงข้อมูล การเปลี่ยนแปลงการตั้งค่า การโอนย้ายข้อมูล กิจกรรมอื่น ๆ ที่อาจบ่งบอกถึงภัยคุกคามต่อความมั่นคงปลอดภัย

(2) ระบุเครื่องมือที่ใช้สำหรับการเฝ้าติดตามกิจกรรม เช่น SIEM, logs

(3) วิเคราะห์ข้อมูลการเฝ้าติดตามเพื่อระบุกิจกรรมที่น่าสงสัย และตอบสนองต่อเหตุการณ์ที่ตรวจพบจากการวิเคราะห์ข้อมูลการเฝ้าติดตาม พร้อมทั้งเก็บหลักฐานการดำเนินการ

8.17 การตั้งค่านาฬิกาให้ตรงกัน (Clock synchronization)

กำหนดให้ระบบประมวลผลเทคโนโลยีสารสนเทศ เครื่องคอมพิวเตอร์ และอุปกรณ์ที่สามารถตั้งเวลาได้มีการเชื่อมต่อสัญญาณนาฬิกาไปที่แหล่งตั้งเวลาที่เชื่อถือได้ เพื่อให้เวลาตรงกันและช่วยในการวิเคราะห์ลำดับการเกิดขึ้นของเหตุการณ์ เช่น เวลาของระบบเครือข่ายอินเทอร์เน็ต, เวลาของระบบ WIFI เป็นต้น

8.18 การใช้งานโปรแกรมยูทิลิตี้ที่ได้รับสิทธิพิเศษ (Use of privileged utility programs)

การใช้งานโปรแกรมยูทิลิตี้ ที่สามารถข้ามผ่านมาตรการควบคุมของระบบและแอปพลิเคชัน ต้องถูกจำกัดและควบคุมอย่างเคร่งครัด มีแนวปฏิบัติในการใช้งานอรรถประโยชน์ ดังนี้

(1) ห้ามติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ของบริษัท
(2) กำหนดให้มีการจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ โดยซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับต้องมีการลงทะเบียนเพื่อใช้งาน ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ และตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไม่
(3) รายชื่อโปรแกรมประเภทอรรถประโยชน์ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งาน ต้องได้รับการจัดทำเป็นเอกสาร และได้รับการอนุมัติโดยผู้บริหารของสายงานเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าซอฟต์แวร์เหล่านี้มีลิขสิทธิ์ถูกต้องครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ในการทำงานของบริษัทเท่านั้น
(4) ไม่อนุญาตให้ใช้งานโปรแกรมประเภทอรรถประโยชน์ที่ลัดขั้นตอนการพิสูจน์ตัวตน
(5) หากมีความจำเป็นต้องใช้งานโปรแกรมอรรถประโยชน์ที่ลัดขั้นตอนการพิสูจน์ตัวตน จำเป็นต้องมีการประเมินความเสี่ยงที่เกิดจากการใช้งานโปรแกรมอรรถประโยชน์ดังกล่าว มีการอนุมัติอย่างเป็นลายลักษณ์อักษร และเปิดใช้บันทึกเหตุการณ์เสมอ

8.19 การติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ (Installation of software on operational system)

ต้องดำเนินการตามขั้นตอนปฏิบัติและมาตรการ เพื่อจัดการการติดตั้งซอฟแวร์บนระบบปฏิบัติการอย่างมั่นคงปลอดภัย กำหนดให้มีการควบคุมซอฟต์แวร์ที่อนุญาตให้ติดตั้งในเครื่องคอมพิวเตอร์และอุปกรณ์ ดังนี้

(1) ให้ติดตั้งเฉพาะซอฟต์แวร์ที่อยู่ในรายการที่ได้รับอนุญาตเท่านั้น
(2) การติดตั้งซอฟต์แวร์ดำเนินการโดยเจ้าหน้าที่ที่ได้รับการแต่งตั้งหรืออนุญาต
(3) มีการทบทวนรายการซอฟต์แวร์ เวอร์ชัน ที่ได้รับอนุญาตอย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้ง
(4) ไม่อนุญาตให้นำซอฟต์แวร์ที่ยังอยู่ในระหว่างการพัฒนาหรือการทดสอบมาใช้ ในสภาพแวดล้อมการดำเนินการจริง หรือหากมีความจำเป็นต้องใช้ ควรมีการประเมินความเสี่ยงและหามาตรการควบคุมที่เพียงพอ
(5) ไม่อนุญาตให้ใช้ระบบปฏิบัติการหรือซอฟต์แวร์ที่ผู้ผลิตยกเลิกการสนับสนุนการให้บริการ หรือหากมีความจำเป็นต้องใช้ ควรมีการประเมินความเสี่ยงและหามาตรการควบคุมที่เพียงพอ

8.20 ความมั่นคงปลอดภัยของเครือข่าย (Networks security)

เครือข่ายและอุปกรณ์เครือข่ายต้องได้รับการรักษาความมั่นคงปลอดภัย บริหารจัดการ และควบคุมเพื่อปกป้องข้อมูลในระบบและแอปพลิเคชัน ควรดำเนินการ ดังนี้

(1) ควรมีการป้องกันเครือข่ายจากการบุกรุกโดยไม่ได้รับอนุญาตผ่านทางการจัดรูปแบบของเครือข่าย (Topology) การเลือกเส้นทางของข้อมูล (Routing) ความสามารถในการเชื่อมต่อ (Connectivity) และการควบคุมการเข้าใช้งาน (Access Control)
(2) ควรจัดทำเอกสารแสดงผังการเชื่อมต่อของเครือข่าย (Network Diagram) และปรับปรุงให้ทันสมัยอยู่เสมอเมื่อมีการเปลี่ยนแปลงเครือข่าย

(3) อนุญาตให้เฉพาะเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่เกี่ยวข้องกับการดำเนินงานของบริษัทที่ได้รับอนุญาตเท่านั้นในการเชื่อมต่อกับระบบเครือข่าย

(4) เฝ้าระวังและจัดเก็บบันทึกการเข้าใช้งาน (logs) ที่เกิดขึ้นจากการใช้บริการเครือข่าย

8.21 ความมั่นคงปลอดภัยของบริการเครือข่าย (Security of network services)

(1) การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(2) ต้องมีการยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกบริษัท (User Authentication for External Connections) และต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกบริษัทสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของบริษัทได้

(3) บุคคลภายนอกสามารถเข้าถึงบริการในเครือข่ายบริการสาธารณะได้แต่ไม่มีสิทธิเข้าถึงทรัพยากรภายในของบริษัท

(4) ไม่อนุญาตให้บุคคลภายนอกเชื่อมต่อกับเครือข่ายสำนักงานโดยไม่ได้รับอนุญาตอย่างเป็นทางการจากเจ้าของระบบ ในกรณีที่การเชื่อมต่อได้รับการอนุมัติ ควรตรวจสอบกิจกรรมบนเครือข่ายของบุคคลภายนอก

(5) ต้องใช้เฉพาะอุปกรณ์ต่อพ่วงไร้สายที่ได้รับการอนุญาตให้ติดตั้งภายในสำนักงาน รวมถึงห้องเซิร์ฟเวอร์และห้องอุปกรณ์

8.22 การแบ่งแยกเครือข่าย (Segregation of network)

ต้องมีการจัดแบ่งแยกกลุ่มเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศออกจากเครือข่ายขององค์กร

8.23 การกรองเว็บ (Web filtering)

การป้องกันการเข้าถึงเว็บไซต์ภายนอก ที่เนื้อหาไม่เหมาะสม ต้องได้รับการจัดการ เพื่อลดปัจจัยเสี่ยงในการเข้าถึงเนื้อหาที่เป็นอันตราย การป้องกันมัลแวร์ หรือการเพิ่มประสิทธิภาพการทำงาน

(1) ระบุประเภทของเว็บไซต์ที่ควรบล็อก และดำเนินการบล็อกเว็บไซต์

(2) กำหนดกระบวนการสำหรับการตรวจสอบและรายงานกิจกรรมการกรองเว็บไซต์

8.24 การเข้ารหัสข้อมูล (Use of cryptography)

(1) การควบคุมการเข้ารหัส

กำหนดให้มีการใช้เทคโนโลยีเข้ารหัสในระบบเทคโนโลยีสารสนเทศ และข้อมูลที่มีความสำคัญสูงโดยเลือกใช้เทคโนโลยีการเข้ารหัส หรืออัลกอริทึมที่ออกแบบเพื่อตอบสนองความต้องการด้านความมั่นคงปลอดภัยและสอดคล้องกับผลการประเมินความเสี่ยง โดยมีแนวปฏิบัติ ดังนี้

- ห้ามไม่ให้มีการติดตั้งซอฟต์แวร์เข้ารหัสที่ไม่ได้รับอนุญาต
- การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล และเป็นการเข้ารหัส (Encryption) ที่ยังไม่มีการประกาศช่องโหว่ออกสู่สาธารณะ

- การเข้ารหัสไม่ควรต่ำกว่า 256 บิต
- เจ้าของข้อมูลที่เป็นความลับให้นำการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากลมาใช้

(2) การบริหารจัดการกุญแจเข้ารหัสข้อมูล

กำหนดให้มีการควบคุมให้มีการใช้กุญแจเข้ารหัสข้อมูล ดังนี้

- มีการใช้กุญแจเข้ารหัสเพื่อสนับสนุนการทำงานของเทคโนโลยีเข้ารหัส
- มีการเปลี่ยนกุญแจเข้ารหัส และทำลายรหัสเก่าเมื่อมีเหตุต้องสงสัยว่ามีบุคคลที่ไม่ได้รับอนุญาตรู้รหัสดังกล่าว

8.25 วงจรการพัฒนาอย่างมั่นคงปลอดภัย (Secure development life cycle)

แนวทางการพัฒนาระบบให้มีความมั่นคงปลอดภัย

(1) นักพัฒนาระบบจำเป็นต้องศึกษาวงจรการพัฒนาระบบ และ เทคนิคในการเขียนระบบให้มีความปลอดภัยให้ดี

(2) ต้องนำหลักการของวงจรการพัฒนาระบบมาใช้ กำหนดหลักเกณฑ์สำหรับการพัฒนาซอฟต์แวร์และระบบอย่างมั่นคงปลอดภัย เพื่อทำให้มั่นใจได้ถึงคุณภาพของซอฟต์แวร์ในการพัฒนาระบบ

(3) การบริหารโครงการด้านเทคโนโลยีสารสนเทศ ต้องคำนึงถึงข้อกำหนดด้านความมั่นคงปลอดภัยในการพิจารณาและดำเนินกิจกรรมในโครงการในแต่ละช่วงของการบริหารโครงการเสมอ

8.26 ข้อกำหนดด้านความมั่นคงปลอดภัยของแอปพลิเคชั่น (Application security requirement)

แนวทางด้านความมั่นคงปลอดภัยของแอปพลิเคชั่น

(1) มีขั้นตอนการออกแบบ การพัฒนา การทดสอบ และการปรับใช้แอปพลิเคชันอย่างปลอดภัยทั้งที่มีการพัฒนาใช้งานเอง และ/หรือจัดจ้างให้หน่วยงานภายนอกพัฒนา โดยต้องผ่านการอนุมัติก่อนการนำมาใช้งาน

(2) มีการตรวจสอบชุดคำสั่งและการทดสอบหาช่องโหว่ด้านความมั่นคงปลอดภัย และจัดการช่องโหว่ที่พบ

(3) มีกระบวนการสำหรับการติดตั้ง การอัปเดตซอฟต์แวร์และแพตช์ความมั่นคงปลอดภัยสำหรับแอปพลิเคชัน

8.27 สถาปัตยกรรมระบบและหลักการทางวิศวกรรมที่มั่นคงปลอดภัย (Secure system architecture and engineering principles)

(1) หลักการด้านความมั่นคงปลอดภัยทางวิศวกรรมระบบ ต้องจัดทำ ทำเป็นเอกสาร บำรุงรักษา และนำไปประยุกต์ใช้กับทุกกิจกรรมของการพัฒนาระบบสารสนเทศ

(2) ในการออกแบบ พัฒนา ควรอ้างอิงมาตรฐานสากลที่ให้คำแนะนำเกี่ยวกับสถาปัตยกรรมระบบและหลักการทางวิศวกรรมที่มั่นคงปลอดภัย

8.28 การเขียนชุดคำสั่งอย่างมั่นคงปลอดภัย (Secure coding)

แนวทางการเขียนชุดคำสั่งอย่างมั่นคงปลอดภัย

(1) ต้องกำหนดมาตรฐานการเขียนชุดคำสั่งที่ต้องปฏิบัติตาม

(2) ตรวจสอบชุดคำสั่งเพื่อหาช่องโหว่ด้านความปลอดภัย และจัดการช่องโหว่ที่พบ

(3) ฝึกอบรมนักพัฒนาระบบเกี่ยวกับหลักการเขียนชุดคำสั่งอย่างมั่นคงปลอดภัย

8.29 การทดสอบความมั่นคงปลอดภัยในการพัฒนาและการยอมรับ (Security testing in development and acceptance)

การทดสอบความมั่นคงปลอดภัย ต้องได้รับการกำหนดและประยุกต์ใช้

(1) จะต้องมีเกณฑ์ในการตรวจรับระบบทุกระบบที่มีการพัฒนาขึ้นมาใหม่หรือมีการปรับปรุงประสิทธิภาพเพิ่มเติม โดยเกณฑ์ที่ใช้ในการตรวจรับจะต้องเป็นเกณฑ์ที่กำหนดอย่างชัดเจน ผ่านการอนุมัติ มีการจัดทำเป็นเอกสาร และผ่านการทดสอบการใช้งานมาแล้ว

(2) การทดสอบเพื่อตรวจรับระบบจะต้องไม่ทำโดยทีมที่เป็นผู้พัฒนาระบบนั้นเอง

8.30 การพัฒนาโดยหน่วยงานภายนอก (Outsourced development)

แนวทางการพัฒนาระบบโดยหน่วยงานภายนอก

(1) ซอฟต์แวร์ที่พัฒนาโดยหน่วยงานภายนอกต้องเป็นไปตามรายละเอียดข้อกำหนดผู้ใช้ และมีการสนับสนุนด้านสินค้าอย่างเหมาะสม

(2) ต้องมั่นใจว่ามีการปรึกษาและทำการตกลงร่วมกันระหว่างบริษัทและหน่วยงานภายนอกในเรื่องการสนับสนุนจากหน่วยงานภายนอก และการปฏิบัติตามกฎหมายอย่างต่อเนื่อง การจัดการใบอนุญาตกรรมสิทธิ์ของโปรแกรม และทรัพย์สินทางปัญญา

(3) ข้อตกลงกับผู้ให้บริการภายนอก (Outsource/Supplier) ต้องครอบคลุมถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยอย่างละเอียด โดยมีการลงนามสัญญารักษาความลับ (NDA), ข้อตกลงประมวลผลหรือแบ่งปันข้อมูล (DPA/DSA) และสามารถตรวจสอบ/ประเมินผลการให้บริการเป็นประจำ

(4) การทดสอบด้านความมั่นคงปลอดภัยของระบบ ต้องมีการดำเนินการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบในระหว่างที่ระบบอยู่ในช่วงการพัฒนา

8.31 การแบ่งแยกสภาพแวดล้อมของการพัฒนา การทดสอบ และการทำงานจริงออกจากกัน (Separation of development, test and production environments)

(1) ควรแยกซอฟต์แวร์ในการปฏิบัติงาน การพัฒนา และการทดสอบให้อยู่ในโดเมนหรือไดเรกทอรี่ที่ต่างกันออกไป

(2) สภาพแวดล้อมในการปฏิบัติ การทดลอง และการพัฒนาต้องถูกแยกด้านตรรกะออกจากกัน และสภาพแวดล้อมของผู้ใช้ควรทำการดูแลแบบแยกส่วนกัน

(3) กำหนดมาตรการควบคุมด้านความมั่นคงปลอดภัยที่เหมาะสมอย่างต่อเนื่อง เพื่อรักษาความมั่นคงปลอดภัย ทั้งการพัฒนา ทดสอบ และการทำงานจริงของซอฟต์แวร์

8.32 การบริหารการจัดการการเปลี่ยนแปลง (Change management)

การเปลี่ยนแปลงใด ๆ ของระบบ/ขั้นตอนการปฏิบัติงานต้องสอดคล้องกับกระบวนการบริหารการเปลี่ยนแปลงในการปฏิบัติงาน และมีแนวปฏิบัติที่สำคัญ ดังนี้

(1) ต้องการขออนุมัติการเปลี่ยนแปลงก่อนดำเนินการทุกครั้ง

(2) หลีกเลี่ยงการดำเนินงานในช่วงเวลาที่มีการใช้งานเป็นจำนวนมาก เพื่อหลีกเลี่ยงผลกระทบที่อาจเกิดขึ้นกับผู้ใช้งาน

(3) ประเมินผลกระทบจากการเปลี่ยนแปลงและกำหนดแผนสำรองเพื่อใช้กู้คืน หากการดำเนินงานไม่สัมฤทธิ์ผล

8.33 ข้อมูลในการทดสอบ (Test information)

การป้องกันข้อมูลที่ใช้ในการทดสอบ กำหนดให้ควบคุมข้อมูลที่ใช้ในการทดสอบตามแนวปฏิบัติ ดังนี้

(1) ไม่ควรใช้ข้อมูลจริงในการทดสอบ โดยเฉพาะส่วนที่เป็นข้อมูลส่วนบุคคล ในกรณีที่มีความจำเป็นต้องใช้ ให้ทำการสับเปลี่ยนข้อมูลเพื่อไม่ให้สามารถย้อนกลับไปยังข้อมูลต้นฉบับได้

(2) เมื่อมีความจำเป็นต้องคัดลอกข้อมูลที่ใช้ในการปฏิบัติงานจริงเพื่อทำการทดสอบ กำหนดให้มีบันทึกเพื่อระบุวัตถุประสงค์ และผู้ดำเนินการคัดลอกอย่างเป็นลายลักษณ์อักษร

(3) เมื่อใช้ข้อมูลทดสอบเสร็จสิ้นแล้วให้ลบข้อมูลออกจากระบบทดสอบทันที

8.34 การปกป้องระบบสารสนเทศระหว่างการทดสอบในการตรวจประเมิน (Protection of information systems during audit testing)

การทดสอบในการตรวจประเมินและกิจกรรมการรับประกันอื่น ๆ ที่เกี่ยวข้องกับการตรวจประเมินระบบปฏิบัติการต้องมีการวางแผนและตกลงร่วมกันระหว่างผู้ทดสอบและผู้บริหารอย่างเหมาะสม

(1) ต้องได้รับการอนุญาตก่อนนำสำเนาข้อมูลปฏิบัติการไปใช้ในการทดสอบระบบทุกครั้ง

(2) ต้องมีการเปลี่ยนแปลงข้อมูลบางส่วนสำหรับข้อมูลที่นำไปทดสอบ ไม่ให้เหมือนข้อมูลต้นทาง เพื่อป้องกันข้อมูลรั่วไหลและถูกนำไปใช้โดยไม่ได้รับอนุญาต

(3) ต้องดำเนินการให้สิทธิขั้นต่ำ (Least Privilege) หมายถึง จำกัดผู้ใช้ที่ทำงาน ข้อมูลและระบบข้อมูลเฉพาะที่จำเป็นในการทำงานเท่านั้น