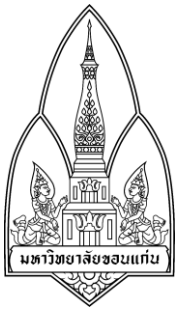

ประกาศสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น

ฉบับที่ 5 / 2568

เรื่อง นโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

(Information Security Policy and Guidelines)

.....

สำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น ได้เล็งเห็นว่าระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2022 เป็นมาตรฐานที่ได้รับการยอมรับอย่างแพร่หลายในระดับสากลและเหมาะสมต่อการนำมาประยุกต์ใช้ภายในหน่วยงาน จึงได้ดำเนินการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐานสากล ISO/IEC 27001:2022 ขึ้นอย่างเป็นทางการ

จากการพิจารณาการศึกษาบริบทของสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น พบว่ามีความต้องการและความมุ่งมั่นในการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างเป็นระบบ เพื่อเสริมสร้างความเชื่อมั่นแก่ผู้ใช้งานระบบสารสนเทศของมหาวิทยาลัยขอนแก่น ให้มีความมั่นคงปลอดภัย การดำเนินงานดังกล่าวยังมีเป้าหมายเพื่อให้สอดคล้องกับวิสัยทัศน์และพันธกิจของสำนักฯ รวมถึงเป็นไปตามข้อกำหนด ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องอย่างเคร่งครัด โดยสำนักฯ ได้นำมาตรฐาน ISO/IEC 27001:2022 มาใช้เป็นกรอบสำคัญในการกำหนดแนวทางและพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้มีประสิทธิภาพและยั่งยืน

อาศัยอำนาจตามความในมาตรา 40 แห่งพระราชบัญญัติมหาวิทยาลัยขอนแก่น พ.ศ. 2558 สำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น จึงออกประกาศนโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ดังนี้

ข้อ 1 ประกาศนี้เรียกว่า “ประกาศสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น เรื่อง นโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ”

ข้อ 2 ให้ประกาศมีผลบังคับใช้ถัดจากวันประกาศเป็นต้นไป

ข้อ 3 แต่งตั้งคณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อให้มีการขับเคลื่อนนโยบาย และรักษาระบบบริหารงานเทคโนโลยีสารสนเทศอย่างต่อเนื่อง

ข้อ 4 นโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศได้กำหนดขึ้น โดยมีวัตถุประสงค์ดังต่อไปนี้

1) เพื่อพัฒนากระบวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างเป็นระบบและมีการพัฒนาปรับปรุงอย่างต่อเนื่อง
2) เพื่อให้การให้บริการตามขอบเขตของการบริหารจัดการระบบเทคโนโลยีสารสนเทศที่สนับสนุนการดำเนินงานที่เกี่ยวข้องมีความพร้อมใช้ (Availability) มีการรักษาความลับ (Confidentiality) และความถูกต้องของข้อมูล (Integrity) ที่ให้บริการแก่ผู้ใช้งานระบบสารสนเทศ
3) เพื่อให้ผู้ปฏิบัติงานขององค์กรมีการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ นโยบายและขั้นตอนปฏิบัติที่เกี่ยวข้อง
4) เพื่อให้ผู้ปฏิบัติงานที่เกี่ยวข้องตามขอบเขตได้รับความรู้เกี่ยวกับการพัฒนาการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ข้อ 5 นโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย

<u>มาตรการควบคุมด้านองค์กร (Organizational controls)</u>

1) นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information security policy)
2) โครงสร้างความมั่นคงปลอดภัยสารสนเทศขององค์กร (Organization of information security)
3) ข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม (Threat intelligence)
4) การบริหารจัดการทรัพย์สินสารสนเทศ (Asset management)
5) การถ่ายโอนข้อมูล (Information transfer)
6) การควบคุมการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ (Access control)
7) ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)
8) การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information security incident management)

/9) การบริหาร. . .

9) การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ
(Information security aspects of business continuity management)

10) การปฏิบัติตามข้อกำหนด
(Compliance)

มาตรการควบคุมด้านบุคลากร (People controls)

1) ความมั่นคงปลอดภัยสารสนเทศสำหรับทรัพยากรบุคคล
(Human resource security)

2) การปฏิบัติงานจากระยะไกล
(Remote working)

มาตรการควบคุมด้านกายภาพ (Physical controls)

1) ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม
(Physical and environmental security)

2) สื่อบันทึกข้อมูล
(Storage media)

มาตรการควบคุมด้านเทคโนโลยี (Technological controls)

1) อุปกรณ์ระดับผู้ใช้งาน
(User endpoint devices)

2) สิทธิพิเศษในการเข้าถึงและการจำกัดการเข้าถึงข้อมูล
(Privileged access rights)

3) การพิสูจน์ตัวตนอย่างมั่นคงปลอดภัย
(Secure authentication)

4) ความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ
(Operations security)

5) การจัดการการตั้งค่าระบบ
(Configuration management)

6) การบริหารจัดการข้อมูล
(Data management)

/7) การบันทึก. . .

7) การบันทึกกิจกรรมและการเฝ้าติดตามกิจกรรม
(Logging and monitoring activities)
8) ความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร
(Communications security)
9) การควบคุมการเข้ารหัสข้อมูล
(Cryptographic control)
10) การจัดหา พัฒนา และบำรุงรักษาระบบคอมพิวเตอร์
(System acquisition, development and maintenance)

จึงประกาศให้ทราบโดยทั่วไป

ประกาศ ณ วันที่ 27 สิงหาคม พ.ศ. 2568

(ผู้ช่วยศาสตราจารย์พิพัธน์ เรืองแสง)
ผู้อำนวยการสำนักเทคโนโลยีดิจิทัล

เอกสารแนบท้ายประกาศ

นโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

สำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น

พ.ศ. 2568

สารบัญ

หน้า

1. บทนำ 1

2. วัตถุประสงค์ 1

3. ขอบเขต 1

4. คำย่อ และคำนิยาม 2

5. หน้าที่และความรับผิดชอบ 4

6. หลักการการรักษาความมั่นคงปลอดภัยสารสนเทศ 5

7. การตรวจสอบและการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ 6

8. การบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ 6

9. การจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ 6

9.1 มาตรการควบคุมด้านองค์กร (Organizational controls) 6

9.1.1 นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information security policy) 6

9.1.2 โครงสร้างความมั่นคงปลอดภัยสารสนเทศขององค์กร (Organization of information security) 8

9.1.3 ข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม (Threat intelligence) 10

9.1.4 การบริหารจัดการทรัพย์สินสารสนเทศ (Asset management) 11

9.1.5 การถ่ายโอนข้อมูล (Information transfer) 12

9.1.6 การควบคุมการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ (Access control) 14

9.1.7 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships) 18

9.1.8 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information security incident management) 27

9.1.9 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information security aspects of business continuity management) 28

9.1.10 การปฏิบัติตามข้อกำหนด (Compliance) 29

9.2 มาตรการควบคุมด้านบุคลากร (People controls) 30

9.2.1 ความมั่นคงปลอดภัยสารสนเทศสำหรับทรัพยากรบุคคล (Human resource security) 30

9.2.2 การปฏิบัติงานจากระยะไกล (Remote working) 31

9.3 มาตรการควบคุมด้านกายภาพ (Physical controls) 33

9.3.1 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security) 33
9.3.2 สื่อบันทึกข้อมูล (Storage media) 37
9.4 มาตรการควบคุมด้านเทคโนโลยี (Technological controls) 38
9.4.1 อุปกรณ์ระดับผู้ใช้งาน (User endpoint devices) 38
9.4.2 สิทธิพิเศษในการเข้าถึงและการจำกัดการเข้าถึงข้อมูล (Privileged access rights) 42
9.4.3 การพิสูจน์ตัวตนอย่างมั่นคงปลอดภัย (Secure authentication) 43
9.4.4 ความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (Operations security) 44
9.4.5 การจัดการการตั้งค่าระบบ (Configuration management) 49
9.4.6 การบริหารจัดการข้อมูล (Data management) 50
9.4.7 การบันทึกกิจกรรมและการเฝ้าติดตามกิจกรรม (Logging and monitoring activities) 52
9.4.8 ความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications security) 53
9.4.9 การควบคุมการเข้ารหัสข้อมูล (Cryptographic control) 55
9.4.10 การจัดหา พัฒนา และบำรุงรักษาระบบคอมพิวเตอร์ (System acquisition, development and maintenance) 56
10. การพัฒนาบุคลากรและการเสริมสร้างความตระหนัก ความรู้ และความเข้าใจ 59
11. บทลงโทษ 59
12. การทบทวน 59

1. บทนำ

เนื่องด้วยสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น (“องค์กร”) มีการติดตั้ง ใช้งาน บำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบเทคโนโลยีสารสนเทศ และระบบอิเล็กทรอนิกส์อื่นใดที่เกี่ยวข้อง ซึ่งใช้ในการดำเนินงานและการให้บริการที่สำคัญขององค์กร ดังนั้น เพื่อให้การดำเนินการบริหารจัดการงานด้านเทคโนโลยีสารสนเทศขององค์กรมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล รวมถึงข้อมูลและทรัพย์สินสารสนเทศขององค์กรได้รับการรักษาความลับ ความถูกต้องครบถ้วนสมบูรณ์ และความพร้อมใช้ต่อการดำเนินงานอย่างเหมาะสม และสอดคล้องกับข้อบังคับ กฎระเบียบ กฎหมายด้านความมั่นคงปลอดภัยสารสนเทศ องค์กรจึงเห็นควรให้กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นกรอบในการบริหารจัดการการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศดังกล่าวข้างต้น

2. วัตถุประสงค์

การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศฉบับนี้ จัดทำขึ้นโดยมีวัตถุประสงค์หลักดังต่อไปนี้

2.1 เพื่อกำกับดูแลการบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กรให้มีประสิทธิผล และเป็นไปโดยถูกต้องตามกฎหมาย

2.2 เพื่อสร้างมาตรการและกลไกที่เหมาะสม เพื่อพัฒนาศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ ที่อาจสร้างความเสียหายต่อการดำเนินงานขององค์กร

2.3 เพื่อให้บุคลากร และ/หรือผู้ปฏิบัติงานทั้งหมดขององค์กร ได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และได้รับทราบถึงหน้าที่ความรับผิดชอบและแนวทางปฏิบัติในการควบคุมความเสี่ยงต่าง ๆ ทางด้านเทคโนโลยีสารสนเทศ

3. ขอบเขต

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศที่ได้กำหนดในเอกสารฉบับนี้บังคับใช้ภายในขอบเขตการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามที่ระบุในเอกสารการวิเคราะห์บริบทขององค์กร ขอบเขต และวัตถุประสงค์ความมั่นคงปลอดภัยสารสนเทศ (Context of the Organization, scope and objectives of information security)

4. คำย่อ และคำนิยาม

องค์กร	หมายถึง สำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น
บุคลากร	หมายถึง ผู้ปฏิบัติงานในมหาวิทยาลัย ได้แก่ พนักงานมหาวิทยาลัย ข้าราชการ ลูกจ้างของส่วนราชการ พนักงานราชการ และลูกจ้างของมหาวิทยาลัยที่เกี่ยวข้องกับการให้บริการภายใต้ขอบเขตการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของสำนักเทคโนโลยีดิจิทัล
บุคลากรภายนอก	หมายถึง หน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิเข้าถึง และใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ขององค์กร ตามอำนาจหน้าที่ที่รับผิดชอบ
ผู้ให้บริการภายนอก	หมายถึง ผู้ให้บริการจากภายนอกซึ่งเป็นคู่สัญญากับองค์กร ได้แก่ กลุ่มผู้ให้บริการด้านฮาร์ดแวร์ ซอฟต์แวร์ ระบบ Cloud ระบบสาธารณูปโภค และบุคคลที่ปฏิบัติหน้าที่ตามสัญญาจ้างขององค์กร ที่เกี่ยวข้องกับการให้บริการภายใต้ขอบเขตการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
ทรัพย์สินสารสนเทศ	หมายถึง อุปกรณ์ ระบบงาน หรือสภาพแวดล้อมที่จำเป็นหรือมีส่วนช่วยให้การประมวลผลข้อมูลเป็นไปอย่างครบถ้วน ถูกต้อง และมีประสิทธิภาพ ซึ่งสามารถแบ่งออกได้เป็น 3 ประเภทหลัก ๆ ดังนี้ (1) ทรัพย์สินสารสนเทศประเภทระบบ ซึ่งได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบงาน (2) ทรัพย์สินสารสนเทศประเภทอุปกรณ์ ซึ่งได้แก่ เครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วงคอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด (3) ทรัพย์สินสารสนเทศประเภทข้อมูล ซึ่งได้แก่ ข้อมูลคอมพิวเตอร์ ข้อมูลอิเล็กทรอนิกส์
ระบบคอมพิวเตอร์	หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
ระบบเทคโนโลยีสารสนเทศ	หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้

	ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น
ระบบเครือข่ายคอมพิวเตอร์	หมายถึง ระบบการเชื่อมโยงระหว่างคอมพิวเตอร์ตั้งแต่สองเครื่องขึ้นไป โดยใช้สื่อกลางและสามารถสื่อสารแลกเปลี่ยนข้อมูลกันทางอิเล็กทรอนิกส์ได้อย่างมีประสิทธิภาพ และสามารถใช้ทรัพยากรที่อยู่ในเครือข่ายร่วมกันได้
การรักษาความมั่นคงปลอดภัย	หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้น เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกองค์กร อันกระทบต่อความมั่นคงขององค์กร
ไซเบอร์	หมายถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้ เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือเครือข่ายโทรคมนาคม รวมทั้งการให้บริการของระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป
ภัยคุกคามทางไซเบอร์	หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

5. หน้าที่และความรับผิดชอบ

5.1 คณะกรรมการบริหารความเสี่ยงและการควบคุมภายใน สำนักเทคโนโลยีดิจิทัล

- กำหนดกลยุทธ์และควบคุมการปฏิบัติงานในองค์กร และอนุมัตินโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร
- กำกับดูแลให้ทุกหน่วยงานถือปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กรโดยเคร่งครัด เพื่อลดความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นต่อระบบคอมพิวเตอร์ ระบบเทคโนโลยีสารสนเทศขององค์กร

5.2 รองผู้อำนวยการฝ่ายโครงสร้างพื้นฐานทางสารสนเทศ และรองผู้อำนวยการฝ่ายบริหาร สำนักงานเทคโนโลยีดิจิทัล

- กำหนดเป้าหมาย นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร วางแผนยุทธศาสตร์ วิเคราะห์ความเสี่ยงที่อาจทำให้ระบบเกิดปัญหา ศึกษาเทคนิคใหม่ ๆ ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ และกำหนดแนวทางการเฝ้าระวังภัยที่อาจเกิดขึ้นกับระบบ นำเสนอผู้บริหารระดับสูง

5.3 ผู้อำนวยการกองบริหารงาน สำนักเทคโนโลยีดิจิทัล / หัวหน้างานอำนวยการ / หัวหน้างานโครงสร้างพื้นฐานดิจิทัล / หัวหน้างานวิจัยและพัฒนาระบบดิจิทัล และเจ้าหน้าที่แต่ละหน่วยงาน

- ปฏิบัติงานเพื่อรักษาความมั่นคงปลอดภัยและสมบูรณ์ของระบบ โดยมีหน้าที่บริหารจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน บังคับใช้นโยบายการให้สิทธิ์เท่าที่จำเป็น (Least Privilege) และรักษาค่าการตั้งค่าระบบให้ปลอดภัย รวมถึงทำหน้าที่ในการติดตั้งแพตช์ความปลอดภัย สำรองข้อมูล และเฝ้าระวังพฤติกรรมที่น่าสงสัย ในกรณีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัย ให้ทำหน้าที่เป็นผู้รับมือเบื้องต้นโดยการแยกระบบที่ได้รับผลกระทบ และรายงานหรือส่งต่อเหตุการณ์ตามความเหมาะสม

5.4 บุคลากร / ผู้ใช้งาน

- ทำความเข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กรโดยเคร่งครัด
- แจ้งให้สำนักเทคโนโลยีดิจิทัลทราบทันที เมื่อพบเห็นการปฏิบัติที่ไม่ถูกต้องหรือไม่เหมาะสม หรือพบเห็นภัยคุกคามทางไซเบอร์ที่อาจสร้างความเสียหายต่อองค์กร
- บุคลากรที่มีหน้าที่เกี่ยวข้องกับบุคคลภายนอก ต้องจัดให้มีการควบคุมดูแลบุคคลภายนอกให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร

6. หลักการการรักษาความมั่นคงปลอดภัยสารสนเทศ

การรักษาความมั่นคงปลอดภัยสารสนเทศมีหลักการที่สำคัญดังต่อไปนี้

- **การรักษาความลับ (Confidentiality)** การรักษาข้อมูล รวมถึงข้อมูลส่วนบุคคลหรือข้อมูลอื่นใดให้มีความลับ เข้าถึงได้เฉพาะผู้มีสิทธิ มีการป้องกันการเข้าถึง และการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต
- **การรักษาความถูกต้องสมบูรณ์ (Integrity)** การทำให้มั่นใจว่าข้อมูลมีความถูกต้องสมบูรณ์และเชื่อถือได้ รวมถึงการปกป้องข้อมูลให้ปราศจากการแก้ไข ดัดแปลง หรือถูกทำลายโดยผู้ที่ไม่ได้รับอนุญาต
- **การรักษาสภาพความพร้อมใช้งาน (Availability)** การทำให้มั่นใจว่าระบบคอมพิวเตอร์ ระบบเทคโนโลยีสารสนเทศ และข้อมูลต่าง ๆ สามารถใช้งานได้อย่างต่อเนื่องและพร้อมสำหรับการใช้งานเสมอ รวมถึงมีการสำรองข้อมูลไว้เพื่อให้มั่นใจว่าไม่ถูกขัดขวางการทำงานทั้งจากความตั้งใจหรือจากภัยพิบัติต่าง ๆ

7. การตรวจสอบและการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

องค์กรต้องจัดให้มีกระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยให้ครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในเกณฑ์ที่องค์กรยอมรับได้ รวมถึงจัดให้มีผู้รับผิดชอบในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม

8. การบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ

องค์กรต้องจัดให้มีกระบวนการในการบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแผนยุทธศาสตร์ขององค์กรที่เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ รวมถึงจัดให้มีการจัดการความเสี่ยงสำคัญในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ

9. การจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ

องค์กรต้องจัดให้มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ ที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศที่ได้ประกาศใช้งาน และดำเนินการประกาศแนวปฏิบัติดังกล่าวให้ผู้เกี่ยวข้องรับทราบ โดยแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ ต้องครอบคลุม 4 หัวข้อหลัก ได้แก่

9.1 มาตรการควบคุมด้านองค์กร (Organizational controls)

9.1.1 นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information security policy)

<u>วัตถุประสงค์</u>

เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และได้รับทราบถึงหน้าที่ความรับผิดชอบและแนวทางปฏิบัติในการควบคุมความเสี่ยงต่าง ๆ โดยองค์กรต้องกำหนดให้มีการจัดทำ ทบทวน ตรวจสอบ ประเมินผล แนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ รวมถึงต้องสั่งการให้เกิดการปฏิบัติตามระเบียบและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศที่ได้กำหนด

<u>แนวปฏิบัติ</u>

1) องค์กรต้องจัดให้มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเป็นลายลักษณ์อักษร โดยได้รับการอนุมัติจากคณะกรรมการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

2) คณะกรรมการบริหารความเสี่ยงและควบคุมภายใน ต้องจัดให้มีทรัพยากรสนับสนุนการดำเนินงาน และงบประมาณที่พอเพียงต่อการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศในแต่ละปีงบประมาณ

3) คณะกรรมการฯ ต้องวางแผนการติดตามและประเมินผลการใช้งานความมั่นคงปลอดภัยสารสนเทศ และนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ

4) คณะกรรมการฯ ต้องกำหนดรอบการทบทวน ตรวจสอบ ประเมินผล และปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงของสภาพแวดล้อมที่มีนัยสำคัญ เช่น สภาพองค์กร กฎเกณฑ์ กฎหมาย และเทคโนโลยี เป็นต้น

5) คณะกรรมการฯ ต้องจัดให้มีการเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศให้บุคลากรขององค์กรได้รับทราบ ในลักษณะที่ให้ผู้ใช้งานเข้าถึงได้ง่าย เพื่อให้บุคลากรที่เกี่ยวข้องทราบและถือปฏิบัติเป็นไปตามที่นโยบายและแนวปฏิบัติที่กำหนด

6) งานอำนวยการ ต้องกำหนดแผนการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศประจำปี เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละ 1 ครั้ง

9.1.2 โครงสร้างความมั่นคงปลอดภัยสารสนเทศขององค์กร (Organization of information security)

<u>วัตถุประสงค์</u>

เพื่อควบคุม กำกับ ติดตามให้มีการแบ่งแยกหน้าที่ในการปฏิบัติงานของบุคลากร เพื่อให้สามารถตรวจสอบการปฏิบัติงานของบุคลากรได้ รวมถึงมีการกำหนดหน้าที่ความมั่นคงปลอดภัยสารสนเทศของบุคลากรให้ชัดเจน เพื่อเป็นการลดความเสี่ยงด้านความมั่นคงปลอดภัยของโครงสร้างและระบบเทคโนโลยีสารสนเทศ จากการเข้าถึง หรือการเข้าไปแก้ไขเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต หรือการนำทรัพย์สินสารสนเทศไปใช้ในงานที่ผิดต่อวัตถุประสงค์

<u>แนวปฏิบัติ</u>

1) การจัดโครงสร้างภายในองค์กร (Internal organization)

1.1) คณะกรรมการบริหารความเสี่ยงและควบคุมภายในมีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศของหน่วยงาน ให้การสนับสนุน และกำหนดทิศทางการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศที่ชัดเจน รวมทั้งมีการมอบหมายงานที่เกี่ยวข้องให้กับผู้ปฏิบัติงานอย่างชัดเจน

1.2) คณะกรรมการฯ ต้องควบคุมให้มีการกำหนดเนื้องาน หรือหน้าที่ความรับผิดชอบต่าง ๆ (Job Description) เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศไว้อย่างชัดเจน เช่น การแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงาน (Developer) ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ (System administrator) ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริง (Production environment) ทั้งนี้ ในกรณีที่ไม่สามารถแบ่งแยกหน้าที่ความรับผิดชอบออกได้เนื่องจากข้อจำกัดต่าง ๆ คณะกรรมการฯ ต้องจัดให้มีกระบวนการติดตาม และตรวจสอบการปฏิบัติของบุคลากรที่เกี่ยวข้องอย่างใกล้ชิดและสม่ำเสมอเพื่อลดความเสี่ยงที่อาจเกิดขึ้น

1.3) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุมดูแลข้อมูลข้อมูลคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ให้มีความปลอดภัยอยู่เสมอ ตลอดจนดูแลรักษา และปรับปรุงเครือข่ายคอมพิวเตอร์เพื่อให้สามารถใช้งานได้ดีอยู่เสมอ รวมทั้งจะต้องสอดส่องดูแลการใช้เครือข่ายคอมพิวเตอร์ของผู้ใช้งาน เพื่อให้เป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ หากบุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลพบว่าผู้ใช้งานผู้ใดมี

พฤติกรรมส่อไปในทางที่จะละเมิดนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลจะต้องรายงานให้รองผู้อำนวยการฝ่ายโครงสร้างพื้นฐานทางสารสนเทศทราบโดยเร็วที่สุด และในกรณีจำเป็น เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นแก่องค์กร บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลมีอำนาจในการระงับการใช้งานระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ของผู้ใช้งานดังกล่าวได้ทันที

1.4) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องไม่ใช้อำนาจหน้าที่ของตนไปในการเข้าถึงข้อมูลที่รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น และจะต้องไม่เปิดเผยข้อมูลที่ตนได้รับมาจาก หรือเนื่องมาจากการปฏิบัติหน้าที่บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัล ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่ควรเปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ

1.5) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องไม่ใช้อำนาจหน้าที่ของตนไปในการเข้าถึงข้อมูล หรือเข้าควบคุมการใช้งานระบบคอมพิวเตอร์ของผู้ใช้งาน เว้นแต่ในกรณีที่มีเหตุจำเป็นเพื่อประโยชน์ในการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือกรณีได้รับอนุญาตจากผู้ใช้งานให้กระทำการดังกล่าวได้

1.6) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุมให้มีการสร้างความร่วมมือระหว่างผู้ที่มีบทบาทเกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน ในงานหรือกิจกรรมใด ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

1.7) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุมให้มีการกำหนดขั้นตอน และช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีหน้าที่ในการกำกับดูแล หรือหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมาย หน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้าน หรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ รวมทั้งหน่วยงานที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน

1.8) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดให้มีการควบคุมความมั่นคงปลอดภัยสารสนเทศในการบริหารจัดการโครงการ ทั้งโครงการที่เป็นโครงการภายใน และโครงการที่จัดซื้อจัดจ้างผู้ให้บริการภายนอกเป็นผู้ดำเนินการ ดังนี้

(1) พิจารณาความเสี่ยง และผลกระทบด้านความมั่นคงปลอดภัยสารสนเทศของโครงการ ทั้งก่อนเริ่มโครงการ ระหว่างดำเนินการโครงการ และเมื่อโครงการเสร็จสิ้น

(2) กำหนดข้อตกลง และความต้องการด้านความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องกับนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมถึงกฎระเบียบ หรือข้อบังคับต่าง ๆ ที่เกี่ยวข้องขององค์กรไว้ในข้อตกลงหรือสัญญาของโครงการ

(3) กำหนดบทลงโทษเมื่อผู้ดำเนินงานไม่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมถึงกฎระเบียบหรือข้อบังคับต่าง ๆ ที่เกี่ยวข้องขององค์กรไว้ในข้อตกลงหรือสัญญาของโครงการ

9.1.3 ข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม (Threat intelligence)

<u>วัตถุประสงค์</u>

เพื่อให้องค์กรตระหนักถึงสภาพแวดล้อมที่เป็นภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ และให้มีการรวบรวมและวิเคราะห์ข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อสร้างข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม ซึ่งจะช่วยลดผลกระทบที่จะเกิดขึ้นได้อย่างเหมาะสม

<u>แนวปฏิบัติ</u>

1) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องมีการระบุ ตรวจสอบ และเลือกแหล่งข้อมูลภัยคุกคามทั้งภายในและภายนอกองค์กรที่จำเป็นและเหมาะสม เพื่อนำมาซึ่งการรวบรวมข้อมูลที่จำเป็นต่อการวิเคราะห์เชิงลึกด้านภัยคุกคาม

2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องมีการประมวลผลข้อมูลที่รวบรวมเพื่อเตรียมการวิเคราะห์เชิงลึกด้านภัยคุกคาม

3) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องวิเคราะห์ข้อมูลเชิงลึกภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อตรวจสอบถึงผลกระทบที่มีต่อระบบคอมพิวเตอร์และระบบเทคโนโลยีสารสนเทศขององค์กร และ

4) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องมีการสื่อสารรายละเอียดภัยคุกคามให้กับผู้ที่เกี่ยวข้องได้รับทราบในรูปแบบที่เข้าใจได้โดยง่าย

5) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องพิจารณานำข้อมูลภัยคุกคามที่ได้ทำการวิเคราะห์เป็นแหล่งข้อมูลในการจัดทำมาตรการควบคุมหรือป้องกันภัยคุกคามในองค์กร เช่น การจัดหาซอฟต์แวร์การตรวจสอบเครือข่าย หรือซอฟต์แวร์ป้องกันมัลแวร์ เป็นต้น

9.1.4 การบริหารจัดการทรัพย์สินสารสนเทศ (Asset management)

<u>วัตถุประสงค์</u>

เพื่อควบคุม กำกับ ติดตามการบริหารจัดการทรัพย์สินสารสนเทศ ให้มีการบันทึกรายการทรัพย์สินสารสนเทศขององค์กรที่ครบถ้วน มีการกำหนดความรับผิดชอบในการดูแลทรัพย์สินทั้งหมด และมีการกำหนดระดับความสำคัญของข้อมูลคอมพิวเตอร์ขององค์กร เพื่อให้การดูแลรักษาข้อมูลคอมพิวเตอร์เป็นไปอย่างเหมาะสม

<u>แนวปฏิบัติ</u>

1) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุมและกำกับให้มีการเก็บบันทึกข้อมูลทรัพย์สินสารสนเทศ โดยข้อมูลที่จัดเก็บต้องประกอบด้วยข้อมูลที่จำเป็นในการค้นหาเพื่อการใช้งานในภายหลัง และจัดให้มีการทบทวนทะเบียนดังกล่าวอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ
2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดบุคลากร หรือหน่วยงานผู้มีหน้าที่ดูแลควบคุมการใช้งานทรัพย์สินสารสนเทศ และผู้มีหน้าที่รับผิดชอบทรัพย์สินสารสนเทศอย่างเหมาะสม ตลอดอายุการใช้งาน
3) บุคลากรและหน่วยงาน หรือบุคลากรภายนอกที่ว่าจ้างต้องส่งคืนทรัพย์สินสารสนเทศขององค์กรเมื่อสิ้นสุดสถานะการเป็นเจ้าหน้าที่ ลูกจ้าง หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงานให้กับองค์กร
4) ผู้บังคับบัญชาต้องควบคุม กำกับให้มีการขอยกเลิกสิทธิในการเข้าใช้งานระบบคอมพิวเตอร์ของเจ้าหน้าที่ ลูกจ้าง หน่วยงาน หรือบุคลากรภายนอกภายใต้การกับกำดูแล เมื่อสิ้นสุดสถานะการเป็นเจ้าหน้าที่ ลูกจ้าง หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงาน หรือควบคุม กำกับให้มีการปรับเปลี่ยนระดับสิทธิในการเข้าใช้งานระบบคอมพิวเตอร์ให้เหมาะสม เมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบใด ๆ เกิดขึ้น
5) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดระดับชั้นความลับของสารสนเทศ ให้มีความเหมาะสมกับประเภทของข้อมูล และลักษณะการนำไปใช้งาน โดยให้พิจารณาจาก

ข้อกำหนดทางกฎหมาย ความสำคัญของข้อมูล ผลกระทบด้านชื่อเสียง และมูลค่าของข้อมูลที่สูญเสียไปในกรณีที่เกิดการเปลี่ยนแปลงแก้ไขข้อมูล หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และต้องมีการกำหนดให้มีขั้นตอนปฏิบัติที่เหมาะสมสำหรับการใช้งานข้อมูลคอมพิวเตอร์

6) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องจัดให้มีฉลาก และปิดฉลากที่ระบุอ้างอิง รหัส หรือบาร์โค้ด ซึ่งสามารถใช้เป็นข้อมูลชี้เฉพาะทรัพย์สินสารสนเทศแต่ละชิ้นได้

7) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องจัดทำขั้นตอนการปฏิบัติงานสำหรับกำหนดระดับชั้นความลับ และการจัดการทรัพย์สินสารสนเทศ โดยให้มีสาระสำคัญครอบคลุมเรื่องต่อไปนี้

   7.1) การกำหนดระดับชั้นความลับข้อมูล โดยคำนึงถึงระดับความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศ ผลกระทบต่อมูลค่า และความเสียหายที่ผู้ใช้บริการอาจได้รับ รวมถึงผลกระทบต่อความเสียหายต่อทรัพย์สินและชื่อเสียงในการดำเนินงานขององค์กร

   7.2) การเปลี่ยนแปลงระดับชั้นความลับของสารสนเทศ

   7.3) การควบคุมและป้องกันสารสนเทศ ได้แก่

      (1) การจัดเตรียมข้อมูล และการระบุชั้นความลับ

      (2) การอ่านหรือทำสำเนาข้อมูล

      (3) การส่งข้อมูล

      (4) การจัดเก็บเอกสาร ข้อมูล

      (5) การทำลายเอกสาร

      (6) การจัดการกับการสูญหายของข้อมูล

   7.4) กำหนดระยะเวลาการจัดเก็บ ระยะเวลาการทำลายข้อมูลและทรัพย์สินสารสนเทศ

9.1.5 การถ่ายโอนข้อมูล (Information transfer)

<u>วัตถุประสงค์</u>

เพื่อรักษาความปลอดภัยของข้อมูลสารสนเทศ และโปรแกรมที่มีการถ่ายโอนกันทั้งภายในองค์กรและคู่สัญญาที่เป็นบุคคล หรือหน่วยงานภายนอก

<u>แนวปฏิบัติ</u>

1) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดให้มีนโยบายหรือวิธีปฏิบัติงานสำหรับการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานภายในองค์กร และระหว่างองค์กรกับหน่วยงานภายนอก รวมทั้งควบคุมการแลกเปลี่ยนข้อมูลคอมพิวเตอร์ผ่านช่องทางการสื่อสารในรูปแบบข้อมูลอิเล็กทรอนิกส์และเครือข่าย โดยต้องพิจารณาและดำเนินการมาตรการที่เหมาะสม เพื่อปกป้องข้อมูลที่ถูกถ่ายโอนให้มีความปลอดภัย และให้สอดคล้องตามระดับชั้นความลับข้อมูลที่ได้กำหนดไว้

2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลมีหน้าที่รับผิดชอบในการกำกับดูแลการดำเนินการและบำรุงรักษากลไกการส่งข้อมูลอย่างปลอดภัย เช่น เครือข่ายส่วนตัวเสมือน (VPN), โปรโตคอลการถ่ายโอนไฟล์แบบปลอดภัย (SFTP) หรือ โปรโตคอลการส่งผ่านข้อมูลแบบปลอดภัย (HTTPS) รวมถึงควบคุมการรับส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-mail) หรือ EDI (Electronic Data Interchange) หรือ Instant Messaging หรือระบบเครือข่ายสังคมออนไลน์ (Social Networking) เป็นต้น ตามนโยบายการใช้ระบบเทคโนโลยีสารสนเทศเพื่อความมั่นคงปลอดภัยสำหรับผู้ใช้งาน (Acceptable Use Policy)

3) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุมให้มีการจัดทำข้อตกลงในการแลกเปลี่ยนข้อมูลคอมพิวเตอร์หรือซอฟต์แวร์ระหว่างหน่วยงานภายในองค์กรกับบุคคลหรือหน่วยงานภายนอก โดยการแลกเปลี่ยนข้อมูลคอมพิวเตอร์ภายในองค์กรกับหน่วยงานภายนอก ควรได้รับการอนุมัติจากเจ้าของข้อมูลก่อนดำเนินการ และควรมีการควบคุมโดยการระบุข้อตกลงเป็นลายลักษณ์อักษร รวมถึงกำหนดเงื่อนไขสำหรับการแลกเปลี่ยน ตลอดจนต้องมีการป้องกันข้อมูลคอมพิวเตอร์ตามระดับชั้นความลับข้อมูลอย่างเหมาะสม

4) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุมให้มีการจัดทำข้อตกลงด้านการรักษาความลับของข้อมูล (Non-disclosure agreement - NDA) กับผู้ให้บริการภายนอก รวมทั้งการกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศไว้ในข้อตกลงหรือสัญญาจ้าง

9.1.6 การควบคุมการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ (Access control)

<u>วัตถุประสงค์</u>

เพื่อควบคุม กำกับ ติดตามการเข้าถึงระบบและเครือข่ายคอมพิวเตอร์ขององค์กร รวมทั้งกำหนดให้สามารถตรวจสอบ ติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบ และเครือข่ายคอมพิวเตอร์ได้อย่างถูกต้อง และเพื่อป้องกันการบุกรุกผ่านเครือข่ายคอมพิวเตอร์จากผู้ไม่ประสงค์ดีที่ต้องการสร้างความเสียหายแก่ข้อมูลคอมพิวเตอร์หรือการทำงานของระบบ หรือประสงค์ให้การให้บริการของเครือข่ายคอมพิวเตอร์ต้องหยุดชะงัก

<u>แนวปฏิบัติ</u>

1) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดให้มีการควบคุมการเข้าถึงระบบคอมพิวเตอร์ตามข้อกำหนดขององค์กร (Requirements of access control) ดังนี้

    1.1) กำหนดการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

    1.2) จำกัดสิทธิการเข้าถึงพื้นที่ที่ต้องการรักษาความมั่นคง โดยให้มีเฉพาะบุคลากรที่มีหน้าที่รับผิดชอบในการปฏิบัติงานเท่านั้น

    1.3) กำหนดสิทธิการเข้าถึงข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ทั้งจากภายในองค์กรและภายนอกองค์กรให้เหมาะสมกับหน้าที่ความรับผิดชอบของผู้ใช้งาน และระดับชั้นความลับของข้อมูล รวมทั้งให้มีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

    1.4) กำหนดระยะเวลาการตัดการใช้งานระบบคอมพิวเตอร์โดยให้พิจารณาตามความสำคัญของระบบ หากไม่มีการใช้งานติดต่อกันภายในระยะเวลาที่กำหนด (Idle Time-Out)

    1.5) กำหนดให้ผู้ใช้งานสามารถเข้าถึงเว็บไซต์ภายนอกได้เฉพาะเว็บไซต์ที่มีความน่าเชื่อถือเท่านั้น

    1.6) กำหนดให้ระบบคอมพิวเตอร์ตัดการเชื่อมต่อ หากมีการระบุรหัสผ่านไม่ถูกต้อง (Password attempt) โดยพิจารณาจากความสำคัญของระบบงาน

    1.7) ควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์ โดยกำหนดการระบุประเภทหรือบริการทางเครือข่าย (Network services) รวมถึงบุคคลที่ได้รับอนุญาตให้เข้าถึง กระบวนการ

ควบคุมและป้องกันการเข้าถึง วิธีการเข้าถึงแบบปลอดภัย เทคนิคการระบุตัวตน และการติดตามการใช้งานของบุคคลที่ได้รับอนุญาตให้เข้าถึง

1.8) จัดให้มีระบบที่สามารถระบุผู้ใช้งานในระบบเครือข่ายคอมพิวเตอร์ได้อย่างชัดเจน เพื่อให้องค์กรมีข้อมูลที่สามารถระบุผู้ใช้งานหมายเลข IP address ในช่วงเวลาที่ใช้งานได้

2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดให้มีการบริหารจัดการบัญชีผู้ใช้งาน (User access management) สำหรับเข้าถึงระบบคอมพิวเตอร์ขององค์กร ดังนี้

2.1) กำหนดขั้นตอนปฏิบัติสำหรับบริหารจัดการการลงทะเบียน และถอดถอนสิทธิผู้ใช้งานอย่างเป็นลายลักษณ์อักษรและปรับปรุงให้เป็นปัจจุบันอยู่เสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม

2.2) กำหนดสิทธิการเข้าถึงระบบคอมพิวเตอร์ตามหน้าที่งานและความรับผิดชอบของผู้ใช้งานนั้น ๆ

2.3) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องจัดทำรายชื่อผู้ใช้งานในระบบเพื่อทบทวนสิทธิการเข้าถึง และจัดส่งให้บังคับบัญชาแต่ละหน่วยงานเพื่อทบทวนรายชื่อและสิทธิการเข้าถึง และจัดส่งกลับมาเพื่อดำเนินการปรับปรุงรายการสิทธิการเข้าถึงตามที่ได้รับการยืนยันจากผู้บังคับบัญชาแต่ละหน่วยงาน อย่างน้อยปีละ 1 ครั้ง

2.4) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัล ต้องดำเนินการถอดถอนสิทธิหรือระงับสิทธิการเข้าถึงระบบคอมพิวเตอร์ และพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยเมื่อพบว่า

(1) มีการโอนย้ายหน่วยงาน หรือเลื่อนตำแหน่ง

(2) สิ้นสุดการจ้างงาน

(3) สิ้นสุดระยะเวลาการขอใช้งาน

3) เมื่อองค์กรตรวจสอบแล้วพบว่ามีแนวโน้มต่อการทุจริตด้านความมั่นคงปลอดภัยสารสนเทศหรือไม่มีความจำเป็นต้องใช้งาน ให้บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลพิจารณาดำเนินการถอดถอนสิทธิหรือระงับสิทธิการเข้าถึงระบบคอมพิวเตอร์ และพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยได้ตามความเหมาะสม

4) การควบคุมการเข้าถึงระบบคอมพิวเตอร์ และโปรแกรมประยุกต์ (System and application access control)

4.1) เจ้าของข้อมูลและบุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดวิธีการเข้าถึงข้อมูล ระบบคอมพิวเตอร์และฟังก์ชั่นในระบบงาน โดยต้องมีการจำกัดให้สอดคล้องกับนโยบายควบคุมการเข้าถึง

4.2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุมการใช้งานระบบคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต และระบบอินทราเน็ตขององค์กร ตามนโยบายการใช้ระบบเทคโนโลยีสารสนเทศเพื่อความมั่นคงปลอดภัยสำหรับผู้ใช้งาน (Acceptable Use Policy)

4.3) บุคลากรงานวิจัยและพัฒนาระบบงานดิจิทัลต้องควบคุมการใช้งานโปรแกรมประยุกต์ (Application) ตามแนวทางปฏิบัติดังนี้

(1) การใช้งานโปรแกรมประยุกต์ใด ๆ ผ่านเครือข่ายคอมพิวเตอร์ขององค์กร ผู้ใช้งานต้องได้รับอนุญาตจากเจ้าของระบบ และต้องได้รับอนุมัติสิทธิการใช้งานจากผู้บังคับบัญชาโดยตรงของตน

(2) ผู้ใช้งานสามารถใช้งานโปรแกรมประยุกต์ผ่านเครือข่ายคอมพิวเตอร์ขององค์กรได้เฉพาะโปรแกรมประยุกต์ที่องค์กรอนุญาตให้ใช้เท่านั้น

(3) ห้ามผู้ใช้งานติดตั้งโปรแกรมประยุกต์ใด ๆ บนระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ขององค์กรโดยไม่ได้รับอนุญาตจากองค์กร

(4) ห้ามผู้ใช้งานใช้งานโปรแกรมประยุกต์ในลักษณะที่อาจเป็นการละเมิดทรัพย์สินทางปัญญาขององค์กร หรือของบุคคลอื่นใด

4.4) บุคลากรงานวิจัยและพัฒนาระบบงานดิจิทัลต้องกำหนดวิธีการเข้าสู่ระบบคอมพิวเตอร์ที่มีความมั่นคงปลอดภัย โดยจัดให้มีระบบสำหรับบริหารจัดการบัญชีผู้ใช้และรหัสผ่านสำหรับการเข้าถึงระบบคอมพิวเตอร์ของผู้ใช้งานภายในองค์กร และการกำหนดรหัสผ่านในการเข้าถึงโดยผู้ใช้งานจะต้อง

(1) ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้งานระบบคอมพิวเตอร์ และเครื่องคอมพิวเตอร์ที่ผู้ใช้งานครอบครองใช้งานอยู่

(2) รหัสผ่านส่วนบุคคลดังกล่าวต้องมีความยาวไม่น้อยกว่า 8 ตัวอักษร และมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ เช่น % $

* ! เป็นต้น เข้าด้วยกัน

(3) ใช้งานวิธีพิสูจน์ตัวตนแบบสองปัจจัย (Two-Factor Authentication) หรือหลายปัจจัย (Multi-Factor Authentication) สำหรับทุกบัญชีผู้ใช้งาน

(4) ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อ หรือนามสกุลของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(5) ในกรณีผู้ใช้งานเข้าสู่ระบบคอมพิวเตอร์ผิดติดต่อกันเกิน 5 ครั้ง ชื่อผู้ใช้ (User ID) จะถูกระงับการเข้าใช้งานในทันที

(6) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Auto save password) สำหรับเครื่องคอมพิวเตอร์ขององค์กรที่ผู้ใช้งานครอบครองอยู่

(7) ไม่จด หรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตุของบุคคลอื่น

(8) ในกรณีที่สงสัยว่าบัญชีผู้ใช้งานถูกโจมตี หรือรหัสผ่านถูกเปิดเผย ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันที

4.5) บุคลากรงานวิจัยและพัฒนาระบบงานดิจิทัลต้องจัดเตรียมรหัสผ่านชั่วคราวที่บังคับให้ผู้ใช้เปลี่ยนรหัสผ่านเมื่อมีการเข้าสู่ระบบครั้งแรก

4.6) บุคลากรงานวิจัยและพัฒนาระบบงานดิจิทัลต้องจัดให้มีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย เช่น การส่งผ่านทางอีเมลที่มีการเข้ารหัส การส่งผ่านทางแพลตฟอร์มการส่งข้อความที่ปลอดภัย (เช่น Google Chat) การแจ้งผ่านทางโทรศัพท์ หรือผ่านหน้าพอร์ทัลสำหรับเข้าถึงชั่วคราวที่มีลิงก์แบบใช้ครั้งเดียว (one-time link) เป็นต้น

4.7) บุคลากรงานวิจัยและพัฒนาระบบงานดิจิทัลควรกำหนดให้มีการควบคุมการใช้โปรแกรมอรรถประโยชน์ เช่น โปรแกรมประเภทการจัดไฟล์ โปรแกรมบีบอัดไฟล์ เป็นต้น ทั้งนี้ควรจำกัดการใช้งานโปรแกรมอรรถประโยชน์สำหรับระบบคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่สำคัญ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้

4.8) บุคลากรงานวิจัยและพัฒนาระบบงานดิจิทัลควรตรวจสอบให้แน่ใจว่า บัญชีผู้ใช้และรหัสผ่านเริ่มต้น (default account and password) ทั้งหมดได้ถูกปิดใช้งานหรือเปลี่ยนแปลงก่อนนำไปใช้ในสภาพแวดล้อมการทำงานจริง (production environment)

9.1.7 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการพิจารณาใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก รวมถึงมาตรการสำหรับการกำกับดูแล ติดตามการดำเนินงาน และรายงานผลการดำเนินงานของผู้ให้บริการรายอื่น และเพื่อให้การใช้บริการดังกล่าวเกิดประสิทธิภาพ มีความมั่นคงปลอดภัย และเกิดประโยชน์สูงสุดแก่องค์กร

<u>แนวปฏิบัติ</u>

1) การรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์จากผู้ให้บริการภายนอก

1.1) องค์กรต้องกำหนดนโยบาย หรือสัญญาจ้าง หรือข้อตกลงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับผู้ให้บริการภายนอก โดยผู้ที่เกี่ยวข้องต้องพิจารณาความเสี่ยงที่อาจเกิดขึ้นและกำหนดแนวทางป้องกันเพื่อลดความเสี่ยง ก่อนที่จะอนุญาตให้ผู้ให้บริการภายนอก หรือบุคลากรภายนอกเข้าถึงระบบคอมพิวเตอร์ หรือใช้ข้อมูลคอมพิวเตอร์ขององค์กร

1.2) องค์กรต้องตรวจสอบให้แน่ใจว่าได้มีการทำข้อตกลงไม่เปิดเผยข้อมูล (NDA) กับผู้ให้บริการภายนอกก่อนที่จะเข้าถึงหรือแลกเปลี่ยนข้อมูลที่เป็นความลับหรือมีลิขสิทธิ์ โดยต้องมีการสื่อสารเรื่องข้อกำหนดและขั้นตอนในการใช้ข้อตกลงไม่เปิดเผยข้อมูล (NDA) รวมถึงวิธีการจัดการข้อมูลที่ละเอียดอ่อนที่ต้องได้รับการปกป้องให้แก่บุคลากรที่เกี่ยวข้อง มีการทบทวนข้อกำหนดเป็นระยะ และกำกับดูแลให้มั่นใจว่ามีความเข้าใจและมีการปฏิบัติตามอย่างต่อเนื่องทั่วทั้งองค์กร

1.3) องค์กรต้องควบคุม กำกับให้มีการดูแลให้บุคคลหรือผู้ให้บริการภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้าง ปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ

1.4) องค์กรต้องดำเนินการคัดเลือกผู้ให้บริการภายนอก ร่วมกับหน่วยงานที่เกี่ยวข้อง และนำเสนอต่อผู้บริหารของหน่วยงานนั้น ๆ เพื่อพิจารณาให้ความเห็นชอบและอนุมัติการคัดเลือก โดยควรให้ความสำคัญในเรื่องการรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์ที่สำคัญ (Confidentiality) ความถูกต้องเชื่อถือได้ของข้อมูลและระบบคอมพิวเตอร์ (Integrity) และความพร้อมใช้งานของระบบคอมพิวเตอร์ที่ใช้บริการ (Availability)

1.5) องค์กรต้องควบคุมการจ้างช่วงให้เป็นไปตามสัญญาจ้างที่องค์กรกำหนด

2) การควบคุมการส่งมอบงานของผู้ให้บริการภายนอก (Supplier service delivery management)

2.1) องค์กรต้องดำเนินการติดตามและตรวจสอบการดำเนินงานของผู้ให้บริการภายนอกอย่างสม่ำเสมอ โดยหากพบข้อสงสัย หรือความผิดปกติใด ๆ ที่อาจส่งผลกระทบหรือส่งผลกระทบต่อการใช้บริการให้รายงานต่อผู้ที่เกี่ยวข้องเพื่อพิจารณาแนวทางการบริหารจัดการโดยเร็ว

2.2) องค์กรต้องประเมินการให้บริการของผู้ให้บริการภายนอกที่ให้บริการที่เกี่ยวข้องกับด้านสารสนเทศ ตามรายสัญญาการให้บริการ โดยกำหนดระยะเวลาการประเมินดังนี้

(1) กรณีสัญญามีผล 1 ปี ให้ดำเนินการประเมินก่อนสิ้นสุดสัญญาล่วงหน้าอย่างน้อย 3 เดือน

(2) กรณีสัญญามีผลมากกว่า 1 ปี ให้ดำเนินการประเมินอย่างน้อยปีละ 1 ครั้ง

(3) กรณีมีการกำหนดระยะเวลาแจ้งยกเลิกสัญญาล่วงหน้าในสัญญา ให้ดำเนินการก่อนวันแจ้งล่วงหน้าอย่า

(4) กรณียกเลิกสัญญา ให้ดำเนินการประเมินทันทีที่มีการยกเลิกสัญญา

2.3) การประเมินผลการให้บริการของผู้ให้บริการภายนอก สามารถพิจารณาจากปัจจัยต่าง ๆ เช่น

(1) ความสะดวกในการติดต่อขอรับบริการ

(2) ความรวดเร็วในการให้บริการหรือแก้ไขปัญญา

(3) ความชำนาญ ความเชี่ยวชาญในการให้บริการหรือแก้ไขปัญหา

(4) ความสุภาพของเจ้าหน้าที่ผู้ให้บริการ

(5) การปฏิบัติตามนโยบาย ระเบียบปฏิบัติ และข้อกำหนดใด ๆ ขององค์กร

(6) คุณภาพของผลิตภัณฑ์หรือบริการที่ได้รับ

(7) ผลิตภัณฑ์หรือการให้บริการมีความครบถ้วน และตรงตามความต้องการ

(8) การส่งมอบผลิตภัณฑ์และบริการเป็นไปตามที่กำหนดไว้

(9) การรักษาความมั่นคงปลอดภัยและความลับของข้อมูล

(10)ความพร้อมในการให้บริการของผู้ให้บริการภายนอก

(11)ข้อร้องเรียนในการใช้บริการระหว่างการให้บริการของผู้ให้บริการภายนอก เป็นต้น

2.4) บุคลากรงานอำนวยการต้องรวบรวมผลการประเมินและจัดทำรายงานผลการใช้บริการให้คณะกรรมการฯ หรือรองผู้อำนวยการฝ่ายโครงสร้างพื้นฐานทางสารสนเทศรับทราบ

2.5) กรณีที่ผู้ให้บริการภายนอกมีการเปลี่ยนแปลงกระบวนการ ขั้นตอน วิธีการปฏิบัติงาน การรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน บุคลากรผู้รับผิดชอบโครงการควรพิจารณาถึงปัจจัยความเสี่ยงจากการเปลี่ยนแปลงดังกล่าวที่อาจส่งผลกระทบต่อการให้บริการ โดยรายงานให้ผู้บริหารและผู้ที่เกี่ยวข้องรับทราบ เพื่อกำหนดแนวทางการจัดการความเสี่ยงดังกล่าวอย่างเหมาะสม

3) ความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์ (Information security for use of cloud services)

สำหรับผู้ให้บริการภายนอกด้านระบบคลาวด์ องค์กรพิจารณาและกำหนดให้มีมาตรการควบคุมต้องไม่น้อยกว่าที่องค์กรกำหนดตามข้อ 1) และ 2) แต่ทั้งนี้จะต้องปฏิบัติตามที่กำหนดแนวทางเฉพาะที่องค์กรกำหนดตามรายละเอียดดังนี้

3.1) <u>นโยบายและมาตรการรักษาความมั่นคงปลอดภัยในการใช้บริการระบบคลาวด์</u>

องค์กรจัดให้มีนโยบาย มาตรการ และข้อกำหนดเกี่ยวกับการใช้บริการระบบคลาวด์ของผู้ให้บริการภายนอกโดยต้องมีแนวทางและเนื้อหาอย่างน้อยดังนี้

(1) การประเมินความเสี่ยงเกี่ยวกับการใช้บริการ

(2) การกำหนดประเภทงานและรูปแบบของการใช้บริการ เช่น Software as a Service (SaaS), Platform as a Service (PaaS) และ Infrastructure as a Service (IaaS)

(3) การกำหนดวิธีการคัดเลือกและประเมินผู้ให้บริการ (Due Diligence) โดยควรให้ความสำคัญในเรื่องการรักษาความปลอดภัยของข้อมูลสารสนเทศที่สำคัญ (Confidentiality) ความถูกต้องเชื่อถือได้ของข้อมูลและระบบสารสนเทศ (Integrity) และความพร้อมใช้งานของระบบสารสนเทศที่ใช้บริการ (Availability)

(4) การทบทวนคุณสมบัติของผู้ให้บริการอย่างสม่ำเสมอ เช่น ฐานะทางการเงิน ความเพียงพอของการให้บริการ (Capacity Planning) เพื่อให้มั่นใจว่าผู้ให้บริการยังคงมีความพร้อมในการให้บริการที่เพียงพอต่อความต้องการขององค์กรอย่างต่อเนื่อง

(5) การเผยแพร่นโยบายเกี่ยวกับการใช้บริการและการสื่อสารให้บุคลากรที่เกี่ยวข้องพร้อมทั้งลงนามรับทราบเพื่อให้ตระหนักถึงความมั่นคงปลอดภัยจากการใช้บริการระบบคลาวด์

(6) การกำหนดบทบาทหน้าที่ความรับผิดชอบของผู้ให้บริการอย่างชัดเจน เช่น การสำรองข้อมูล การรับเรื่องแก้ไขปัญหา ขั้นตอนและกระบวนการแก้ไขปัญหา รายชื่อและช่องทางสำหรับติดต่อ

(7) การกำหนดมาตรการรักษาความปลอดภัยของข้อมูลแต่ละประเภทที่จะใช้ในระบบคลาวด์ โดยแบ่งชั้นความลับของข้อมูล และกำหนดวิธีปฏิบัติแต่ละระดับชั้นความลับของข้อมูล

(8) มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามการใช้งานแต่ละประเภท เพื่อป้องกันภัยคุกคามและการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

(9) การกำหนดใช้วิธีพิสูจน์ตัวตนแบบ Multi-Factor Authentication สำหรับการเข้าถึงหน้าผู้บริหารระบบ (Administrator Page) สำหรับระบบสารสนเทศที่มีความสำคัญ

(10) กำหนดให้มีการตรวจสอบบันทึกหลักฐานและติดตามปัญหาที่อาจส่งผลต่อการใช้บริการ

3.2) <u>ข้อตกลงระหว่างองค์กรและผู้ให้บริการระบบคลาวด์</u>

องค์กรกำหนดให้มีเนื้อหาในข้อตกลงระหว่างองค์กรและผู้ให้บริการระบบคลาวด์โดยอย่างน้อยต้องมีเนื้อหาครอบคลุมข้อกำหนดดังต่อไปนี้

(1) กำหนดให้องค์กรเป็นเจ้าของข้อมูลสารสนเทศ

(2) ประเภทและรูปแบบการใช้บริการ

(3) มาตรฐานความปลอดภัย เช่น การเข้ารหัสข้อมูลที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์ การป้องกันการโจมตีในลักษณะ DDoS (Distributed Denial of Service) การป้องกันการบุกรุกจากโปรแกรมไม่ประสงค์ดี การป้องกันภัยคุกคามในรูปแบบใหม่ (Advanced Persistent Threat) การแบ่งแยกเครือข่าย การเข้ารหัสระหว่างแอปพลิเคชัน (Application) การป้องกันการบุกรุกแบบลำดับชั้น (Defense-in-depth) และการสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศ (Hardening) เป็นต้น

(4) การควบคุมการเข้าถึงข้อมูล เช่น วิธีการเข้าใช้งานระบบ วิธีการกำหนดสิทธิการใช้งาน การติดตามการแก้ปัญหา และการรายงานข้อผิดพลาดอย่างชัดเจน

(5) บทบาท หน้าที่ และความรับผิดชอบของผู้ให้บริการในการให้บริการ มาตรฐานการให้บริการ (Service Level Agreement) ระยะเวลาและกระบวนการกลับคืนสู่สภาพการดำเนินงานปกติของระบบสารสนเทศ (Recovery Time objectives: RTO) และเป้าหมายในการกู้คืนข้อมูล เช่น กำหนดประเภทของข้อมูลและชุดข้อมูลล่าสุดที่จะกู้คืนได้ (Recovery Point Objective: RPO) ให้ชัดเจน

(6) กำหนดเงื่อนไขความรับผิดชอบในกรณีที่ผู้ให้บริการไม่สามารถให้บริการตามสัญญาที่กำหนด

(7) ข้อตกลงที่เกี่ยวกับนโยบายการป้องกันการรั่วไหลของข้อมูลที่อาจเกิดขึ้นจากผู้ให้บริการ

(8) ผู้ให้บริการต้องไม่มีสิทธิเข้าถึงและเปิดเผยข้อมูลขององค์กรเว้นแต่ได้รับความยินยอมหรือแจ้งให้ทราบหากเป็นไปตามกฎหมายของประเทศที่ผู้ให้บริการไปตั้งศูนย์

คอมพิวเตอร์ (Cloud Server Hosting Country) หรือเป็นไปตามกฎหมายเกี่ยวกับความมั่นคงของประเทศผู้ให้บริการ (Origin Country)

(9) ผู้ให้บริการต้องปรับปรุงการปฏิบัติงานให้เป็นไปตามมาตรฐานการรับรองความมั่นคงปลอดภัยด้านสารสนเทศในระดับสากลโดยไม่ชักช้าในกรณีที่มีการปรับปรุงมาตรฐานสากลดังกล่าว

(10) ต้องมีมาตรการเพื่อให้มั่นใจได้ว่าผู้ให้บริการจัดให้มีการตรวจสอบขั้นตอนและการปฏิบัติงานอย่างน้อยปีละ 1 ครั้ง จากผู้ตรวจสอบอิสระ

(11) มีข้อกำหนดเมื่อสิ้นสุดการใช้บริการ (Exit Plan) เช่น กำหนดระยะเวลารักษาข้อมูลและวิธีการทำลายข้อมูลเพื่อให้มั่นใจว่าไม่สามารถกู้คืนข้อมูลกลับมาได้

(12) ต้องมีการเปิดเผยขั้นตอนปฏิบัติงานและเงื่อนไขการใช้บริการต่อจากผู้ให้บริการระบบคลาวด์รายอื่น (Sub Cloud) อย่างชัดเจน

(13) ข้อกำหนดให้องค์กรสามารถเข้าตรวจสอบความปลอดภัยสารสนเทศของผู้ให้บริการหรือจัดส่งเอกสารมาตรฐานความปลอดภัยตามที่องค์กรร้องขอ หรือยินยอมให้หน่วยงานกำกับดูแลที่เกี่ยวข้องเข้าตรวจสอบตามความจำเป็น

3.3) <u>กรณีผู้ให้บริการภายนอกมีการใช้บริการระบบคลาวด์ต่อจากผู้ให้บริการรายอื่น (Sub Cloud)</u>

จัดให้มีข้อกำหนดและข้อตกลงเพิ่มเติมในกรณีที่ผู้ให้บริการคลาวด์ใช้บริการผู้ให้บริการคลาวด์รายอื่นอย่างน้อยดังนี้

(1) การแจ้งรายละเอียดส่วนที่ใช้บริการผู้ให้บริการคลาวด์รายอื่นให้องค์กรทราบและให้ถือว่าบริการดังกล่าวเป็นส่วนหนึ่งของบริการของผู้ให้บริการด้วยโดยต้องมีคุณสมบัติด้านความปลอดภัยเทียบเท่ากับผู้ให้บริการ

(2) มีการเปิดเผยขั้นตอนปฏิบัติงานและเงื่อนไขการใช้บริการผู้ให้บริการคลาวด์รายอื่นแก่องค์กร

(3) มีมาตรการรักษาความลับและความปลอดภัยของข้อมูลในกรณีที่มีการรับส่งข้อมูลระหว่างผู้ให้บริการระบบคลาวด์และผู้ให้บริการระบบคลาวด์รายอื่น

3.4) <u>การติดตาม ประเมิน และทบทวนการให้บริการของผู้ให้บริการระบบคลาวด์</u>

กำหนดให้มีกระบวนการและขั้นตอนในการติดตามและทบทวนการให้บริการของผู้ให้บริการระบบคลาวด์ อย่างน้อยดังต่อไปนี้

(1) ติดตามตรวจสอบประสิทธิภาพของการให้บริการ มาตรการด้านความมั่นคงปลอดภัย ให้สอดคล้องกับข้อกำหนดตามสัญญาหรือข้อตกลงในการให้บริการ

(2) ประเมินความเพียงพอของระบบงานของผู้ให้บริการระบบคลาวด์อย่างสม่ำเสมอ

(3) ทบทวนเงื่อนไขการบริการในกรณีที่มีการเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าการให้บริการยังคงสอดคล้องกับการใช้งานและนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร

(4) ทบทวนคุณสมบัติของผู้ให้บริการอย่างต่อเนื่อง เช่น การตรวจสอบความมั่นคงในฐานะทางการเงิน กระบวนการปฏิบัติงาน และประสิทธิภาพการปฏิบัติงาน เป็นต้น

3.5) <u>กรณีต้องโอนย้ายข้อมูลไปยังผู้ให้บริการรายใหม่ (Data Migration)</u>

ในกรณีที่มีการเปลี่ยนผู้ให้บริการระบบคลาวด์ องค์กรต้องตรวจสอบขั้นตอนและมาตรการในการโอนย้ายข้อมูลไปยังผู้ให้บริการรายใหม่ รวมถึงมาตรการในการรักษาความลับและความปลอดภัยของข้อมูลในการโอนย้ายข้อมูลเพื่อให้มั่นใจได้ว่าข้อมูลสารสนเทศยังคงเป็นความลับ มีความครบถ้วน ถูกต้องและพร้อมใช้งานอยู่เสมอ ทั้งนี้รายละเอียดปรากฏตามข้อ 4)

4) การควบคุมการโอนย้ายข้อมูลของผู้ให้บริการ

ในกรณีที่ต้องมีการโอนย้ายข้อมูลไม่ว่าในกรณีการโอนให้ผู้ให้บริการช่วง หรือกรณีที่องค์กรประสงค์ให้มีการโอนย้ายข้อมูลไปยังผู้ให้บริการระบบคลาวด์รายใหม่ องค์กรกำหนดให้มีแนวทางในการตรวจสอบและควบคุมการโอนย้ายข้อมูลดังต่อไปนี้ โดยกำหนดให้งานโครงสร้างพื้นฐานระบบดิจิทัลภายใต้การกำกับดูแลของรองผู้อำนวยการฝ่ายโครงสร้างพื้นฐานทางสารสนเทศ เป็นผู้รับผิดชอบในการควบคุมและตรวจสอบ

4.1) <u>การกำหนดนโยบายและมาตรการ</u>

องค์กรจัดให้มีนโยบายและมาตรการเพื่อเป็นกรอบในการดำเนินงานของฝ่ายงานที่เกี่ยวข้องกับการโอนย้ายข้อมูลขององค์กร โดยคำนึงถึงความเสี่ยง ความปลอดภัย และการรักษาความลับของข้อมูล โดยเฉพาะข้อมูลส่วนบุคคลและข้อมูลความลับขององค์กร

พร้อมจัดให้มีการอบรมแก่บุคลากรในฝ่ายโครงสร้างพื้นฐานทางสารสนเทศที่เกี่ยวข้องเป็นประจำ ทั้งนี้ นโยบายและมาตรการในการโอนย้ายข้อมูลต้องได้รับการทบทวนเป็นประจำสม่ำเสมออย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าแนวทางในการดำเนินงานสอดคล้องกับเทคโนโลยีและมีความปลอดภัย

4.2) <u>ก่อนการโอนย้ายข้อมูล</u>

(1) องค์กรกำหนดให้ผู้ให้บริการภายนอกต้องแจ้งการโอนย้ายข้อมูลแก่องค์กรก่อนการโอนย้ายข้อมูล และแจ้งแนวทางในการโอนย้ายข้อมูลอย่างชัดเจนกรณีที่องค์กรร้องขอ โดยการโอนย้ายข้อมูลจะต้องดำเนินการในกรณีที่มีความจำเป็นและเพื่อการดำเนินการตามสัญญากับองค์กรเท่านั้น

(2) กำหนดให้ฝ่ายโครงสร้างพื้นฐานทางสารสนเทศเป็นผู้พิจารณาและตรวจสอบแนวทางในการถ่ายโอนข้อมูลว่ามีมาตรการในการรักษาความลับและความปลอดภัยเหมาะสมกับระดับความลับและขนาดของข้อมูลที่มีการถ่ายโอนหรือไม่

(3) ตรวจสอบข้อมูลก่อนการโอนย้ายเพื่อให้มั่นใจได้ว่าข้อมูลมีความสมบูรณ์ ถูกต้อง และครบถ้วนก่อนเข้ารหัสข้อมูลเพื่อทำการโอนย้าย

4.3) <u>ภายหลังการโอนย้ายข้อมูล</u>

(1) กำหนดให้ผู้ให้บริการภายนอกแจ้งผลการโอนย้ายข้อมูลขององค์กร โดยฝ่ายโครงสร้างพื้นฐานทางสารสนเทศตรวจสอบผลการโอนย้ายที่ผู้ให้บริการแจ้งแก่องค์กรควบคู่กับการตรวจสอบข้อมูลจริงที่มีการโอนย้าย เพื่อให้มั่นใจได้ว่าการโอนย้ายสำเร็จและครบถ้วนเป็นอย่างดี

(2) กำหนดให้มีการทบทวนกระบวนการในการโอนย้ายข้อมูลเพื่อพิจารณาปรับปรุงนโยบายและมาตรการในการโอนย้ายข้อมูลขององค์กร เพื่อนำเสนอและอนุมัติใช้ต่อไป

(3) กำหนดให้มีมาตรการรักษาความปลอดภัยด้านข้อมูลขององค์กร โดยผู้ให้บริการภายนอกต้องลบหรือทำลายข้อมูลที่องค์กรได้เปิดเผยแก่ผู้ให้บริการภายนอก ทั้งนี้ ให้ฝ่ายโครงสร้างพื้นฐานทางสารสนเทศเป็นผู้ตรวจสอบการลบหรือการทำลายข้อมูลดังกล่าวเพื่อให้มั่นใจว่าข้อมูลขององค์กรจะไม่เกิดการรั่วไหลภายหลังจากที่มีการโอนย้ายข้อมูลจากผู้ให้บริการภายนอกรายเดิมเสร็จเรียบร้อยแล้ว

9.1.8 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information security incident management)

<u>วัตถุประสงค์</u>

เพื่อควบคุม กำกับ ติดตามเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ รวมถึงกำหนดช่องทางการรายงานสำหรับบุคลากรและผู้ให้บริการภายนอก เมื่อพบเห็นเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ และช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศ

<u>แนวปฏิบัติ</u>

1) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องจัดทำขั้นตอนการปฏิบัติงานและกำหนดขอบเขตความรับผิดชอบของผู้ที่เกี่ยวข้องอย่างเป็นลายลักษณ์อักษร เพื่อตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่คาดคิดอย่างรวดเร็ว มีระเบียบ และมีประสิทธิผล
2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดช่องทางการรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศขององค์กร และแจ้งให้บุคลากร หน่วยงานภายนอก และบุคลากรภายนอกที่เกี่ยวข้องรับทราบ
3) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องแจ้งให้ผู้ใช้งานรายงานช่องโหว่หรือจุดอ่อนใด ๆ ด้านความมั่นคงปลอดภัยสารสนเทศ ที่อาจสังเกตพบให้บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลรับทราบ
4) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องดำเนินการตรวจสอบและประเมินช่องโหว่หรือจุดอ่อนใด ๆ ด้านความมั่นคงปลอดภัยสารสนเทศ จัดแยกกลุ่มและลำดับความสำคัญตามเกณฑ์ที่องค์กรกำหนด และแจ้งผู้เกี่ยวข้องเพื่อแก้ไขในกรณีที่พบว่าช่องโหว่หรือจุดอ่อนนั้นอาจเป็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ
5) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลและผู้ให้บริการภายนอกที่ทำหน้าที่แก้ไขเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องดำเนินการตามขั้นตอนการปฏิบัติงานที่ได้กำหนดไว้
6) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องมีการบันทึกเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่พบและวิธีการแก้ไข เพื่อนำมาวิเคราะห์ในการลดโอกาสเกิดในอนาคต
7) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลและผู้ให้บริการภายนอกที่ทำหน้าที่แก้ไขเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องดำเนินการรวบรวม จัดเก็บ และนำเสนอหลักฐานให้สอดคล้องกับหลักเกณฑ์ของกฎหมายที่ใช้บังคับ

8) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลควรแจ้งบุคคลที่เกี่ยวข้อง เช่น ผู้ใช้งาน รับทราบโดยไม่ชักช้า ในกรณีที่เหตุการณ์ส่งผลกระทบต่อบุคคลดังกล่าว

9) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลควรจัดให้มีการรายงานความคืบหน้าในการบริหารจัดการสถานการณ์และผลการบริหารจัดการต่อผู้ที่เกี่ยวข้องเป็นระยะ และเมื่อเหตุการณ์ยุติแล้ว

10) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลควรจัดให้มีการจำลองสถานการณ์ เพื่อทดสอบการเตรียมความพร้อมรับมือต่อเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ

9.1.9 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information security aspects of business continuity management)

<u>วัตถุประสงค์</u>

เพื่อควบคุม กำกับ ติดตามแผนงานการสร้างความต่อเนื่องของการดำเนินงานสำหรับกระบวนการดำเนินงานที่สำคัญขององค์กร เพื่อป้องกันการติดขัด หรือหยุดชะงักของการดำเนินงานขององค์กร และป้องกันกระบวนการการดำเนินงานที่สำคัญอันเป็นผลมาจากการล้มเหลวของระบบคอมพิวเตอร์ และเพื่อให้สามารถกู้คืนระบบคอมพิวเตอร์กลับมาได้ในระยะเวลาที่เหมาะสม

<u>แนวปฏิบัติ</u>

1) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องระบุเหตุการณ์ที่อาจส่งผลกระทบกับกระบวนการดำเนินงาน ประเมินความเสี่ยงเหตุการณ์และระบบงานสำคัญ เพื่อให้ได้มาซึ่งข้อมูลที่มีความถูกต้องและครบถ้วน เพื่อใช้ในการจัดทำแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉิน โดยให้กำหนดมาตรการด้านความมั่นคงปลอดภัยสารสนเทศไว้เป็นส่วนหนึ่งของแผน และให้มีความสอดคล้องกับแผนบริหารความต่อเนื่องทางธุรกิจขององค์กร ทั้งนี้ควรประกอบไปด้วยหัวข้อต่อไปนี้

   2.1) กำหนดขั้นตอนดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ให้เป็นไปตามแนวปฏิบัติการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

   2.2) กำหนดขั้นตอนการแก้ไขปัญหาในแต่ละเหตุการณ์โดยละเอียดและชัดเจน พร้อมทั้งกำหนดผู้มีหน้าที่รับผิดชอบที่สามารถปฏิบัติงานได้ในแต่ละเหตุการณ์

2.3) มีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน เช่น รุ่นของเครื่องคอมพิวเตอร์ คุณลักษณะของเครื่องคอมพิวเตอร์ (Specification) ขั้นต่ำ ข้อมูลเกี่ยวกับการปรับแต่ง (Configuration) และอุปกรณ์เครือข่ายคอมพิวเตอร์ เป็นต้น

2.4) ระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรอง (ถ้ามี) ให้ชัดเจน เช่น สถานที่ตั้ง แผนที่ เป็นต้น

3) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องทดสอบแผนรองรับกรณีเกิดเหตุฉุกเฉินอย่างน้อยปีละ 1 ครั้ง และจัดให้มีการบันทึกผลการทดสอบ เพื่อให้มั่นใจว่าแผนงานที่จัดทำมีความถูกต้องและสามารถตอบสนองต่อการดำเนินงานได้เป็นอย่างดี

4) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุมให้มีการประเมินความต้องการด้านการรักษาความพร้อมใช้งาน (Availability) ของระบบที่มีความสำคัญสูง และให้มีการติดตั้งอุปกรณ์หรือระบบสำรอง (Redundancy) เพื่อรักษาความต่อเนื่องในการดำเนินงานอย่างเหมาะสม

9.1.10 การปฏิบัติตามข้อกำหนด (Compliance)

<u>วัตถุประสงค์</u>

เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ และให้การตรวจประเมินระบบคอมพิวเตอร์ได้ประสิทธิภาพสูงสุด และมีการแทรกแซงหรือทำให้หยุดชะงักต่อกระบวนการดำเนินงานน้อยที่สุด

<u>แนวปฏิบัติ</u>

1) องค์กรต้องพิจารณาถึงกฎหมาย กฎระเบียบ หรือข้อบังคับตามสัญญาต่าง ๆ ที่มีผลบังคับใช้กับระบบคอมพิวเตอร์ขององค์กร

2) บุคลากรทุกคนต้องไม่ทำสำเนาหรือเผยแพร่ซอฟต์แวร์ที่องค์กรได้จัดซื้อลิขสิทธิ์เพื่อการใช้งาน ยกเว้นการทำสำเนานั้นเพียงแต่เพื่อไว้ใช้สำหรับเหตุฉุกเฉิน หรือเพื่อเป็นสำเนาไว้ใช้แทนซอฟต์แวร์ต้นฉบับเท่านั้น

3) บุคลากรทุกคนและเจ้าของข้อมูลคอมพิวเตอร์ต้องกำหนดแนวทางการจัดการข้อมูลคอมพิวเตอร์ระยะเวลาในการจัดเก็บให้สอดคล้องกับระดับชั้นความลับ รวมถึงข้อบังคับที่เกี่ยวข้อง

4) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุมข้อมูลคอมพิวเตอร์ส่วนบุคคลของบุคลากรให้สามารถเปิดเผยได้เฉพาะผู้ที่มีสิทธิตามที่องค์กรกำหนด

5) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องจัดให้มีการตรวจสอบระบบคอมพิวเตอร์ โดยผู้ตรวจสอบภายในขององค์กร (Internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor) เพื่อให้มั่นใจว่าการดำเนินงานสอดคล้องตามนโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงานด้านความปลอดภัยสารสนเทศที่กำหนดไว้ อย่างน้อยปีละ 1 ครั้ง

6) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุม กำกับให้ระบบคอมพิวเตอร์ โดยเฉพาะระบบที่สำคัญและมีความเสี่ยงสูงให้ได้รับการทดสอบระดับมาตรฐานความปลอดภัยสารสนเทศของระบบคอมพิวเตอร์อย่างสม่ำเสมอ เช่น การทดสอบการเจาะระบบ เพื่อตรวจสอบถึงจุดเปราะบางของระบบและประสิทธิผลของการควบคุมด้านความปลอดภัยสารสนเทศ

9.2 มาตรการควบคุมด้านบุคลากร (People controls)

9.2.1 ความมั่นคงปลอดภัยสารสนเทศสำหรับทรัพยากรบุคคล (Human resource security)

<u>วัตถุประสงค์</u>

เพื่อควบคุม กำกับ ติดตามให้มีการแบ่งแยกหน้าที่ในการปฏิบัติงานของบุคลากร สามารถตรวจสอบการปฏิบัติงานของบุคลากรได้ รวมถึงต้องมีการกำหนดหน้าที่ด้านความมั่นคงปลอดภัยสารสนเทศของบุคลากรให้ชัดเจน ซึ่งจะเป็นการลดความเสี่ยงด้านความมั่นคงปลอดภัยของโครงสร้างและระบบคอมพิวเตอร์ขององค์กร จากการเข้าถึงหรือการเข้าไปแก้ไขเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต หรือการนำทรัพย์สินสารสนเทศไปใช้ในงานที่ผิดต่อวัตถุประสงค์

<u>แนวปฏิบัติ</u>

1) คณะกรรมการบริหารความเสี่ยงและควบคุมภายใน ควรดำเนินงานร่วมกับฝ่ายทรัพยากรบุคคลเพื่อควบคุม กำกับ ติดตามให้มีการกำหนดลักษณะงาน (Job description) ซึ่งต้องระบุถึงหน้าที่และความรับผิดชอบของแต่ละตำแหน่งงาน และหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของบุคลากร หรือหน่วยงาน หรือบุคลากรภายนอกที่ว่าจ้าง โดยให้สอดคล้องกับความมั่นคงปลอดภัยสารสนเทศ และนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ

2) งานอำนวยการ ต้องตรวจสอบประวัติหรือคุณสมบัติ รวมถึงความสามารถของผู้ที่ได้รับคัดเลือกเข้ามาเป็นบุคลากรขององค์กร รวมถึงผู้ให้บริการภายนอกเพื่อให้เป็นไปตามระเบียบต่าง ๆ ที่เกี่ยวข้องตามที่องค์กรกำหนดไว้

3) งานอำนวยการ ต้องกำหนด ควบคุม และกำกับให้บุคลากรขององค์กร และหน่วยงานภายนอกหรือบุคลากรภายนอกที่ว่าจ้าง ต้องปฏิบัติงานตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศที่องค์กรประกาศใช้

4) งานอำนวยการ ต้องกำหนดให้บุคลากรได้รับการอบรมเพื่อเพิ่มความสามารถ และสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศในส่วนที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตน และได้รับการสื่อสารให้ทราบถึงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศที่องค์กรประกาศใช้อย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลง และสังเกตถึงความผิดปกติใด ๆ ที่อาจส่งผลต่อความปลอดภัยของระบบสารสนเทศ และรายงานบุคคลหรือหน่วยงานที่ทำหน้าที่รับแจ้งสถานการณ์ (Point of contact) ทันที เมื่อพบความผิดปกติดังกล่าวทุกครั้ง

5) งานอำนวยการ ต้องควบคุมการจัดเตรียมหลักฐานเพื่อใช้สนับสนุนการพิจารณาการลงโทษบุคลากรที่พบว่ากระทำความผิดตามแนวปฏิบัติการกำหนดบทลงโทษขององค์กร ให้สอดคล้องกับแนวทางการจัดการข้อมูลตามระดับชั้นความลับ

6) กรณีที่ได้รับแจ้งจากงานอำนวยการ หรือหน่วยงานต้นสังกัดว่ามีบุคลากรพ้นสภาพการเป็นบุคลากร หรือโยกย้ายตำแหน่งงาน รองผู้อำนวยการฝ่ายบริหารต้องมอบหมายให้บุคลากรงานอำนวยการเป็นผู้เรียกคืนทรัพย์สินสารสนเทศ และระงับสิทธิหรือปรับปรุงสิทธิการเข้าถึงให้เป็นปัจจุบัน

9.2.2 การปฏิบัติงานจากระยะไกล (Remote working)

<u>วัตถุประสงค์</u>

เพื่อควบคุม กำกับ ติดตามให้มีการกำหนดมาตรการรักษาด้านความมั่นคงปลอดภัยและสามารถนำไปปฏิบัติได้อย่างถูกต้องเหมาะสม เมื่อบุคลากรปฏิบัติงานจากระยะไกล เพื่อปกป้องข้อมูลที่ถูกเข้าถึง การประมวลผล หรือจัดเก็บจากภายนอกองค์กร รวมทั้งให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

<u>แนวปฏิบัติ</u>

การปฏิบัติงานที่มีการใช้อุปกรณ์แบบพกพา (Mobile device) เพื่อเข้าถึงระบบคอมพิวเตอร์ขององค์กร และการปฏิบัติงานจากเครือข่ายคอมพิวเตอร์จากภายนอกสถานที่ทำการขององค์กร (Teleworking) ให้ปฏิบัติตามแนวทางดังต่อไปนี้

1) เฉพาะบุคลากรที่ได้รับอนุญาตจากองค์กรเท่านั้น ที่มีสิทธิเข้าใช้งานระบบคอมพิวเตอร์บนเครือข่ายคอมพิวเตอร์ขององค์กร โดยผ่านการเข้าถึงเครือข่ายจากทางไกลที่องค์กรกำหนดขึ้น เพื่อให้การเข้าถึงเครือข่ายจากทางไกลดังกล่าวไม่ก่อให้เกิดความเสี่ยงภัยใด ๆ แก่ระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ขององค์กร

2) กำหนดประเภทการใช้งาน (Application service) ที่อนุญาตให้ใช้งานผ่านอุปกรณ์คอมพิวเตอร์ประเภทพกพา และกำหนดมาตรการควบคุมการเข้าถึงการใช้งานดังกล่าว โดยคำนึงถึงความปลอดภัยของการเชื่อมต่อกับเครือข่าย เช่น จำกัดให้เข้าถึงบริการการใช้งานบางประเภท หากเป็นการเชื่อมต่อกับเครือข่ายภายนอก เป็นต้น

3) บุคลากรที่ได้รับอนุญาตจากองค์กรตามข้อ 9.2.1 ต้องปฏิบัติตามนโยบายการใช้งานระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์เพื่อความมั่นคงปลอดภัยโดยเคร่งครัด เสมือนหนึ่งบุคลากรมีการใช้งานระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ ณ ที่ตั้งสถานที่ทำการขององค์กร

4) ก่อนเข้าใช้งานระบบคอมพิวเตอร์บนเครือข่ายคอมพิวเตอร์ขององค์กร โดยผ่านการเข้าถึงเครือข่ายจากทางไกลทุกครั้ง บุคลากรต้องตรวจสอบให้แน่ใจว่าเครื่องคอมพิวเตอร์ รวมทั้งอุปกรณ์ที่เกี่ยวข้องทั้งหมดที่จะใช้เข้าถึงเครือข่ายจากทางไกลนั้น ได้รับการอัพเดทโปรแกรมแก้ไขจุดอ่อน หรือช่องโหว่ (Vulnerability) ให้เป็นรุ่นล่าสุดแล้ว

5) เครื่องคอมพิวเตอร์รวมทั้งอุปกรณ์ที่เกี่ยวข้องทั้งหมดต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัสรุ่นล่าสุด ณ ขณะที่ใช้งานแล้วเท่านั้นที่จะได้รับอนุญาตจากองค์กรให้เข้าใช้งานระบบคอมพิวเตร์บนเครือข่ายคอมพิวเตอร์ขององค์กร โดยผ่านการเข้าถึงเครือข่ายจากทางไกล

6) มีมาตรการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญ (Sensitive data) กรณีที่อุปกรณ์คอมพิวเตอร์ประเภทพกพาสูญหาย เช่น การกำหนดให้ใส่รหัสผ่านก่อนใช้งานอุปกรณ์ (Lock screen) หรือการลบข้อมูลจากระยะไกล (Remote wipe-out)

7) กำหนดให้มีการเข้ารหัสข้อมูลสารสนเทศที่สำคัญและที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์ตามระดับชั้นความลับของข้อมูล

8) จัดให้มีการอบรมผู้ใช้งานเพื่อตระหนักและทราบถึงความเสี่ยงจากการใช้งาน และแนวทางการควบคุมความเสี่ยงดังกล่าว

9) จัดให้มีการดำเนินการเพื่อลดผลกระทบเมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลสารสนเทศ เช่น ตัดการเชื่อมต่อโดยทันทีที่ทราบสาเหตุ เป็นต้น

9.3 มาตรการควบคุมด้านกายภาพ (Physical controls)

9.3.1 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)

<u>วัตถุประสงค์</u>

เพื่อควบคุม กำกับ ติดตาม รวมถึงกำหนดมาตรการและวิธีป้องกันการเข้าถึงศูนย์คอมพิวเตอร์ และพื้นที่ปฏิบัติงานของเจ้าหน้าที่บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัล เพื่อรักษาความมั่นคงปลอดภัยในเชิงกายภาพ (Physical security) จากการเข้าถึงโดยไม่ได้รับอนุญาตที่อาจก่อให้เกิดความเสียหายต่อทรัพย์สินสารสนเทศ หรือเกิดการรบกวนข้อมูลของระบบคอมพิวเตอร์ และอุปกรณ์สนับสนุนในการประมวลผลข้อมูลคอมพิวเตอร์

<u>แนวปฏิบัติ</u>

1) การสร้างความมั่นคงปลอดภัยสำหรับพื้นที่ควบคุม (Secure areas)

1.1) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุม กำกับให้มีการป้องกันขอบเขตพื้นที่ศูนย์คอมพิวเตอร์ที่มีการติดตั้ง จัดเก็บ หรือใช้งาน ระบบและเครือข่ายคอมพิวเตอร์ รวมถึงข้อมูลคอมพิวเตอร์

1.2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดขั้นตอนปฏิบัติเพื่อควบคุมการเข้า-ออกพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure area) ได้แก่ ศูนย์คอมพิวเตอร์หลัก และพื้นที่ปฏิบัติงานของบุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัล โดยต้องกำหนดให้เฉพาะผู้มีสิทธิที่สามารถเข้า-ออกได้ และมีการเก็บบันทึกการเข้า-ออกศูนย์คอมพิวเตอร์ และบันทึกการเข้า-ออกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล เวลาผ่านเข้า-ออก รวมถึงต้องมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

1.3) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องมีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันพื้นที่ห้องปฏิบัติงานของเจ้าหน้าที่บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัล หรืออุปกรณ์สารสนเทศต่าง ๆ ที่ใช้ในการปฏิบัติงาน

1.4) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุม กำกับให้มีการออกแบบ และติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันภัยพิบัติต่าง ๆ ทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติ เช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น

1.5) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุมบริเวณที่ผู้ไม่มีสิทธิเข้าถึงอาจสามารถเข้าถึงได้ เช่น จุดรับส่งของ เป็นต้น โดยกำหนดพื้นที่การส่งมอบสินค้า และพื้นที่การเตรียมหรือประกอบอุปกรณ์สารสนเทศก่อนนำเข้าศูนย์คอมพิวเตอร์หลัก โดยต้องควบคุมการเข้า-ออกเพื่อหลีกเลี่ยงการเข้าถึงระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต

1.6) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดให้มีการบันทึกภาพเคลื่อนไหวผ่านกล้องวงจรปิด โดยข้อมูลที่บันทึกไว้จะต้องสามารถตรวจสอบย้อนหลังไม่น้อยกว่า 30 วัน ทั้งนี้ บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลจะต้องคำนึงถึงข้อกำหนดทางด้านกฎหมายและระเบียบข้อบังคับขององค์กรที่เกี่ยวข้องในการคุ้มครองข้อมูลส่วนบุคคลและระยะเวลาการเก็บรักษาบันทึกภาพเคลื่อนไหวดังกล่าว

2) การสร้างความมั่นคงปลอดภัยสำหรับทรัพย์สินสารสนเทศประเภทอุปกรณ์ (Equipment)

2.1) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดให้มีการจัดวางและป้องกันอุปกรณ์สารสนเทศ เพื่อลดความเสี่ยงจากภัยธรรมชาติหรืออันตรายต่าง ๆ และเพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต

2.2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องมีการป้องกันอุปกรณ์สารสนเทศ ที่อาจเกิดจากไฟฟ้าขัดข้อง (Power failure) หรือที่อาจหยุดชะงักจากข้อผิดพลาดของโครงสร้างพื้นฐาน (Supporting utilities) โดยจัดหา ติดตั้ง และบำรุงรักษา อุปกรณ์หรือระบบสนับสนุนในการรักษาความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์ เช่น อุปกรณ์ดับเพลิง อุปกรณ์สำรองไฟฟ้า ระบบควบคุมอุณหภูมิและความชื้น ระบบเตือนภัยน้ำรั่ว หรือระบบแจ้งเตือนเมื่ออุปกรณ์สารสนเทศทำงานผิดปกติ เป็นต้น

2.3) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องมีการป้องกันสายเคเบิลที่ใช้เพื่อการสื่อสารหรือสายไฟ และอุปกรณ์ที่เกี่ยวข้อง เช่น Floor switch และท่อเดินสายเคเบิล และสายไฟอย่างเหมาะสม เพื่อไม่ให้มีการดักรับสัญญาณ (Interception) หรือมีความเสียหายเกิดขึ้น

2.4) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องมีการดูแลและบำรุงรักษาอุปกรณ์สารสนเทศอย่างถูกวิธี เพื่อให้คงไว้ซึ่งความถูกต้องครบถ้วน และอยู่ในสภาพพร้อมใช้งานอยู่เสมอ

2.5) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุม กำกับให้มีการรักษาความมั่นคงปลอดภัยให้กับอุปกรณ์สารสนเทศที่มีการนำไปใช้งานนอกสถานที่ปฏิบัติงานของหน่วยงาน โดยให้คำนึงถึงระดับความเสี่ยงที่แตกต่างกันจากการนำไปใช้งานในสถานที่ต่าง ๆ

2.6) ผู้ใช้งานต้องไม่นำอุปกรณ์สารสนเทศ ข้อมูลคอมพิวเตอร์ หรือซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานขององค์กร หากมิได้รับอนุญาต

2.7) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดมาตรการหรือเทคนิคสำหรับการทำลายข้อมูลที่อยู่ในสื่อบันทึกข้อมูลหรืออุปกรณ์สารสนเทศให้มีความสอดคล้องกับการจัดระดับชั้นความลับข้อมูล

2.8) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องมีการตรวจสอบอุปกรณ์สารสนเทศนั้นว่าได้มีการลบ ย้าย หรือทำลายข้อมูลที่สำคัญหรือซอฟต์แวร์ที่จัดซื้อและติดตั้งไว้ด้วยวิธีการที่ทำให้ไม่สามารถกู้คืนได้อีก ก่อนการยกเลิกการใช้งานหรือจำหน่ายอุปกรณ์สารสนเทศที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์

2.9) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดมาตรการควบคุมการป้องกันเครื่องคอมพิวเตอร์และอุปกรณ์สารสนเทศที่ทิ้งไว้โดยไม่มีผู้ดูแล เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลที่ไม่ได้รับอนุญาต โดยควบคุมให้มีการล็อคหน้าจอคอมพิวเตอร์เมื่อไม่ได้ใช้งาน (Clear Screen) หรือเมื่อออกห่างจากเครื่องคอมพิวเตอร์นานกว่า 15 นาที ในกรณีที่พิจารณาแล้วว่าไม่สามารถกำหนดให้มีการล็อคหน้าจอตามที่กำหนดไว้โดยข้อจำกัดใด ๆ ให้บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลพิจารณาถึงความเสี่ยงที่อาจส่งผลกระทบและรายงานผู้บริหารรับทราบ

2.10) ผู้ใช้งานต้องไม่ละทิ้งข้อมูลคอมพิวเตอร์ที่สำคัญ เช่น เอกสารกระดาษ หรือสื่อบันทึกข้อมูล ให้อยู่ในสถานที่ที่ไม่ปลอดภัย พื้นที่สาธารณะ หรือสถานที่ที่พบเห็นได้โดยง่าย ผู้ใช้งานต้องจัดเก็บข้อมูลคอมพิวเตอร์ในสถานที่ที่เหมาะสม รวมถึงมีการป้องกันเพื่อให้ยากต่อการเข้าถึงจากผู้ไม่มีสิทธิ์

3) แนวทางการปฏิบัติก่อนเข้าพื้นที่ศูนย์คอมพิวเตอร์หลัก

3.1) ผู้ไม่มีสิทธิเข้าพื้นที่ที่มีความประสงค์เข้า-ออกศูนย์คอมพิวเตอร์หลักจะต้องแจ้งผู้ดูแลศูนย์ฯ ก่อนเข้าดำเนินการอย่างน้อย 3 วันทำการ

3.2) ผู้ไม่มีสิทธิเข้าพื้นที่ต้องลงชื่อ-เวลาการเข้าออกศูนย์คอมพิวเตอร์หลักทุกครั้งที่มีการใช้บริการ

3.3) กรณีที่มีการนำอุปกรณ์เข้าออกศูนย์คอมพิวเตอร์หลัก จะต้องกรอกเอกสารการนำอุปกรณ์เข้า-ออก ก่อนนำอุปกรณ์เข้าออกจากศูนย์

3.4) ในกรณีผู้ไม่มีสิทธิเข้าพื้นที่มีความจำเป็นต้องเข้าออกหรือนำอุปกรณ์เข้า-ออกศูนย์คอมพิวเตอร์หลัก ต้องมีการควบคุมอย่างรัดกุม โดยกำหนดให้มีเจ้าหน้าที่ที่ได้รับมอบหมายควบคุมดูแลการทำงานตลอดเวลา

3.5) ห้ามนำวัตถุระเบิด เชื้อเพลิง วัสดุติดเพลิงง่าย อาวุธ สารเคมี แร่แม่เหล็ก หรือสิ่งอื่นใดอันอาจก่อให้เกิดความเสียหายทั้งต่อชีวิตและทรัพย์สิน เข้ามาภายในศูนย์คอมพิวเตอร์หลัก

3.6) ห้ามสูบบุหรี่ หรือกระทำการใด ๆ อันอาจก่อให้เกิดควัน เพลิง หรือความเสียหายต่อชีวิตและทรัพย์สินภายในศูนย์คอมพิวเตอร์หลัก

3.7) ห้ามนำอาหาร เครื่องดื่ม และขนมขบเคี้ยวทุกชนิดเข้ามาภายในศูนย์คอมพิวเตอร์หลัก

3.8) ห้ามถ่ายรูปภายในศูนย์คอมพิวเตอร์หลัก ยกเว้นกรณีที่การถ่ายรูปนั้นจะเป็นไปเพื่อการทำงานที่เป็นประโยชน์ต่อองค์กร โดยหากจำเป็นต้องมีการถ่ายรูปจะต้องแจ้งต่อผู้ดูแลศูนย์ฯ ให้รับทราบก่อนดำเนินการ

3.9) กรณีที่บุคลากรหรือบุคคลภายนอกมีการส่งมอบหรือเปิดกล่องอุปกรณ์ ต้องดำเนินการภายในบริเวณพื้นที่ที่กำหนดไว้เท่านั้น

4) การเฝ้าระวังความมั่นคงปลอดภัยทางกายภาพ (Physical security monitoring)

4.1) พื้นที่ควบคุมขององค์กรต้องได้รับการเฝ้าระวังและติดตามสำหรับการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาตอย่างต่อเนื่อง โดยจัดให้มีระบบเฝ้าระวังความมั่นคงปลอดภัยทางกายภาพ เช่น ระบบกล้องวงจรปิด เพื่อบันทึกเหตุการณ์และการเข้าออกพื้นที่ตามจุดสำคัญในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย หรือระบบสัญญาณแจ้งเตือนไปยังเจ้าหน้าที่รักษาความปลอดภัยหรือเจ้าหน้าที่บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลในกรณีที่ตรวจพบการเข้าถึงพื้นที่ทางกายภาพโดยไม่ได้รับอนุญาต

4.2) ระบบเฝ้าระวังความมั่นคงปลอดภัยทางกายภาพต้องได้รับการปกป้องจากการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อป้องกันไม่ให้ข้อมูลการเฝ้าระวัง เช่น ข้อมูลบันทึกกล้องวงจรปิด ถูกเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต หรือระบบถูกปิดการใช้งานจากระยะไกล

4.3) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องมีการทดสอบระบบเฝ้าระวังความมั่นคงปลอดภัยทางกายภาพเป็นประจำอย่างสม่ำเสมอ เพื่อให้แน่ใจว่าระบบที่ได้มีการติดตั้งสามารถทำงานได้ตามที่กำหนดไว้

9.3.2 สื่อบันทึกข้อมูล (Storage media)

<u>วัตถุประสงค์</u>

เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบ หรือการทำลายข้อมูลบนสื่อบันทึกข้อมูลโดยไม่ได้รับอนุญาต

<u>แนวปฏิบัติ</u>

1) สื่อบันทึกข้อมูลต้องได้รับการบริหารจัดการตลอดวงจรชีวิตนับตั้งแต่การจัดหา การใช้งาน การขนย้าย/การขนส่ง และการจำหน่ายออก โดยให้เป็นไปตามขั้นตอนปฏิบัติการจัดระดับชั้นความลับและการจัดการกับข้อมูลและทรัพย์สินสารสนเทศที่เกี่ยวข้องขององค์กรที่ได้กำหนดไว้

2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุมและตรวจสอบการใช้งานหรือการถ่ายโอนข้อมูลไปยังสื่อบันทึกข้อมูลอย่างสม่ำเสมอ รวมทั้งการนำสื่อบันทึกข้อมูลออกนอกองค์กร

3) ในการรักษาความลับและความสมบูรณ์ของข้อมูลบนสื่อบันทึก บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องพิจารณาการใช้เทคนิคการเข้ารหัสตามระดับชั้นความลับและความเสี่ยงที่มีต่อข้อมูล เพื่อปกป้องข้อมูลที่สำคัญขององค์กรจากภัยคุกคามและความเสี่ยงที่อาจเกิดขึ้น

4) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องจัดเก็บสื่อบันทึกข้อมูลให้อยู่ในสภาพแวดล้อมที่มั่นคงปลอดภัยและเหมาะสมตามระดับชั้นความลับของข้อมูล โดยป้องกันจากภัยคุกคามต่อสิ่งแวดล้อม เช่น ความร้อน ความชื้น สนามไฟฟ้า เป็นต้น ตลอดจนจัดเก็บให้สอดคล้องตามข้อกำหนดของผู้ผลิตอุปกรณ์คอมพิวเตอร์นั้น ๆ

5) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องป้องกันการเข้าถึงสื่อบันทึกข้อมูลโดยไม่ได้รับอนุญาตและป้องกันการนำไปใช้งานผิดวัตถุประสงค์ รวมทั้งป้องกันการเกิดความเสียหายต่อข้อมูลสารสนเทศในระหว่างการจัดส่งสื่อบันทึกข้อมูลออกนอกองค์กร

6) หากจำเป็นต้องใช้สื่อบันทึกข้อมูลที่มีข้อมูลที่เป็นความลับซ้ำภายในองค์กร บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องดำเนินการลบหรือทำลายข้อมูลอย่างปลอดภัยตามระดับชั้นความลับของข้อมูลก่อนที่จะนำมาใช้งานใหม่

7) เมื่อหมดความจำเป็นในการใช้งานสื่อบันทึกข้อมูล หรือสื่อบันทึกข้อมูลมีการเสื่อมสภาพการใช้งาน บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องดำเนินการขออนุญาตทำลายสื่อบันทึกข้อมูลดังกล่าวให้เป็นไปตามระดับชั้นความลับและการจัดการกับข้อมูลสารสนเทศตามที่องค์กรกำหนด และต้องจัดเก็บบันทึกหลักฐานการลบทำลายไว้สำหรับการตรวจสอบ

9.4 มาตรการควบคุมด้านเทคโนโลยี (Technological controls)

9.4.1 อุปกรณ์ระดับผู้ใช้งาน (User endpoint devices)

<u>วัตถุประสงค์</u>

เพื่อปกป้องข้อมูลจากความเสี่ยงที่เกิดขึ้นจากการใช้อุปกรณ์ปลายทางของผู้ใช้งาน

<u>แนวปฏิบัติ</u>

บททั่วไปและความรับผิดชอบของผู้ใช้งาน

1) ผู้ใช้งานต้องรับทราบข้อกำหนดและนโยบายการใช้ระบบเทคโนโลยีสารสนเทศเพื่อความมั่นคงปลอดภัยสำหรับผู้ใช้งาน สำหรับการปกป้องอุปกรณ์ปลายทางของผู้ใช้งาน ตลอดจนความรับผิดชอบในการใช้มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว เช่น ผู้ใช้งานต้องออกจากระบบสารสนเทศ และล็อคหน้าจอคอมพิวเตอร์ทุกครั้งเมื่อไม่ได้ใช้งาน หลีกเลี่ยงการเปิดอ่านข้อมูลที่เป็นความลับหากบุคคลอื่นสามารถอ่านได้จากด้านหลัง หรือใช้ตัวกรองหน้าจอความเป็นส่วนตัว เป็นต้น

2) ผู้ใช้งานมีหน้าที่ต้องรักษาความปลอดภัยของข้อมูลและเครื่องคอมพิวเตอร์ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ

3) ผู้ใช้งานต้องรับผิดชอบ ดูแล รักษาเครื่องคอมพิวเตอร์ โดยต้องระวังการสูญหายของตัวเครื่องและอุปกรณ์ต่อพ่วงอื่น ๆ รวมถึงการสูญหายของข้อมูลซึ่งจัดเก็บอยู่ภายในเครื่องคอมพิวเตอร์

4) ผู้ใช้งานต้องไม่ละทิ้งข้อมูลคอมพิวเตอร์ที่สำคัญ เช่น เอกสารกระดาษ หรือสื่อบันทึกข้อมูล ให้อยู่ในสถานที่ที่ไม่ปลอดภัย พื้นที่สาธารณะ หรือสถานที่ที่พบเห็นได้โดยง่าย ผู้ใช้งานต้องจัดเก็บข้อมูลคอมพิวเตอร์ในสถานที่ที่เหมาะสม รวมถึงมีการป้องกันเพื่อให้ยากต่อการเข้าถึงจากผู้ไม่มีสิทธิ์

5) บุคลากรงานวิจัยและพัฒนาระบบงานดิจิทัลต้องกำหนดให้มีการติดตั้งระบบที่สามารถระบุตัวตน พิสูจน์ตัวตน กำหนดสิทธิการใช้งาน กำหนดสิทธิในการเข้าถึงข้อมูลสารสนเทศ กำหนดสิ่งแวดล้อมการใช้งานเครื่องของผู้ใช้งาน (User Profile) เพื่อให้องค์กรสามารถลบข้อมูลจากระยะไกลได้ในกรณีที่ถูกขโมยหรืออุปกรณ์สูญหาย

<u>การนำอุปกรณ์ส่วนตัวมาใช้ในงานขององค์กร (BYOD)</u>

ผู้ที่นำคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์แบบพกพาส่วนบุคคล เช่น Notebook โทรศัพท์มือถือและแท็บเล็ต เป็นต้น เข้ามาใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร จะต้องปฏิบัติตามดังต่อไปนี้

1) ผู้ใช้งานต้องดำเนินการร้องขออนุญาตการใช้งานคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์แบบพกพาส่วนบุคคล โดยดำเนินการร้องขอกับบุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลผ่านแบบฟอร์มคำขอใช้อุปกรณ์เคลื่อนที่ส่วนบุคคลในการปฏิบัติงานตามช่องทางที่องค์กรกำหนด

2) ผู้ใช้งานสามารเข้าถึงระบบสารสนเทศตามสิทธิในการเข้าถึงระบบสารสนเทศที่กำหนดไว้เท่านั้น ในกรณีที่ผู้ใช้งานต้องการเข้าถึงระบบสารสนเทศเกินกว่าสิทธิที่ได้รับ ให้ดำเนินการกรอกแบบฟอร์มลงทะเบียน เปลี่ยนแปลง และยกเลิกสิทธิผู้ใช้งานระบบโดยให้ผู้บังคับบัญชาเป็นผู้พิจารณาอนุมัติ

3) ผู้ใช้งานต้องพิสูจน์ตัวตนในการเข้าถึงระบบสารสนเทศ หรือการเข้าถึงเครือข่ายภายในขององค์กร

4) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องดำเนินการติดตั้งซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดีในคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์แบบพกพาส่วนบุคคลของผู้ใช้งาน

5) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องตรวจสอบการติดตั้งซอฟต์แวร์อันตรายที่ติดตั้งภายในคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์แบบพกพาส่วนบุคคลของผู้ใช้งาน ก่อนการอนุญาตให้ใช้งาน ถ้าพบซอฟต์แวร์อันตราย บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลจะดำเนินการถอดถอนซอฟต์แวร์ออกจากคอมพิวเตอร์ของผู้ใช้งาน หรือถอดถอนสิทธิการใช้งานคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์แบบพกพาส่วนบุคคลเครื่องนั้น

6) ผู้ใช้งานต้องติดตั้งโปรแกรมในอุปกรณ์คอมพิวเตอร์ตามที่องค์กรอนุญาตให้ใช้งานเท่านั้น หากต้องการติดตั้งโปรแกรมที่นอกเหนือจากที่องค์กรอนุญาตจะต้องทำการร้องขอกับบุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลอย่างชัดเจน เป็นลายลักษณ์อักษร

7) ผู้ใช้งานต้องตั้งรหัสผ่านและล็อคหน้าจอทุกครั้งเมื่อไม่ใช้งานเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

8) ผู้ใช้งานต้องออกจากระบบและล็อคหน้าจอทุกครั้งเมื่อไม่ใช้งาน

9) ในการรับส่งข้อมูลสำคัญผ่านระบบเครือข่าย ผู้ใช้งานต้องดำเนินการเข้ารหัสข้อมูลที่เป็นมาตรฐานสากล เช่น SSL หรือ XML Encryption เป็นต้น

10) ผู้ใช้งานจะต้องไม่นำอุปกรณ์คอมพิวเตอร์แบบพกพาวางทิ้งไว้ในพื้นที่สาธารณะ เพื่อป้องกันการสูญหาย

11) เมื่ออุปกรณ์คอมพิวเตอร์แบบพกพาของผู้ใช้งานสูญหายจะต้องดำเนินการแจ้งให้บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลรับทราบภายใน 24 ชั่วโมง ผ่านช่องทางที่องค์กรกำหนด

12) เมื่อผู้ใช้งานต้องการยกเลิกการใช้งาน หรือลาออก บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลจะต้องดำเนินการลบข้อมูลที่เป็นความลับออกจากคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์แบบพกพาของผู้ใช้งาน

13) เมื่อผู้ใช้งานเจอเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศให้ดำเนินการแจ้งบุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลทางช่องทางที่องค์กรกำหนด เพื่อให้เจ้าหน้าที่ฯ ดำเนินการประเมินความเร่งด่วนของเหตุการณ์และจัดการกับเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น

14) องค์กรไม่อนุญาตให้นำอุปกรณ์คอมพิวเตอร์แบบพกพาในรูปแบบ Rooted (Android) หรือ jailbroken (iOS) เข้าถึงเครือข่ายและระบบสารสนเทศขององค์กร

15) องค์กรขอสงวนสิทธิ์ให้บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลดำเนินการตรวจสอบคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์แบบพกพาของผู้ใช้งาน และตัดสิทธิ์การใช้งานเมื่อพบเจอสิ่งผิดปกติ

16) กรณีที่ต้องเข้าถึงข้อมูลหรือระบบจากระยะไกล (Teleworking) ผู้ใช้งานต้องปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่องค์กรกำหนด

17) ในการใช้บริการเว็บไซต์และเว็บแอปพลิเคชั่นต่าง ๆ ผู้ใช้งานต้องระมัดระวังในการใช้งาน และเข้าใช้งานในแหล่งที่ปลอดภัย น่าเชื่อถือ เพื่อป้องกันความปลอดภัยของสารสนเทศ

<u>การเชื่อมต่อแบบไร้สาย (Wireless connections)</u>

1) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดค่าการเชื่อมต่อไร้สายบนอุปกรณ์ให้มีความมั่นคงปลอดภัยตามมาตรฐานขั้นต่ำที่องค์กรกำหนด เพื่อป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต และลดความเสี่ยงจากการโจมตีเครือข่าย เช่น การเปลี่ยนค่าตั้งต้นของระบบ (Default) เช่น SSID, Username, Password และ SNMP Community String การปิดการใช้งาน Service ที่ไม่จำเป็น เช่น SNMP, Telnet และการใช้เทคนิคการเข้ารหัสที่ปลอดภัยหรือการตั้งค่าความปลอดภัยที่เหมาะสม เช่น WPA2-PSK, WPA2 Enterprise เป็นต้น

2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลควรสแกนหา Access Point (AP) แปลกปลอมที่ไม่ได้รับอนุญาตให้ติดตั้ง เพื่อป้องกันไม่ให้ผู้บุกรุกใช้ AP เหล่านี้เป็นช่องทางในการเข้าถึงเครือข่ายภายในขององค์กร

9.4.2 สิทธิพิเศษในการเข้าถึงและการจำกัดการเข้าถึงข้อมูล (Privileged access rights)

<u>วัตถุประสงค์</u>

เพื่อกำหนดการบริหารจัดการสิทธิพิเศษในการเข้าถึงและการจำกัดการเข้าถึงข้อมูล ระบบเครือข่าย ระบบปฏิบัติการ และแอปพลิเคชันขององค์กร เพื่อป้องกันการเข้าถึงหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต หรือได้รับสิทธิพิเศษเกินกว่าหน้าที่รับผิดชอบ

<u>แนวปฏิบัติ</u>

1) องค์กรต้องกำหนดขั้นตอนปฏิบัติสำหรับการใช้งานสิทธิจำเพาะ หรือสิทธิพิเศษอย่างเป็นลายลักษณ์อักษร อาทิ สิทธิสูงสุดในการเข้าถึงระบบหรือข้อมูล และสิทธิที่เข้าถึงระบบหรือข้อมูลได้มากกว่าหน้าที่รับผิดชอบ ทั้งนี้ การให้สิทธิดังกล่าวต้องจัดสรรอย่างจำกัดและอยู่ภายใต้การควบคุมอย่างเคร่งครัด โดยการให้สิทธิดังกล่าวควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง
2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดรายชื่อและฟังก์ชันการใช้งาน โดยต้องระบุสิทธิสูงหรือสิทธิพิเศษในการเข้าถึงระบบให้เป็นไปตามความจำเป็นและหน้าที่ความรับผิดชอบ รวมทั้งต้องกำหนดสิทธิการใช้งานและจัดทำตารางสิทธิการใช้งานตามที่เจ้าของข้อมูลกำหนด โดยบัญชีผู้ใช้งานที่มีสิทธิสูงหรือสิทธิพิเศษที่สามารถบริหารจัดการระบบได้ทั้งหมด (Administrator accounts) ควรใช้เฉพาะสำหรับการบริหารจัดการระบบเท่านั้น และไม่ควรใช้สำหรับการปฏิบัติงานทั่วไปประจำวัน
3) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดสิทธิสูงสำหรับบัญชีผู้ใช้งานในการเข้าถึงระบบสารสนเทศตามความจำเป็นและความรับผิดชอบ รวมทั้งต้องระบุช่วงเวลาที่อนุญาตให้ใช้สิทธิสูงตามความเหมาะสม
4) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องเปลี่ยนรหัสผ่านทุกครั้งภายหลังจากผู้ที่ได้รับอนุญาตเข้าถึงระบบสารสนเทศ เสร็จสิ้นการใช้งานบัญชีผู้ใช้งานที่มีสิทธิสูงดังกล่าว
5) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องมีการบันทึก จัดเก็บหลักฐานในการขอใช้สิทธิระดับสูง เพื่อการทบทวนและตรวจสอบสิทธิดังกล่าว

9.4.3 การพิสูจน์ตัวตนอย่างมั่นคงปลอดภัย (Secure authentication)

<u>วัตถุประสงค์</u>

เพื่อให้มั่นใจว่าองค์กรมีการกำหนดการพิสูจน์ตัวตนอย่างมั่นคงปลอดภัย เมื่อมีการขอเข้าถึงระบบสารสนเทศขององค์กร ตลอดจนมีการจัดทำขั้นตอนปฏิบัติที่จำเป็นต่อการดำเนินงานในการควบคุมการเข้าถึงระบบ

<u>แนวปฏิบัติ</u>

1) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องติดตั้งและกำหนดการตั้งค่าของระบบปฏิบัติการและแอปพลิเคชันตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยจัดให้มีการพิสูจน์ตัวตนและควบคุมการเข้าถึงระบบเฉพาะผู้ที่ได้รับอนุญาตตามช่วงเวลาที่กำหนด
2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องพิจารณาการใช้วิธีพิสูจน์ตัวตนที่ซับซ้อนมากขึ้นสำหรับการเข้าใช้งานบัญชีสิทธิสูงหรือสิทธิพิเศษ รวมถึงการเข้าถึงหน้าผู้บริหารจัดการระบบ (Administrator Page) สำหรับระบบสารสนเทศที่มีความสำคัญ เช่น การพิสูจน์ตัวตนแบบ Multi-Factor Authentication เป็นต้น
3) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดให้ระบบหรือแอปพลิเคชันไม่แสดงข้อมูลรายละเอียดสำคัญของระบบหรือแอปพลิเคชัน หรือข้อความช่วยเหลือในระหว่างขั้นตอนการเข้าสู่ระบบ (เช่น หากเกิดข้อผิดพลาดขึ้น ระบบไม่ควรระบุว่าส่วนใดของข้อมูลถูกต้องหรือไม่ถูกต้อง) เพื่อหลีกเลี่ยงการให้ความช่วยเหลือในการพยายามเข้าถึงระบบโดยผู้ไม่ประสงค์ดีหรือผู้ที่ไม่ได้รับอนุญาต รวมถึงต้องยกเลิกสิทธิในการเข้าถึงระบบทันที เมื่อสงสัยว่ามีการเข้าสู่ระบบโดยไม่ได้รับอนุญาตหรือไม่เหมาะสม และต้องมีการบันทึกกิจกรรมการเข้าถึงระบบทั้งในกรณีที่สำเร็จและไม่สำเร็จ
4) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดมาตรการควบคุมการส่งผ่านข้อมูลรหัสผ่านที่ปลอดภัย โดยจะต้องไม่ส่งรหัสผ่านที่เป็นข้อความธรรมดาผ่านเครือข่ายเพื่อหลีกเลี่ยงการถูกจับโดยโปรแกรม "sniffer" ของเครือข่าย
5) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องจำกัดระยะเวลาการเชื่อมต่อระบบเพื่อเพิ่มความปลอดภัยให้กับแอปพลิเคชันที่มีความเสี่ยงสูง และลดโอกาสการเข้าถึงระบบโดยไม่ได้รับอนุญาต

6) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องจัดทำ จัดเก็บ และปรับปรุงคู่มือการปฏิบัติงานที่จำเป็นต่อการติดตั้ง บันทึกค่าการติดตั้ง รวมถึงต้องสำรองข้อมูลระบบปฏิบัติการให้เป็นปัจจุบัน และเก็บไว้ในที่ที่สามารถเข้าถึงได้โดยสะดวกเมื่อจำเป็น หรือต้องกู้คืนระบบปฏิบัติการ

7) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดสิทธิในการเข้าถึงไฟล์และไดเรกทอรี่ที่สำคัญของระบบปฏิบัติการ โดยอนุญาตเฉพาะบัญชีผู้ใช้งานที่ได้รับอนุญาตเท่านั้น

9.4.4 ความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (Operations security)

<u>วัตถุประสงค์</u>

เพื่อควบคุม กำกับ ติดตามการปฏิบัติงานประจำของบุคลากรที่เกี่ยวข้องกับระบบคอมพิวเตอร์ และระบบเครือข่ายที่ให้บริการระบบคอมพิวเตอร์ขององค์กร ได้แก่ การติดตามการทำงานของระบบ (Monitoring) การจัดการปัญหาที่เกิดกับระบบ และการจัดทำรายงานการปฏิบัติงานที่เกี่ยวข้อง เพื่อให้การปฏิบัติงานด้านเทคโนโลยีสารสนเทศเป็นไปอย่างถูกต้อง และไม่เกิดผลกระทบด้านความมั่นคงปลอดภัยต่อระบบและข้อมูลคอมพิวเตอร์

<u>แนวปฏิบัติ</u>

1) การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Operational procedures and responsibilities)

1.1) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดให้มีการจัดทำขั้นตอนหรือวิธีปฏิบัติงานประจำในด้านต่าง ๆ ที่สำคัญ รวมทั้งดำเนินการทบทวนและปรับปรุงขั้นตอนหรือวิธีการปฏิบัติงานให้เป็นปัจจุบันอยู่เสมอ เพื่อให้บุคลากรสามารถนำไปปฏิบัติได้

1.2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุม กำกับให้มีการจัดการควบคุมการเปลี่ยนแปลงของระบบคอมพิวเตอร์อย่างเป็นทางการ โดยกำหนดวิธีปฏิบัติที่เป็นลายลักษณ์อักษร โดยครอบคลุมขั้นตอนการขออนุมัติจากผู้มีอำนาจ การประเมินผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง การทดสอบเพื่อให้มั่นใจว่าการเปลี่ยนแปลงดังกล่าวเป็นไปตามความต้องการของผู้ร้องขอหรือไม่ เป็นต้น

1.3) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องติดตามผลการใช้งานทรัพยากรสารสนเทศ (Capacity) และวางแผนด้านทรัพยากรสารสนเทศให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม

1.4) บุคลากรงานวิจัยและพัฒนาระบบงานดิจิทัลต้องจัดให้มีการแบ่งแยกระบบคอมพิวเตอร์สำหรับการพัฒนา ทดสอบ และใช้งานจริงออกจากกัน โดยการแบ่งแยกระบบดังกล่าวอาจใช้เครื่องคอมพิวเตอร์คนละเครื่องหรือแบ่งโดยการจัดเนื้อที่แยกไว้ต่างหากภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้ เพื่อลดความเสี่ยงในการเข้าใช้งานหรือการเปลี่ยนแปลงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต

2) การป้องกันภัยคุกคามจากโปรแกรมไม่พึงประสงค์ (Protection from malware)

2.1) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้คืนระบบเพื่อป้องกันทรัพย์สินจากซอฟต์แวร์ไม่พึงประสงค์

2.2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องจัดให้มีการติดตั้งซอฟต์แวร์ตรวจสอบโปรแกรมไม่พึงประสงค์ (Antivirus) และปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ พร้อมทั้งกำหนดผู้มีหน้าที่รับผิดชอบให้รายงานและแก้ไขปัญหากรณีพบภัยคุกคาม

2.3) สิทธิ์การเข้าถึงระดับผู้ดูแลระบบ (Administrative Access) บนอุปกรณ์ปลายทางต้องจำกัดเฉพาะบุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลหรือผู้ดูแลระบบเท่านั้น ผู้ใช้งานทั่วไปไม่ควรสามารถแก้ไขการตั้งค่าความปลอดภัย ปิดการทำงานของโปรแกรมป้องกันไวรัส หรือถอนการติดตั้งซอฟต์แวร์ป้องกันได้

2.4) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องตรวจสอบซอฟต์แวร์บนเครื่องคอมพิวเตอร์แม่ข่าย เพื่อป้องกันการติดตั้งหรือเปลี่ยนแปลงที่ไม่ได้รับอนุญาต

2.5) หากมีระบบสารสนเทศ หรืออุปกรณ์ปลายทางใดถูกใช้งานโดยไม่มีซอฟต์แวร์ป้องกันมัลแวร์ (ไม่ว่าจะเนื่องมาจากข้อจำกัดในการปฏิบัติงาน กรณีการใช้งานเฉพาะทาง หรือเหตุผลอื่น ๆ) จะต้องมีการดำเนินมาตรการรักษาความปลอดภัยอื่น ๆ ทดแทน เพื่อบรรเทาความเสี่ยงจากการติดมัลแวร์และให้มั่นใจว่าระบบยังคงปลอดภัย

3) การสำรองข้อมูล (Backup)

3.1) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องจัดให้มีการสำรองข้อมูลสำคัญ รวมถึงระบบปฏิบัติการ (Operating system) แอปพลิเคชันระบบงานคอมพิวเตอร์ (Application system) และชุดคำสั่งที่ใช้ปฏิบัติงานให้ครบถ้วนให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง

3.2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องทดสอบอุปกรณ์บันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

3.3) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องจัดให้มีการทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง เพื่อตรวจสอบว่าข้อมูลยังคงสามารถใช้งานได้ตามปกติ

3.4) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลและเจ้าของข้อมูลต้องกำหนดเป้าหมายในการกู้คืนข้อมูล เช่น กำหนดประเภทของข้อมูล และชุดข้อมูลล่าสุดที่จะกู้คืนได้ (Recovery point objective : RPO) เพื่อให้ข้อมูลสามารถพร้อมใช้งานได้ตามความต้องการของการดำเนินงาน

4) การตั้งค่าเวลาระบบ (Time synchronization)

4.1) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดให้มีการตั้งค่าระบบเวลาของระบบคอมพิวเตอร์และระบบเครือข่ายที่ใช้ในองค์กร หรือในขอบเขตที่องค์กรต้องรับผิดชอบดูแลด้านความมั่นคงปลอดภัยสารสนเทศ โดยต้องกำหนดให้มีการตั้งค่าการเชื่อมต่อเวลา (Time synchronization) จากแหล่งเวลาที่เชื่อถือได้ ทั้งกรณีที่อุปกรณ์ไม่สามารถตั้งการเชื่อมต่อเวลาจากแหล่งเวลาที่เชื่อถือได้โดยอัตโนมัติ ให้บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลกำหนดรอบการตรวจสอบ และปรับปรุงการตั้งค่าให้เป็นปัจจุบันเสมอ

5) การควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน (Installation of software on operational systems)

5.1) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดขั้นตอนควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน และมีมาตรการจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งาน เพื่อให้ระบบปฏิบัติงานต่าง ๆ มีความถูกต้องครบถ้วนและน่าเชื่อถือ

5.2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลควรกำหนดรายการซอฟต์แวร์มาตรฐาน (Software Standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ขององค์กร เพื่อใช้ในการควบคุมการติดตั้งซอฟต์แวร์ และปรับปรุงให้เป็นปัจจุบันเสมอ

5.3) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดและควบคุมให้ผู้ใช้งานติดตั้งเฉพาะซอฟต์แวร์ที่ได้รับอนุญาต เพื่อป้องกันการติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ในเครื่องคอมพิวเตอร์ขององค์กร

6) การบริหารจัดการช่องโหว่ทางเทคนิค (Technical vulnerability management)

6.1) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุมให้ระบบคอมพิวเตอร์ขององค์กร ได้รับการพิสูจน์ถึงช่องโหว่ทางเทคนิคซึ่งอาจเกิดขึ้นได้ โดยให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) จัดให้มีการทดสอบการเจาะระบบ (Penetration test) กับระบบงานที่มีความสำคัญหรือเป็นระบบที่มีการเชื่อมต่อกับระบบอินเทอร์เน็ต ซึ่งอาจมีความเสี่ยงต่อภัยคุกคามภายนอกสูง อย่างน้อยทุก 3 ปี และเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ

(2) จัดให้มีการประเมินช่องโหว่ของระบบ (Vulnerability Assessment) กับระบบงานที่มีความสำคัญหรือเป็นระบบที่มีการเชื่อมต่อกับระบบอินเทอร์เน็ต อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ และรายงานผลไปยังผู้บริหารที่เกี่ยวข้องเพื่อให้รับทราบและหาแนวทางการแก้ไขและป้องกัน

6.2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุมให้ระบบคอมพิวเตอร์ขององค์กรได้รับการพิสูจน์ถึงช่องโหว่ทางเทคนิคซึ่งอาจเกิดขึ้นตามนโยบายที่องค์กรกำหนดไว้ และมีมาตรการดำเนินการเพื่อปิดช่องโหว่หรือกำหนดแผนรองรับกรณีที่ระบบถูกบุกรุกผ่านช่องโหว่ โดยครอบคลุมแนวทางดำเนินการดังนี้

(1) กำหนดผู้มีหน้าที่รับผิดชอบในการดำเนินการเพื่อปิดช่องโหว่ (Patching) และการประสานงานกับบุคคลที่เกี่ยวข้อง และการประเมินความเสี่ยงของทรัพย์สินสารสนเทศที่เกี่ยวข้องซึ่งอาจได้รับผลกระทบจากช่องโหว่ดังกล่าว

(2) ปิดช่องโหว่ที่พบโดยไม่เร็ว โดยควรมีการประเมินความเสี่ยงของโปรแกรม และทดสอบโปรแกรมที่ใช้ในการปิดช่องโหว่ (Patches) ก่อนการติดตั้งโปรแกรมจริง เพื่อป้องกันผลกระทบที่อาจเกิดจากการติดตั้งโปรแกรมดังกล่าว ทั้งนี้ กรณีที่ไม่มีโปรแกรมเพื่อปิดช่องโหว่ให้ปฏิบัติตามคำแนะนำขององค์กรผู้ผลิตทรัพย์สินสารสนเทศที่เกี่ยวข้อง

(3) กระบวนการจัดการช่องโหว่ด้านเทคนิคควรสอดคล้องกับกระบวนการจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ (Incident management) ที่กำหนดไว้ เพื่อเตรียมความพร้อมรองรับกรณีที่ระบบถูก

บุกรุกผ่านช่องโหว่ ทั้งนี้ ให้รวมถึงกรณีที่ตรวจพบช่องโหว่แต่ยังไม่สามารถหาวิธีปิดช่องโหว่ได้

(4) บันทึกและจัดเก็บหลักฐานในการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับการจัดการช่องโหว่ทางเทคนิค โดยกรณีที่ใช้วิธีปรับปรุงโปรแกรมเพื่อปิดช่องโหว่แบบอัตโนมัติ (Automatic patching) สำหรับระบบหรืออุปกรณ์ใด ๆ ที่พิจารณาแล้วว่าไม่สร้างความเสียหายต่อระบบงาน ผู้รับผิดชอบในการดำเนินงานสามารถงดเว้นการบันทึกและจัดเก็บหลักฐานสำหรับการ Patching ระบบหรืออุปกรณ์นั้นได้

6.3) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลควรมีการติดตามข้อมูลข่าวสารเกี่ยวกับช่องโหว่ทางเทคนิคที่อาจเป็นความเสี่ยงต่อระบบคอมพิวเตอร์ขององค์กรอย่างทันต่อเหตุการณ์

7) การตรวจสอบระบบคอมพิวเตอร์ (Information systems audit)

7.1) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องจัดทำแผนการตรวจสอบระบบคอมพิวเตอร์ให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้ เช่น แผนการตรวจสอบช่องโหว่ของระบบคอมพิวเตอร์ (Vulnerability Assessment) เป็นต้น

7.2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องแจ้งให้หน่วยงานที่เกี่ยวข้องรับทราบก่อนดำเนินการตรวจสอบระบบคอมพิวเตอร์ทุกครั้ง

7.3) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดขอบเขตการตรวจสอบทางเทคนิค (Technical Audit Test) ให้ครอบคลุมจุดเสี่ยงที่สำคัญ และต้องควบคุมการตรวจสอบดังกล่าวไม่ให้กระทบต่อการปฏิบัติงานตามปกติ โดยกรณีที่การตรวจสอบระบบคอมพิวเตอร์มีโอกาสกระทบต่อความพร้อมใช้งานของระบบ (System Availability) ควรจัดให้มีการทดสอบนอกเวลาทำการ

7.4) การตรวจสอบระบบจะต้องดำเนินการโดยบุคลากรที่มีคุณสมบัติเหมาะสมและใช้เครื่องมือที่เหมาะสม เช่น เครื่องมือสแกนช่องโหว่ (vulnerability scanners) และการตรวจสอบควรดำเนินการทั้งจากภายนอก (ผ่านทางอินเทอร์เน็ต) และจากภายใน (ภายในเครือข่าย)

9.4.5 การจัดการการตั้งค่าระบบ (Configuration management)

<u>วัตถุประสงค์</u>

เพื่อให้มั่นใจว่าองค์ประกอบ รวมถึงความมั่นคงปลอดภัยขององค์ประกอบของอุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ และอุปกรณ์เครือข่ายที่สำคัญต่อการให้บริการได้รับการกำหนดค่า และมีการควบคุมการเข้าถึงอย่างเหมาะสม และป้องกันการปรับแต่งแก้ไขระบบโดยไม่ได้รับอนุญาต

<u>แนวปฏิบัติ</u>

1) องค์กรควรมีการกำหนดแม่แบบมาตรฐานสำหรับการกำหนดค่าฮาร์ดแวร์ ซอฟต์แวร์ บริการ และเครือข่ายอย่างปลอดภัย โดยพิจารณาจากระดับการป้องกันเพื่อกำหนดระดับความปลอดภัยที่เหมาะสม รวมทั้งแม่แบบมาตรฐานดังกล่าวควรได้รับการทบทวนอย่างสม่ำเสมอ และมีการปรับปรุงให้สอดคล้องกับภัยคุกคามหรือช่องโหว่ใหม่ ๆ หรือเมื่อมีการเปิดตัวซอฟต์แวร์หรือฮาร์ดแวร์เวอร์ชันใหม่
2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดการตั้งค่าอุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ และอุปกรณ์เครือข่าย ตามแม่แบบมาตรฐานที่กำหนดไว้ โดยอย่างน้อยให้ครอบคลุมในเรื่องดังต่อไปนี้
    2.1) การจำกัดสิทธิการเข้าถึงในระดับพิเศษหรือระดับบุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัล
    2.2) การปิดการใช้งานบัญชีผู้ใช้งานที่ไม่จำเป็น ไม่ได้ใช้ หรือไม่ปลอดภัย
    2.3) การปิดการใช้งานหรือจำกัดฟังก์ชันและบริการที่ไม่จำเป็น
    2.4) การจำกัดการเข้าถึงโปรแกรมอรรถประโยชน์และการตั้งค่าพารามิเตอร์ของระบบ
    2.5) การตั้งค่าการเชื่อมต่อเวลา (Time synchronization) จากแหล่งเวลาที่เชื่อถือได้
    2.6) การปรับเปลี่ยนข้อมูลการตั้งค่าเริ่มต้นของอุปกรณ์หรือระบบจากผู้ผลิต เช่น การเปลี่ยนรหัสผ่านตั้งต้นทันทีหลังจากการติดตั้ง และการตรวจสอบพารามิเตอร์ที่เกี่ยวข้องกับความปลอดภัยเริ่มต้นที่สำคัญ
    2.7) การกำหนดระยะเวลาการตัดการใช้งานระบบคอมพิวเตอร์ หากไม่มีการใช้งานติดต่อกันภายในระยะเวลาที่กำหนด (Idle Time-Out)

3) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องบันทึกการเปลี่ยนแปลงการกำหนดค่าอุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ และอุปกรณ์เครือข่าย และจัดเก็บหลักฐานการเปลี่ยนแปลงให้สอดคล้องกับกระบวนการบริหารจัดการการเปลี่ยนแปลง ดังนี้

3.1) เจ้าของทรัพย์สินหรือข้อมูลการติดต่อ

3.2) วันที่ที่มีการเปลี่ยนแปลงการตั้งค่า

3.3) เวอร์ชันที่มีการตั้งค่า

3.4) อุปกรณ์อื่นที่เกี่ยวข้องกับการตั้งค่า

4) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลควรมีการทบทวนการตั้งค่าอุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ และอุปกรณ์เครือข่ายเป็นประจำทุกปี เพื่อตรวจสอบความถูกต้องครบถ้วนของการตั้งค่าอุปกรณ์ให้เป็นไปตามแม่แบบมาตรฐานที่กำหนดไว้

9.4.6 การบริหารจัดการข้อมูล (Data management)

<u>วัตถุประสงค์</u>

เพื่อให้มั่นใจว่าข้อมูลที่มีการจัดเก็บไว้บนระบบ อุปกรณ์ หรือสื่อบันทึกข้อมูลต่าง ๆ ได้รับการลบทำลายเมื่อหมดความจำเป็นต่อการใช้งาน หรือมีการปิดบังข้อมูล ตลอดจนการป้องกันข้อมูลรั่วไหลออกนอกองค์กร

<u>แนวปฏิบัติ</u>

องค์กรกำหนดให้มีแนวทางในการจัดการและจัดเก็บข้อมูลเพื่อป้องกันการเข้าถึงและใช้ข้อมูลโดยไม่ได้รับอนุญาตตามแนวทางดังต่อไปนี้

1) กำหนดให้มีนโยบายและมาตรการจัดการและจัดเก็บข้อมูลเป็นลายลักษณ์อักษรที่สอดคล้องกับกฎหมายและหลักเกณฑ์การจัดเก็บข้อมูลที่หน่วยงานกำกับดูแล โดยจำแนกประเภทของข้อมูลเพื่อกำหนดมาตรการเฉพาะและประเมินความเสี่ยง รวมถึงผลกระทบต่อองค์กรหากมีการสูญเสียดังกล่าว พร้อมจัดให้มีการอบรมแก่บุคลากรทุกคนขององค์กร

2) กำหนดให้มีการจัดระดับความปลอดภัยสำหรับการจัดการและจัดเก็บข้อมูลโดยพิจารณาจากประเภทและระดับความลับของข้อมูล เมื่อจัดระดับแล้วให้กำหนดมาตรการเฉพาะสำหรับข้อมูลแต่ละระดับ และเงื่อนไขหรือข้อกำหนดที่บุคคลผู้ได้รับอนุญาตต้องปฏิบัติตามก่อนเข้าถึง

หรือใช้ข้อมูลโดยสอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร

3) กำหนดให้ทุกฝ่ายต้องจัดทำทะเบียนข้อมูลโดยแบ่งตามประเภทและระดับความลับของข้อมูล

4) กำหนดผู้มีหน้าที่รับผิดชอบข้อมูลแต่ละประเภทอย่างชัดเจนโดยพิจารณาจากการได้รับ การสร้าง และความจำเป็นในการใช้ข้อมูล (“เจ้าของข้อมูล”) โดยเจ้าของข้อมูลต้องกำหนดมาตรการเฉพาะเพื่อการจัดเก็บ การป้องกัน การสำรองข้อมูล การทำลาย และการตรวจสอบการเข้าถึงหรือใช้ข้อมูลภายใต้การกำกับดูแลของตนอย่างเหมาะสมและสอดคล้องกับระดับความลับของข้อมูล เช่น กรณีข้อมูลความลับเฉพาะต้องจัดให้มีการใส่รหัสผ่าน หรือการเข้ารหัสข้อมูล เป็นต้น ทั้งนี้ ให้มาตรการดังกล่าวต้องเป็นไปในแนวทางเดียวกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร

5) กำหนดบุคคลที่มีสิทธิเข้าถึงและใช้ข้อมูล เงื่อนไขของสิทธิ และการระงับซึ่งสิทธิให้ชัดเจนโดยเฉพาะข้อมูลที่เป็นความลับ เช่น สิทธิให้อ่านข้อมูลอย่างเดียว สิทธิในการสร้างและแก้ไขข้อมูล เป็นต้น

6) กำหนดให้มีการจัดเก็บและการสำรองข้อมูลแต่ละประเภทอย่างสม่ำเสมอ โดยกำหนดให้มีระยะเวลาและวิธีการในการจัดเก็บและสำรองข้อมูลตามที่กฎหมาย ประกาศ ระเบียบ และข้อกำหนดของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

7) กำหนดให้มีมาตรการและขั้นตอนในการกำจัดหรือทำลายข้อมูลและเอกสารสำหรับกรณีข้อมูลพ้นระยะเวลาจัดเก็บหรือไม่สามารถใช้การได้อย่างชัดเจน เช่น กรณีเอกสารมีหน้าหลังว่างให้สามารถเอากลับมาใช้ทำสำเนาหรือพิมพ์เอกสารทั่วไปอีกครั้งได้ แต่ต้องคำนึงถึงประเภทและระดับความลับของเอกสารดังกล่าวโดยเอกสารที่สามารถนำมาใช้ซ้ำดังกล่าวได้ต้องเป็นข้อมูลที่มีระดับความลับเป็นข้อมูลทั่วไปเท่านั้น ข้อมูลใดที่มีระดับความลับสูงกว่าข้อมูลทั่วไป องค์กรกำหนดห้ามเผยแพร่และต้องทำลายด้วยวิธีที่องค์กรกำหนด เช่น การใช้เครื่องทำลาย การฉีกหรือขีดเครื่องหมายทำลายเอกสาร เป็นต้น ทั้งนี้ ให้พิจารณาให้ครอบคลุม ในเรื่องดังต่อไปนี้

    7.1)การเลือกวิธีการลบข้อมูล เช่น การเขียนทับข้อมูล

    7.2)บันทึกผลการลบข้อมูล

    7.3)กรณีใช้ผู้ให้บริการภายนอกในการลบข้อมูล ต้องมีหลักฐานในการลบข้อมูลดังกล่าว

7.4)หากมีการจัดเก็บข้อมูลโดยผู้ให้บริการภายนอกต้องมีข้อตกลงการประมวลผลเกี่ยวกับการลบข้อมูล

8) จัดให้มีข้อกำหนดเกี่ยวกับการเข้าถึงและการใช้ข้อมูลกรณีองค์กรใช้บริการของผู้ให้บริการภายนอก (Outsourcing) โดยต้องกำหนดและระบุประเภทข้อมูลที่ผู้ให้บริการภายนอกสามารถเข้าถึงได้ตามหลักความจำเป็นในการรู้ข้อมูล (Need to know basis) ตลอดจนกำหนดข้อตกลงเกี่ยวกับข้อมูลดังกล่าวและการรักษาความลับของข้อมูลตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ

9) สำหรับมาตรการในการจัดการและจัดเก็บข้อมูลส่วนบุคคลที่องค์กรได้รับจากการดำเนินการให้เป็นไปตามนโยบายคุ้มครองข้อมูลส่วนบุคคลขององค์กร (Personal Data Protection Policy) โดยบุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดมาตรการปิดบังข้อมูล จำกัดการเปิดเผยข้อมูลอ่อนไหว โดยอาจเลือกใช้เทคนิคการจัดทำเป็นข้อมูลนิรนาม (Anonymization) หรือการแฝงข้อมูล (Pseudonymisation)

10) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่สำคัญหรือที่เป็นความลับ เช่น ข้อมูลส่วนบุคคล เป็นต้น เพื่อป้องกันการรั่วไหลของข้อมูล และต้องจัดให้มีกระบวนการเฝ้าระวังเหตุการณ์ผิดปกติที่เกี่ยวข้องกับข้อมูลรั่วไหล ในกรณีที่เกิดเหตุการณ์ข้อมูลรั่วไหลต้องดำเนินการร่วมกับผู้ที่เกี่ยวข้องในการตรวจสอบและวิเคราะห์หาสาเหตุที่ทำให้เกิดข้อมูลรั่วไหล เพื่อให้สามารถแก้ไขปัญหาได้อย่างมีประสิทธิภาพและทันท่วงที

9.4.7 การบันทึกกิจกรรมและการเฝ้าติดตามกิจกรรม (Logging and monitoring activities)

<u>วัตถุประสงค์</u>

เพื่อตรวจจับการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต รวมทั้งเหตุการณ์ที่อาจก่อให้เกิดความเสียหาย หรือการหยุดชะงักของการดำเนินงาน

<u>แนวปฏิบัติ</u>

1) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุมให้มีการบันทึกหลักฐาน (Logs) ซึ่งบันทึกข้อมูลกิจกรรมการใช้งานของผู้ใช้งานระบบคอมพิวเตอร์และเหตุการณ์เกี่ยวกับความมั่นคง

ปลอดภัยต่าง ๆ โดยรายละเอียดการจัดเก็บบันทึกต้องสอดคล้องกับข้อกำหนดในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และฉบับปรับปรุง

2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุมให้มีการจัดเก็บบันทึกหลักฐานที่เกี่ยวข้องกับข้อผิดพลาดใด ๆ ของระบบคอมพิวเตอร์ มีการวิเคราะห์บันทึกหลักฐานดังกล่าวอย่างสม่ำเสมอ และมีการจัดการแก้ไขข้อผิดพลาดที่ตรวจพบอย่างเหมาะสม

3) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องตรวจสอบบันทึกหรือบันทึกเหตุการณ์ (event logs) อย่างสม่ำเสมอ เพื่อหาการละเมิดกฎเกณฑ์ หรือกิจกรรมที่น่าสงสัยหรืออาจก่อให้เกิดปัญหา ซึ่งอาจละเมิดต่อกฎหมายหรือข้อกำหนดขององค์กร

4) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดกระบวนการสำหรับการยกระดับเหตุการณ์ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัยขององค์กร ความเป็นส่วนตัวของข้อมูล หรือการดำเนินงาน ให้แก่บุคคลที่รับผิดชอบที่เกี่ยวข้องเพื่อดำเนินการอย่างเหมาะสมและทันท่วงที

5) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องป้องกันการแก้ไขเปลี่ยนแปลงบันทึกหลักฐานและจำกัดสิทธิการเข้าถึงบันทึกหลักฐาน เพื่อป้องกันการเข้าถึง หรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต เพื่อประโยชน์ในการสืบสวน สอบสวนในอนาคต และเพื่อการติดตามการควบคุมการเข้าถึง

6) เมื่อมีการใช้บริการสารสนเทศจากภายนอก เจ้าหน้าที่เทคโนโลยีต้องทำพิจารณาและประเมินฟังก์ชันหรือฟีเจอร์การติดตามตรวจสอบ (monitoring) ที่มีอยู่ในบริการนั้น เพื่อให้สามารถควบคุมและติดตามกิจกรรมในระบบได้อย่างเหมาะสม ตรวจจับภัยคุกคามด้านความมั่นคงปลอดภัย สนับสนุนการปฏิบัติตามข้อกำหนด และดำเนินการตอบสนองต่อเหตุการณ์ได้อย่างทันท่วงที

9.4.8 ความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications security)

<u>วัตถุประสงค์</u>

เพื่อป้องกันการกระทำที่มีความเสี่ยงต่อข้อมูลคอมพิวเตอร์ในระบบเครือข่ายคอมพิวเตอร์ และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายคอมพิวเตอร์ รวมถึงรักษาความมั่นคงปลอดภัยในการรับส่งข้อมูลคอมพิวเตอร์ผ่านระบบเครือข่ายภายในองค์กร และระหว่างระบบเครือข่ายภายในองค์กร กับระบบเครือข่ายภายนอก

<u>แนวปฏิบัติ</u>

1) การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ (Network Security Management)

1.1) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุม กำกับ กำหนดให้มีขั้นตอนการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ เพื่อป้องกันภัยคุกคาม และมีการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และแอปพลิเคชันที่ทำงานบนเครือข่ายคอมพิวเตอร์ รวมทั้งข้อมูลคอมพิวเตอร์ที่มีการแลกเปลี่ยนบนเครือข่าย

1.2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดให้มีการแบ่งแยกเครือข่ายขององค์กรตามกลุ่มของการบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบคอมพิวเตอร์ และทบทวนการแบ่งแยกเครือข่ายตามความเหมาะสม

1.3) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องเปิดพอร์ตสื่อสาร (Port) เท่าที่จำเป็นต้องใช้งานเท่านั้น โดยบุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องดำเนินการตรวจสอบพอร์ตสื่อสาร และปิดพอร์ตสื่อสารที่ไม่มีความจำเป็นในการใช้งานของระบบหรืออุปกรณ์ และกรณีที่จำเป็นต้องใช้งานพอร์ตสื่อสารจะต้องมีการยืนยันตัวตนทุกครั้งก่อนอนุญาตให้ใช้งาน

1.4) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์ และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

(1) จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ ได้แก่ ระบบอินเทอร์เน็ต และระบบอินทราเน็ต เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ เพื่อเข้าถึงระบบที่นอกเหนือจากที่ได้รับอนุญาตได้

(2) ควบคุมดูแลระบบเครือข่ายทั้งหมดขององค์กรที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกองค์กร โดยต้องเชื่อมต่อผ่านไฟร์วอลล์ และระบบตรวจจับและป้องกันการบุกรุกเท่านั้น

(3) จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงเกิดขึ้น

1.5) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องจัดให้มีการบันทึกและจัดเก็บหลักฐานที่ติดต่อกับระบบงานสำคัญและมีความเสี่ยงสูง เพื่อติดตามตรวจสอบการทำงานที่เกี่ยวข้องหรืออาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์

1.6) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องควบคุมการเข้าถึงเว็บไซต์ที่ไม่ปลอดภัยหรือจำกัดการเข้าถึงเว็บไซต์ที่มีความเสี่ยงต่อการถูกโจมตี เพื่อลดความเสี่ยงในการเข้าถึงเนื้อหาที่เป็นอันตรายและป้องกันระบบสารสนเทศจากการบุกรุกโดยมัลแวร์จากการเข้าถึงเว็บไซต์ดังกล่าว โดยให้บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลพิจารณาเว็บไซต์ที่ไม่ปลอดภัยตามประเภท ดังต่อไปนี้

(1) เว็บไซต์ที่มีฟังก์ชันการอัปโหลดข้อมูลโดยไม่ได้รับอนุญาต

(2) เว็บไซต์ที่ต้องสงสัยว่าเป็นอันตราย เช่น เว็บไซต์ที่เผยแพร่มัลแวร์หรือมีเนื้อหาล่อลวง (Phishing)

(3) เว็บไซต์ที่เป็นอันตรายซึ่งได้ข้อมูลมาจากการวิเคราะเชิงลึกด้านความมั่นคงปลอดภัยสารสนเทศ (Threat intelligence)

(4) เว็บไซต์ที่มีเนื้อหาผิดกฎหมาย

9.4.9 การควบคุมการเข้ารหัสข้อมูล (Cryptographic control)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการในการเข้ารหัสลับข้อมูล และกำหนดแนวทางการบริหารจัดการกุญแจ (Key) ที่ใช้เข้ารหัสลับข้อมูล ไม่ให้สูญเสียซึ่งความลับ และความถูกต้องสมบูรณ์ของข้อมูล

<u>แนวปฏิบัติ</u>

1) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลต้องกำหนดให้มีขั้นตอนในการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับ ดังนี้

1.1) กำหนดให้มีการจัดประเภทของข้อมูลและการสื่อสารที่จะต้องได้รับการเข้ารหัส

1.2) กำหนดให้มีการใช้โปรแกรมที่มีความสามารถในการเข้ารหัสข้อมูล เพื่อให้บุคลากรใช้เป็นมาตรฐานเดียวกัน โดยคำนึงถึงชนิด และขั้นตอนวิธีการเข้ารหัสข้อมูล (Algorithm) ที่สอดคล้องเหมาะสมกับระดับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูล ทั้งนี้ โปรแกรมจะต้องทำ

หน้าที่ในการเข้ารหัสข้อมูลอย่างเหมาะสม เมื่อมีการเชื่อมต่อผ่านระบบเครือข่ายภายในองค์กรไปยังเครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์เครือข่ายต่าง ๆ ขององค์กร หรือเมื่อมีการเชื่อมต่อจากเครือข่ายภายนอกองค์กร เข้ามายังเครือข่ายภายในองค์กร

2) บุคลากรงานโครงสร้างพื้นฐานระบบดิจิทัลควรกำหนดให้มีแนวทางการบริหารจัดการกุญแจ (Key) ที่ใช้เข้ารหัสข้อมูล เพื่อรองรับการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับขององค์กรอย่างเหมาะสม โดยควรให้มีการควบคุม กำกับ ติดตาม ให้ครอบคลุมตลอดทั้งวงจรในการนำกุญแจรหัสลับไปใช้งาน ได้แก่ การสร้างกุญแจรหัสลับ การจัดเก็บและดูแลรักษากุญแจรหัสลับ การนำกุญแจรหัสลับไปใช้ การกำหนดอายุของกุญแจรหัสลับ ตลอดจนการทำลายกุญแจรหัสลับเมื่อไม่ได้ใช้งาน

9.4.10 การจัดหา พัฒนา และบำรุงรักษาระบบคอมพิวเตอร์ (System acquisition, development and maintenance)

<u>วัตถุประสงค์</u>

เพื่อควบคุม กำกับ ติดตาม และกำหนดมาตรการสำหรับการพัฒนาหรือเปลี่ยนแปลงระบบคอมพิวเตอร์ เพื่อให้การดำเนินการระหว่างการพัฒนาหรือเปลี่ยนแปลงมีความถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน และมาตรการต้องครอบคลุมกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้น ซึ่งได้แก่ การร้องขอเพื่อดำเนินการ จนถึงการนำระบบงานที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง

<u>แนวปฏิบัติ</u>

1) บุคลากรฝ่ายวิจัยและพัฒนาระบบต้องจัดให้มีการกำหนดคุณลักษณะความต้องการด้านความมั่นคงปลอดภัยสารสนเทศไว้อย่างชัดเจนสำหรับระบบที่จะพัฒนาขึ้นมาใช้งาน หรือระบบที่จัดหามาใช้งานในองค์กร

2) บุคลากรฝ่ายวิจัยและพัฒนาระบบต้องมีมาตรการป้องกันการรับส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง (Miss-Routing) การเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และการสำเนาข้อมูลโดยไม่ได้รับอนุญาต

3) บุคลากรฝ่ายวิจัยและพัฒนาระบบต้องกำหนดให้มีการควบคุมการเปลี่ยนแปลงต่าง ๆ ในการพัฒนาระบบคอมพิวเตอร์ โดยมีขั้นตอนการควบคุมที่เป็นทางการ

4) บุคลากรฝ่ายวิจัยและพัฒนาระบบต้องควบคุมให้มีการตรวจสอบทบทวนการทำงานของโปรแกรมที่มีความสำคัญในกรณีที่มีการเปลี่ยนแปลงใด ๆ เกิดขึ้นในระบบปฏิบัติการคอมพิวเตอร์ และต้องควบคุมให้มีการทดสอบการใช้งานเพื่อให้มั่นใจว่าผลของการเปลี่ยนแปลงดังกล่าว จะไม่ส่งผลกระทบใด ๆ ต่อความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการให้บริการของหน่วยงาน

5) บุคลากรฝ่ายวิจัยและพัฒนาระบบต้องยึดหลักการความมั่นคงปลอดภัยในการพัฒนาระบบดังต่อไปนี้

   5.1) การให้สิทธิต่ำที่สุด (Least privilege) แก่บุคลากรผู้เข้ามาใช้งานระบบ เพื่อป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต

   5.2) การให้สิทธิเฉพาะที่จำเป็นในการปฏิบัติงาน (Need to know) แก่บุคลากรผู้เข้ามาใช้งานระบบ เพื่อป้องกันการรั่วไหลของข้อมูลสำคัญ

   5.3) การออกแบบระบบให้สามารถป้องกันได้หลายระดับชั้น (Defense in-depth) เพื่อลดความเสี่ยงของการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

   5.4) การออกแบบในลักษณะเปิด (Open design) เพื่อให้การพัฒนาระบบมีการใช้กลไกหรืออัลกอริทึม (Algorithm) ที่เป็นมาตรฐานและสามารถตรวจสอบการทำงานได้

   5.5) การออกแบบระบบแบบ fail-safe เพื่อให้ระบบสามารถดำเนินการได้อย่างปลอดภัยและมีประสิทธิภาพ แม้จะเกิดข้อผิดพลาดหรือความล้มเหลวที่ไม่คาดคิด และป้องกันผลกระทบร้ายแรง เช่น การสูญหายของข้อมูล การละเมิดความปลอดภัย หรือการหยุดทำงานของระบบ เป็นต้น

   5.6) การพิจารณาแนวปฏิบัติด้านความปลอดภัย (Security guidelines) ข้อแนะนำจากผู้จำหน่าย (Vendor recommendations) และแนวทางปฏิบัติที่ดีที่สุด (Best practice) ในการตั้งค่าระบบและการดำเนินการ เพื่อสร้างระบบที่มีความปลอดภัย น่าเชื่อถือ และสอดคล้องกับข้อกำหนด

6) บุคลากรฝ่ายวิจัยและพัฒนาระบบต้องมีการควบคุมสภาพแวดล้อมของการพัฒนาและบูรณาการระบบ (System development and Integration) ให้มีความมั่นคงปลอดภัย โดยต้องป้องกันข้อมูลของระบบที่เกิดขึ้นในระหว่างการพัฒนา การรับส่งข้อมูล การสำรองข้อมูล และการควบคุมการเข้าถึงระบบ

7) บุคลากรฝ่ายวิจัยและพัฒนาระบบต้องจัดให้มีการควบคุมอย่างเข้มงวดในการเข้าถึงซอร์สโค้ดและรายการข้อมูลการพัฒนาระบบที่เกี่ยวข้อง (เช่น ข้อกำหนดความต้องการของระบบ ข้อมูลการออกแบบระบบ แผนการทดสอบการทำงานของระบบ) และเครื่องมือการพัฒนาระบบต่าง ๆ (เช่น Compilers, Builders, Integration tools และแพลตฟอร์มทดสอบ)

8) บุคลากรฝ่ายวิจัยและพัฒนาระบบต้องควบคุมให้มีการจัดทำข้อกำหนดขั้นต่ำของระบบคอมพิวเตอร์ และข้อกำหนดการควบคุมความมั่นคงปลอดภัยสารสนเทศของระบบคอมพิวเตอร์ใหม่ หรือการปรับปรุงระบบคอมพิวเตอร์เดิม ลงในข้อตกลงหรือสัญญา ทั้งโครงการที่เป็นโครงการภายในและโครงการที่จัดซื้อจัดจ้างผู้ให้บริการภายนอกเป็นผู้ดำเนินการ

9) บุคลากรฝ่ายวิจัยและพัฒนาระบบต้องมีการทดสอบฟังก์ชันการทำงานด้านความมั่นคงปลอดภัยสารสนเทศในระบบที่ได้รับการพัฒนาขึ้นใหม่ หรือทุกครั้งที่มีการเปลี่ยนแปลง

10) บุคลากรฝ่ายวิจัยและพัฒนาระบบควรใช้ข้อมูลที่ถูกทำให้เป็นนิรนาม (anonymization) หรือข้อมูลที่มีการใช้ชื่อแฝง (pseudonymization) หรือข้อมูลจำลอง (mock data) แทนการใช้ข้อมูลจากระบบงานจริง (production) ในการนำมาทดสอบระบบ ทั้งนี้ หากจำเป็นต้องใช้ข้อมูลจากระบบงานจริงในการทดสอบ สภาพแวดล้อมการทดสอบต้องมีมาตรการความมั่นคงปลอดภัยที่เทียบเท่ากับภาพแวดล้อมระบบงานจริง และต้องมีการกำหนดมาตรการการจัดการข้อมูลที่ใช้ทดสอบทั้งวงจรชีวิตของข้อมูลอย่างชัดเจน เช่น การลบข้อมูล เป็นต้น

11) บุคลากรฝ่ายวิจัยและพัฒนาระบบต้องกำหนดให้มีเกณฑ์ในการตรวจรับระบบคอมพิวเตอร์ใหม่หรือที่ปรับปรุงเพิ่มเติม ทั้งที่มาจากส่วนงานพัฒนาระบบเทคโนโลยีสารสนเทศพัฒนาขึ้นเองหรือที่มีการจัดหาจากหน่วยงานภายนอก ก่อนใช้งานจริง เพื่อให้มั่นใจได้ว่าระบบคอมพิวเตอร์ดังกล่าวทำงานได้อย่างมีประสิทธิภาพ สามารถประมวลผลได้อย่างถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน

10. การพัฒนาบุคลากรและการเสริมสร้างความตระหนัก ความรู้ และความเข้าใจ

10.1 องค์กรต้องจัดให้มีการฝึกอบรมแก่บุคลากรเพื่อสร้างความตระหนัก มีความรู้ ความเข้าใจการใช้งานระบบคอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศอย่างปลอดภัย

10.2 องค์กรต้องจัดฝึกอบรม หรือส่งเสริมให้ฝึกอบรม หรือสนับสนุนให้ศึกษาเพิ่มเติมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศแก่บุคลากรที่ทำงานด้านระบบคอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศ

11. บทลงโทษ

ให้บุคลากรที่เกี่ยวข้องภายในองค์กรยึดถือปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด ผู้ใดฝ่าฝืนจะมีความผิดและต้องได้รับการลงโทษทางวินัยตามแนวปฏิบัติการลงโทษขององค์กร

12. การทบทวน

ให้มีการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ และในกรณีที่มีการเปลี่ยนแปลงในเนื้อหาสาระของนโยบายฉบับนี้ โดยให้นำเสนอต่อคณะกรรมการบริหารความเสี่ยงและควบคุมภายใน เพื่อพิจารณาอนุมัติและลงนามประกาศใช้บังคับ