JTS

Jasmine Technology Solution

ประกาศบริษัท ฉบับที่ 004/2565
เรื่อง นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

บริษัท จัสมิน เทคโนโลยี โซลูชั่น จำกัด (มหาชน) และบริษัทย่อย ("บริษัท") ได้เล็งเห็นความสำคัญในการพัฒนาระบบเทคโนโลยีสารสนเทศขององค์กร และจัดการด้านความมั่นคงปลอดภัยสารสนเทศให้เป็นไปอย่างเหมาะสมและมีประสิทธิภาพ เพื่อให้การดำเนินการในด้านบริการ มีความปลอดภัยสามารถดำเนินการได้อย่างต่อเนื่อง และมีการป้องกันปัญหาที่เกิดขึ้นจากการใช้ระบบสารสนเทศในลักษณะที่ไม่ถูกต้อง และการคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อองค์กร รวมถึงสนับสนุนให้มีการบริหารจัดการข้อมูลสารสนเทศ เพื่อรักษาไว้ซึ่งการรักษาความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลและมีการพัฒนาอย่างต่อเนื่อง มีความสอดคล้องกับกฎหมาย มาตรฐานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศที่เป็นสากล และข้อบังคับที่เกี่ยวข้อง

จึงได้จัดทำนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อใช้ในการกำกับดูแลความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้ถือปฏิบัติไปในแนวทางเดียวกัน โดยอ้างอิงระเบียบและแนวทางปฏิบัติจากเอกสาร "นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ" ของบริษัท จัสมิน เทคโนโลยี โซลูชั่น จำกัด (มหาชน) และบริษัทย่อย ตามเอกสารแนบท้ายประกาศนี้ ซึ่งพนักงานขององค์กรและหน่วยงานภาคนอกต้องถือปฏิบัติตามอย่างเคร่งครัด

โดยให้มีผลตั้งแต่วันที่ 1 มิถุนายน 2565 เป็นต้นไป

ประกาศ ณ วันที่ 31 พฤษภาคม 2565

(คุณดสิต ศรีสง่าโอฬาร)

กรรมการผู้จัดการ

Jasmine Technology Solution

นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

บริษัท จัสมิน เทคโนโลยี โซลูชั่น จำกัด (มหาชน) และบริษัทฯย่อย

รหัสเอกสาร :	[ITGS-CS-001]
หมายเลขปรับปรุงเอกสาร :	1.0
วันที่เอกสารมีผลบังคับใช้ :	01/06/2565
เจ้าของเอกสาร :	สมเจตน์ แซ่จัง
ผู้อนุมัติเอกสาร :	ดุสิต ศรีสง่าโอฬาร

ประวัติการปรับปรุงเอกสาร

เวอร์ชัน	คำอธิบายและเหตุผลในการแก้ไข	ผู้แก้ไข	วันที่
1.0	เอกสารเผยแพร่ฉบับแรก	สมเจตน์ แซ่จัง	01/06/2565

ลายเซ็นรับรองเอกสาร

หน้าที่	ชื่อ	ลายเซ็น	ตำแหน่ง	วันที่
จัดทำโดย	สมเจตน์ แซ่จัง		Senior Manager	01/06/2565
อนุมัติโดย	ดุสิต ศรีสง่าโอฬาร		President	01/06/2565

สารบัญ

1. บทนำ 6

1.1 วัตถุประสงค์ 6

1.2 ขอบเขตของเอกสาร 6

1.3 ระยะเวลาทบทวน 6

2. กลยุทธ์การป้องกันความปลอดภัยของข้อมูล (Information Security Protection Strategy) 6

2.1 การรักษาความมั่นคงปลอดภัยของข้อมูล (Security Principles) 6

2.2 การบริหารจัดการความเสี่ยงด้านปลอดภัยสารสนเทศ (Information Security Risk Management) 7

3. การบังคับใช้นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ 7

3.1 การบังคับใช้นโยบาย 7

3.2 การจัดการมาตรการควบคุมด้านเทคนิคที่ล้าสมัย (Handling of Technical Controls Obsolescence) 7

3.3 การจัดการมาตรการที่ได้รับการยกเว้น (Handling of Policy Deviations) 7

3.4 การทบทวนการจัดการความมั่นคงปลอดภัยสารสนเทศโดยผู้ตรวจสอบที่เป็นอิสระ 8

4. โครงสร้างความปลอดภัยข้อมูลขององค์กร (Organization of Information Security) 9

4.1 ความมั่นคงปลอดภัยภายในบริษัท (Internal organization) 9

4.2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking) 10

5. ความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resource Security) 11

5.1 ก่อนการจ้างงาน 11

5.2 ระหว่างการจ้างงาน (During employment) 11

5.3 การสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน (Termination and change of employment) 11

6. การบริหารจัดการทรัพย์สิน (Asset Management) 12

6.1 หน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for assets) 12

6.2 การจัดชั้นความลับของข้อมูลสารสนเทศ (Information classification) 12

6.3 การจัดการสื่อบันทึกข้อมูล (Media Handling) 13

7. ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security) 14

7.1 พื้นที่ที่มีความมั่นคงปลอดภัย (Secure areas) 14

7.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment) 16
8. ความมั่นคงปลอดภัยสำหรับการปฏิบัติงาน (Operations security) 18
8.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational procedure and responsibilities) 18
8.2 การป้องกันซอฟต์แวร์ประสงค์ร้าย (Protection from malware) 19
8.3 การสำรองข้อมูล (Backup) 20
8.4 การบันทึกข้อมูลและการเฝ้าระวัง (Logging and monitoring) 20
9. ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security) 22
9.1 การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network security management) 22
9.2 การถ่ายโอนสารสนเทศ (Information transfer) 23
10. การควบคุมการเข้าถึง (Access Control) 27
10.1 ข้อกำหนดทางธุรกิจเรื่องการควบคุมการเข้าถึง (Business requirement of access control) 27
10.2 การจัดการการเข้าถึงของผู้ใช้งาน (User access management) 28
10.3 หน้าที่และความรับผิดชอบของผู้ใช้งาน 30
10.4 การควบคุมการเข้าใช้งานระบบปฏิบัติการ 30
10.5 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ 32
11. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information System Acquisition Development and Maintenance) 33
11.1 ข้อกำหนดด้านความปลอดภัยของระบบ (Security requirements of information system) 33
11.2 การประมวลผลข้อมูลในโปรแกรม 34
11.3 มาตรการการเข้ารหัส (Cryptography) 35
11.4 ความมั่นคงปลอดภัยของไฟล์ระบบ 35
11.5 ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in development and support processes) 36
11.6 ข้อมูลสำหรับการทดสอบ (Test data) 38
12. ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships) 38
12.1 ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplie

relationship) 38
12.2 การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก 39
13. การบริหารจัดการเหตุละเมิดด้านความมั่นคงปลอดภัยสารสนเทศ (Information security management) 40
13.1 การบริหารจัดการเหตุละเมิดด้านความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security and improvements) 40
14. มุมมองด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารความต่อเนื่องของธุรกิจ (Information security aspects of business continuity management) 42
14.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity) 42
15. ความสอดคล้อง (Compliance) 43
15.1 ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง (Compliance with legal and contractual requirements) 43
16. การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information security reviews) 44
16.1 การทบทวนด้านความมั่นคงปลอดภัยของข้อมูลโดยอิสระ 44
16.2 การปฏิบัติให้เป็นไปตามแนวปฏิบัติและมาตรฐานด้านความปลอดภัย 44
16.3 การตรวจสอบความสอดคล้องทางเทคนิค 44
17. บทลงโทษทางวินัย 45

1. บทนำ

1.1 วัตถุประสงค์

นโยบายด้านความมั่นคงปลอดภัยสารสนเทศจัดทำขึ้นโดยมีวัตถุประสงค์ดังนี้

1. เพื่อกำหนดทิศทางและให้การสนับสนุนการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ คงไว้ซึ่งการรักษาความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลและมีการพัฒนาอย่างต่อเนื่อง โดยสอดคล้องกับกฎหมายและข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้อง
2. เพื่อกำหนดเป็นแนวทางให้บุคลากรในบริษัทและบุคคลอื่นใดที่ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศ เป็นแนวปฏิบัติในการเข้าถึงข้อมูลสารสนเทศ และระบบเทคโนโลยีสารสนเทศของบริษัทให้เป็นไปอย่างถูกต้อง เหมาะสม และปลอดภัย
3. เพื่อปกป้องสารสนเทศให้ปลอดภัยจากความสูญเสียในรูปแบบต่างๆ เช่น การสูญหาย การถูกทำลาย การแก้ไขโดยไม่ได้รับอนุญาต การลักลอบนำข้อมูลไปใช้หรือเปิดเผย ตลอดจนสร้างความมั่นใจว่าระบบสารสนเทศมีความมั่นคงปลอดภัย น่าเชื่อถือ และสามารถให้บริการได้อย่างต่อเนื่อง

1.2 ขอบเขตของเอกสาร

บริษัทกำหนดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัท และต้องมีการประกาศใช้สำหรับพนักงานและหน่วยงานทั้งหมดของบริษัท หรือหน่วยงานภายนอก ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของบริษัท เพื่อให้มีความเข้าใจและปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยสารสนเทศฉบับนี้

1.3 ระยะเวลาทบทวน

บริษัทกำหนดให้มีการปรับปรุงและทบทวนนโยบายในการรักษาความมั่นคงปลอดภัยของข้อมูล (Review of the policies for information security) อย่างสม่ำเสมอ เพื่อให้การรักษาความมั่นคงปลอดภัยสารสนเทศคงความถูกต้อง สมบูรณ์ และมีความพร้อมใช้งาน โดยสอดคล้องเหมาะสมกับการเปลี่ยนแปลงและความต้องการทางธุรกิจของบริษัทให้เป็นปัจจุบัน อย่างน้อยปีละ 1 ครั้ง

2. กลยุทธ์การป้องกันความปลอดภัยของข้อมูล (Information Security Protection Strategy)

2.1 การรักษาความมั่นคงปลอดภัยของข้อมูล (Security Principles)

การรักษาความมั่นคงปลอดภัยของข้อมูล มีหลักการเพื่อให้บรรลุผลตามวัตถุประสงค์ดังต่อไปนี้

- ความลับ (Confidentiality) คือ การปกป้องความลับของข้อมูล โดยป้องกันการเข้าถึงและการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต รวมไปถึงข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นกรรมสิทธิ์ของบริษัท
- ความถูกต้องสมบูรณ์ (Integrity) คือ การทำให้มั่นใจว่าข้อมูลสารสนเทศ ต้องไม่มีการแก้ไข ดัดแปลง หรือโดนทำลายโดยผู้ที่ไม่ได้รับอนุญาต
- ความพร้อมใช้งาน (Availability) คือ การทำให้มั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลและบริการได้อย่างรวดเร็วและเชื่อถือได้

- ความรับผิดชอบ (Accountability) คือ การระบุหน้าที่ความรับผิดชอบของแต่ละบุคคล รวมถึงการรับผิดและรับชอบในผลของกระทำตามบทบาทหน้าที่นั้นๆ
- การพิสูจน์ตัวตน (Authentication) คือ การทำให้มั่นใจว่าสิทธิการเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศต้องผ่านกระบวนการยืนยันตัวตนที่สมบูรณ์แล้วเท่านั้น
- การกำหนดสิทธิ (Authorization) คือ การทำให้มั่นใจว่าการให้สิทธิเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศเป็นไปตามความจำเป็น (Least Privilege) และสอดคล้องกับความต้องการพื้นฐาน (Need to Know Basis) ตามที่ได้รับอนุญาต

2.2 **การบริหารจัดการความเสี่ยงด้านปลอดภัยสารสนเทศ** (Information Security Risk Management)

การบริหารความเสี่ยงเป็นความรับผิดชอบร่วมกันของผู้บริหารและพนักงานทุกระดับ และต้องมีการปฏิบัติอย่างต่อเนื่องโดยกระบวนการบริหารความเสี่ยงต้องประกอบด้วยขั้นตอนหลัก ดังนี้

- การระบุความเสี่ยงที่อาจเกิดขึ้นและมีผลกระทบต่อการรักษาความปลอดภัยข้อมูล
- การประเมินความเสี่ยง
- การจัดการความเสี่ยง
- การติดตามความเสี่ยงและการรายงาน

3. การบังคับใช้นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

นโยบายนี้มีผลบังคับใช้ภายในบริษัท โดยครอบคลุมประเด็นด้านมั่นคงความปลอดภัยสารสนเทศของบริษัทดังนี้

3.1 **การบังคับใช้นโยบาย**

การประกาศใช้นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ ต้องมีการประกาศและสื่อสารไปยังผู้ที่เกี่ยวข้องทราบเพื่อปฏิบัติได้อย่างเหมาะสม โดยผู้บังคับบัญชาตามสายงานตั้งแต่ระดับฝ่ายขึ้นไป มีหน้าที่รับผิดชอบในการจัดทำมาตรการควบคุมที่เหมาะสมเพื่อให้สอดคล้องกับนโยบายด้านความปลอดภัยสารสนเทศ ภายใต้ขอบเขตความรับผิดชอบของตน และให้มีการตรวจสอบมาตการควบคุมด้านความปลอดภัยสารสนเทศโดยผู้ตรวจสอบอิสระ

3.2 **การจัดการมาตรการควบคุมด้านเทคนิคที่ล้าสมัย** (Handling of Technical Controls Obsolescence)

ในกรณีที่มีการใช้มาตรการควบคุมด้านเทคนิคที่ล้าสมัยหรือกำลังจะล้าสมัย เนื่องจากข้อจำกัดของระบบหรืออุปกรณ์ บริษัทต้องกำหนดระยะเวลาที่อนุญาตให้ใช้งานเทคนิคที่ล้าสมัยหรือกำลังจะล้าสมัย ก่อนการปรับปรุงหรือเปลี่ยนแปลง เพื่อให้มีการควบคุมการใช้งานมาตรการทางเทคนิคที่ล้าสมัยหรือกำลังจะล้าสมัยอย่างเหมาะสม

3.3 **การจัดการมาตรการที่ได้รับการยกเว้น** (Handling of Policy Deviations)

หากมีความจำเป็นที่ต้องใช้บางมาตรการควบคุมที่ไม่เป็นไปตามนโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศ ผู้บังคับบัญชาตามสายงานที่เกี่ยวข้องกับมาตรการควบคุมที่ได้รับการยกเว้นนั้น ต้องทบทวนและพิจารณาความเสี่ยงในการใช้มาตรการควบคุมดังกล่าวเป็นประจำทุกปี

3.4 การทบทวนการจัดการความมั่นคงปลอดภัยสารสนเทศโดยผู้ตรวจสอบที่เป็นอิสระ

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงกำกับให้มีการตรวจประเมินระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละ 1 ครั้ง ทั้งนี้ผู้ตรวจสอบจะต้องเป็นอิสระและไม่มีความเกี่ยวข้องกับส่วนงานที่ได้รับการตรวจประเมิน

นโยบายด้านความมั่นคงปลอดภัยด้านสารสนเทศ

แนวปฏิบัติหรือแนวทางการจัดทำมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ มีดังนี้

4. **โครงสร้างความปลอดภัยข้อมูลขององค์กร** (Organization of Information Security)

4.1 **ความมั่นคงปลอดภัยภายในบริษัท** (Internal organization)

มีการกำหนดกรอบในการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ การกำหนดหน้าที่ความรับผิดชอบภายในองค์กร รวมถึงการขอรับคำแนะนำจากผู้เชี่ยวชาญความมั่นคงปลอดภัยด้านสารสนเทศ

4.1.1 **บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ** (Roles and Responsibilities)

มีการกำหนดหน้าที่ความรับผิดชอบที่ชัดเจนสำหรับคณะกรรมการบริหาร และคณะทำงานที่เกี่ยวข้องกับระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ และควรกำหนดหน่วยงานหรือบุคคลต่างๆ ที่มีส่วนเกี่ยวข้องในการดำเนินงานภายใต้ขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ

4.1.2 **การติดต่อกับหน่วยงานของทางการ** (Contacts with Authorities)

คณะกรรมการบริหารด้านความมั่นคงปลอดภัยจะต้องทำการสื่อสารอย่างมีประสิทธิภาพกับหน่วยงานที่มีอำนาจในการบังคับใช้กฎหมาย หน่วยงานที่กำกับดูแลบริษัท และผู้ให้บริการทางด้านโทรคมนาคม คณะทำงานเมื่อเกิดเหตุฉุกเฉินด้านระบบสารสนเทศ รวมถึงหน่วยงานของทางการที่ต้องทำการติดต่อเมื่อเกิดเหตุการณ์ต่างๆ โดยจะต้องมีการทบทวนและปรับปรุงข้อมูลให้ทันสมัยอยู่เสมอ

4.1.3 **การติดต่อกับผู้ที่อยู่ในแวดวงด้านการรักษาความปลอดภัยและผู้เชี่ยวชาญด้านความปลอดภัย** (Contacts with Special Interest Groups)

บริษัทจะต้องได้รับแจ้งข้อมูลต่างๆ ด้านความปลอดภัยจากผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย หรือได้รับข้อมูลเทคโนโลยีใหม่ๆ ข้อมูลเกี่ยวกับวิธีปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ ข้อมูลด้านการเตือนล่วงหน้า คำปรึกษา และการติดตั้งแพตช์ (Patch) เกี่ยวกับการโจมตี และช่องโหว่ต่างๆ คำแนะนำด้านความมั่นคงปลอดภัยจากผู้ขายผลิตภัณฑ์ และการแลกเปลี่ยนข้อมูลกับองค์กรอื่นๆ เพื่อลดความเสี่ยงจากการถูกคุกคามจากช่องโหว่ด้านความปลอดภัยสารสนเทศและเพื่อให้ผู้ได้รับผลกระทบพิจารณาและดำเนินการทันทีภายใต้กรอบเวลาที่กำหนดไว้

4.1.4 **ความมั่นคงปลอดภัยสำหรับสารสนเทศในการบริหารโครงการ** (Project Management)

ต้องมีการระบุถึงความมั่นคงปลอดภัยสารสนเทศในวัตถุประสงค์ของโครงการสำหรับทุกโครงการที่เกี่ยวข้องกับระบบสารสนเทศทั้งหมด โดยให้มีข้อตกลงการรักษาความลับของข้อมูลและข้อกำหนดในการปฏิบัติงานครอบคลุมถึงความมั่นคงปลอดภัยสารสนเทศกับผู้ที่เกี่ยวข้องในการปฏิบัติงานโครงการนั้นๆ

4.2 **อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล** (Mobile devices and teleworking)

การรักษาความมั่นคงปลอดภัยของอุปกรณ์คอมพิวเตอร์แบบพกพา และการปฏิบัติงานจากระยะไกล(Remote Access) มีขอบเขตครอบคลุมถึงอุปกรณ์พกพา หรืออุปกรณ์เคลื่อนที่ใดๆ ของบริษัทที่ใช้ในการเก็บข้อมูลหรือประมวลผลข้อมูลของบริษัท โดยมีแนวทางปฏิบัติดังนี้

1) ห้ามใช้ทรัพยากรของบริษัท เพื่อหรือสนับสนุนวัตถุประสงค์ที่ผิดกฎหมายตามที่กฎหมายได้บัญญัติไว้โดยเด็ดขาด
2) ห้ามใช้ทรัพยากรของบริษัททำกิจกรรมทางการเมืองภายในบริษัทโดยเด็ดขาด
3) การใช้งานทรัพยากรของบริษัทจะทำได้เฉพาะพนักงานหรือผู้ที่ได้รับอนุญาตเท่านั้น และใช้เพื่อวัตถุประสงค์ในการทำงานเท่านั้น
4) ห้ามใช้อุปกรณ์ประมวลผลส่วนตัวในการเก็บหรือประมวลผลข้อมูลของบริษัท เว้นเสียแต่ได้รับการอนุมัติ
5) ต้องมีการป้องกันหรือการล็อกอุปกรณ์พกพา และคอมพิวเตอร์พกพาอย่างเหมาะสม เมื่อไม่ได้ใช้งานภายในสำนักงาน
6) ควรปฏิบัติตามคำแนะนำของผู้ผลิตในการปกป้องอุปกรณ์ตลอดเวลา เช่นการป้องกันการสัมผัสกับสนามแม่เหล็กไฟฟ้าแรงๆ การป้องกันแสงแดดโดยตรง ฯลฯ
7) ต้องไม่วางอุปกรณ์ไว้ในที่สาธารณะโดยที่ไม่มีคนดูแล ผู้ดูแลทรัพย์สินนั้นมีหน้าที่รับผิดชอบในการดูแลและป้องกันอุปกรณ์ต่างๆ นั้น หากอุปกรณ์เสียหาย สูญหาย หรือเกิดการลักขโมย จะต้องแจ้งผู้บังคับบัญชาและผู้ดูแลระบบให้ทราบทันทีเพื่อให้มีการติดตามและมีวิธีการจัดการกับเหตุการณ์ได้อย่างมีประสิทธิภาพ
8) คอมพิวเตอร์แบบพกพาต้องได้รับการป้องกันอย่างเหมาะสมจากการเข้าถึงโดยไม่ได้รับอนุญาต
9) ต้องติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ (Antivirus) บนคอมพิวเตอร์แบบพกพา และทำการปรับปรุงข้อมูลไวรัส (Virus Pattern) ให้ทันสมัยอยู่เสมอ
10) พนักงานและผู้จัดการส่วนหรือเทียบเท่าขึ้นไปของบริษัทมีหน้าที่จะต้องดูแลให้เครื่องคอมพิวเตอร์ที่ใช้งานในความรับผิดชอบ ได้รับการติดตั้งโปรแกรมใช้งานโดยถูกต้องตามนโยบายของบริษัท
11) การจัดการข้อมูล ต้องเป็นไปตามมาตรฐานการจัดการข้อมูลตามระดับชั้นสูงสุดที่มีอยู่ภายในอุปกรณ์นั้น
12) ผู้ใช้งานต้องทำการสำรองข้อมูลสารสนเทศที่อยู่ในอุปกรณ์พกพาบนแหล่งจัดเก็บข้อมูลที่จัดไว้ให้ หรือหากจำเป็นสามารถสำรองข้อมูลสารสนเทศบนสื่อบันทึกพกพาที่ได้รับอนุญาตเท่านั้น
13) ข้อมูลสารสนเทศสำรองบนสื่อบันทึกพกพาต้องถูกลบ หรือทำลายอย่างปลอดภัยตามมาตรฐานการกำจัดสื่อเมื่อไม่ได้ใช้งาน
14) การทำงานจากระยะไกล (Remote Access) ต้องผ่านช่องทางที่มีความมั่นคงปลอดภัยตามที่กำหนดไว้เท่านั้น และต้องได้รับการอนุมัติอย่างเป็นทางการ

5. ความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resource Security)

5.1 ก่อนการจ้างงาน

ก่อนการจ้างงานในส่วนของทรัพยากรบุคคล ไม่ว่าจะเป็นพนักงานและ/ หรือหน่วยงานภายนอกจำเป็นต้องมีการคัดเลือกบุคลากรที่มีความเหมาะสมตามตำแหน่งงาน โดยเฉพาะงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ มีการกำหนดหน้าที่ความรับผิดชอบ และการลงลายมือชื่อในสัญญา

5.1.1 การคัดสรรบุคลากร

จัดให้มีการคัดสรรพนักงานและหน่วยงานภายนอกโดยจะต้องตรวจสอบประวัติของผู้สมัครในด้านต่างๆ เพื่อให้มั่นใจว่ามีคุณสมบัติครบถ้วน ถูกต้อง และสอดคล้องกับหน้าที่ที่ได้รับ

5.1.2 เงื่อนไขและเกณฑ์การจ้าง

จัดให้มีการลงลายมือชื่อในสัญญารับทราบเงื่อนไขและเกณฑ์การจ้างให้กับพนักงานและหน่วยงานภายนอก รวมถึงรับทราบข้อกำหนดด้านความมั่นคงปลอดภัย และข้อตกลงการรักษาความลับ

5.2 ระหว่างการจ้างงาน (During employment)

5.2.1 หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities)

ผู้บริหารทุกระดับของบริษัท มีหน้าที่กำกับดูแล และเสริมสร้างค่านิยม ให้กับพนักงานและหน่วยงานภายนอกให้มีการปฏิบัติตามแนวปฏิบัติและกระบวนการความมั่นคงปลอดภัยด้านสารสนเทศ ในด้านต่างๆ ดังนี้

(1) มีการสื่อสารให้กับพนักงานและหน่วยงานภายนอกให้รับทราบถึงหน้าที่และความรับผิดชอบความมั่นคงปลอดภัยของตนเอง และบทลงโทษหากพบการกระทำผิด

(2) มีการสื่อสารหรืออบรมให้กับพนักงานและหน่วยงานภายนอกที่เกี่ยวข้อง มีความตระหนักรู้ และปฏิบัติงานโดยคำนึงถึงการรักษาความมั่งคงปลอดภัยของข้อมูล

(3) ให้ทิศทางกำกับดูแลและการสนับสนุนให้เกิดความมั่นคงปลอดภัยสารสนเทศภายในบริษัท

5.2.2 การสร้างความตระหนักรู้ การให้ความรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information security awareness, education and training)

จัดให้มีการอบรมด้านความมั่นคงปลอดภัยสารสนเทศให้กับพนักงาน ลูกจ้าง หรือหน่วยงานภายนอก ที่ปฏิบัติงานเกี่ยวข้องกับระบบสารสนเทศของบริษัทอย่างน้อยปีละ 1 ครั้ง โดยมีการทดสอบเพื่อวัดผลความสำเร็จในการฝึกอบรมดังกล่าว

5.2.3 กระบวนการทางวินัย (Disciplinary process)

มีมาตรการหรือกระบวนการลงโทษทางวินัยของบริษัท ต้องให้ครอบคลุมถึงการละเมิดด้านความปลอดภัยของข้อมูลด้วย

5.3 การสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน (Termination and change of employment)

หากมีการสิ้นสุดหรือเปลี่ยนแปลงการจ้าง ให้มีการทบทวนบทบาทและหน้าที่ความรับผิดชอบที่ได้รับ เพื่อการบริหารจัดการทรัพย์สินและสิทธิการเข้าถึงระบบสารสนเทศที่เหมาะสม และแจ้งให้กับพนักงานหรือหน่วยงานภายนอกที่

เกี่ยวข้องได้รับทราบและปฏิบัติตาม รวมถึงให้มีการส่งถ่ายความรู้ในการทำงานอย่างเป็นทางการ และมีประสิทธิภาพให้กับบุคคลที่ได้รับมอบหมาย ก่อนสิ้นสุดหรือเปลี่ยนแปลงสัญญาจ้างงาน

6. การบริหารจัดการทรัพย์สิน (Asset Management)

6.1 หน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for assets)

ผู้บริหารแต่ละสายงานต้องกำกับให้มีการจัดทำรายการทรัพย์สิน โดยกำหนดผู้ที่ได้รับมอบหมายให้ครอบครองดูแลและหน้าที่ความรับผิดชอบที่มีต่อทรัพย์สินนั้น

6.1.1 รายการทรัพย์สิน (Inventory of assets)

ทรัพย์สินทั้งหมดที่เกี่ยวข้องกับการดำเนินงานจะต้องได้รับการจัดเก็บในรายการทรัพย์สิน โดยครอบคลุมถึงทรัพย์สินประเภทต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศของบริษัท โดยรายการทรัพย์สินต้องทำการทบทวนบัญชีรายการทรัพย์สินเป็นประจำ อย่างน้อยปีละ 1 ครั้ง

6.1.2 ความเป็นเจ้าของทรัพย์สิน (Ownership of assets)

ทรัพย์สินทั้งหมดจะต้องมีผู้ดูแลและมีการกำหนดชื่อผู้ที่ได้รับมอบหมายให้ครอบครองดูแลอาจจะเป็นบุคคลหรือหน่วยงานก็ได้ ในกรณีที่กำหนดให้ทรัพย์สินใดเป็นของหน่วยงานในบริษัท ความรับผิดชอบต่อทรัพย์สินดังกล่าวจะขึ้นกับหัวหน้าหน่วยงานนั้นๆ

6.1.3 การใช้งานทรัพย์สินอย่างเหมาะสม (Acceptable use of assets)

มีการกำหนดแนวปฏิบัติการใช้งานระบบสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศอย่างเหมาะสม โดยมีการระบุข้อกำหนดอย่างชัดเจน จัดทำเป็น ลายลักษณ์อักษร และบังคับใช้ภายในบริษัท

6.1.4 การคืนทรัพย์สิน (Return of assets)

พนักงานและลูกจ้างของหน่วยงานทั้งหมดต้องคืนทรัพย์สินของบริษัททั้งหมดที่ตนถือครอง เมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง รวมถึงการถอดถอนสิทธิการเข้าถึงข้อมูล พื้นที่ ระบบเทคโนโลยีสารสนเทศทันทีที่มีการสิ้นสุดหรือเปลี่ยนแปลงการจ้าง

6.2 การจัดชั้นความลับของข้อมูลสารสนเทศ (Information classification)

6.2.1 ชั้นความลับของข้อมูล (Classification of information)

ให้ทำการจัดประเภทข้อมูลสารสนเทศ ลำดับความสำคัญหรือระดับชั้นความลับของข้อมูล รวมถึงระดับชั้นการเข้าถึง เวลาที่อนุญาตให้เข้าถึง และเจ้าของข้อมูลเป็นผู้กำหนดระดับชั้นความลับของข้อมูล ข้อมูลทั้งหมดที่อยู่ภายในขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศจะต้องได้รับการจัดระดับชั้นความลับ โดยมีแนวปฏิบัติดังนี้

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

(2) การใช้งานหรือการเข้าถึงข้อมูลให้อยู่ภายในเวลาทำการ หรือให้สอดคล้องกับประเภทข้อมูลและการปฏิบัติงานของผู้ดูแลข้อมูล

(3) เจ้าของข้อมูลจะต้องเป็นผู้กำหนดระดับชั้นความลับของข้อมูลที่ตนเป็นเจ้าของ และกำหนดให้มีการทบทวนระดับชั้นความลับอย่างสม่ำเสมอ

6.2.2 **การบ่งชี้ประเภทข้อมูล** (labelling of information)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงกำหนดให้มีการบ่งชี้ประเภทข้อมูลโดยการติดป้าย เพื่อการจัดการข้อมูลที่อยู่ในขั้นตอนการจัดเก็บ การขนส่ง การประมวลผล และการทำลายทิ้ง ให้สอดคล้องตามประเภทข้อมูล โดยมีแนวปฏิบัติดังนี้

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

(2) เจ้าของข้อมูลจะต้องกำหนดมาตรการในการจัดการข้อมูลให้สอดคล้องตามระดับชั้นความลับ และมีการทบทวนประสิทธิภาพของมาตรการอย่างสม่ำเสมอ

(3) ข้อมูลที่ไม่สามารถติดป้ายได้ เช่น ไฟล์อิเล็กทรอนิกส์ในเครื่องคอมพิวเตอร์ จะต้องมีวิธีปฏิบัติให้สอดคล้องกับระดับชั้นความลับสูงสุดที่มีในเครื่อง โดยไม่จำเป็นต้องติดป้าย

6.2.3 **การจัดการทรัพย์สิน** (Handling of assets)

สื่อบันทึกข้อมูลจะต้องได้รับการจัดประเภทของข้อมูลตามระดับความลับสูงสุดของข้อมูลที่มีอยู่ในสื่อบันทึกข้อมูลนั้น ซึ่งการเปิดเผยหรือเผยแพร่ข้อมูลจะต้องสอดคล้องกับข้อกำหนดที่ระบุไว้ในแนวทางตามแนวปฏิบัติการจัดระดับชั้นความลับ การติดป้าย และการจัดการข้อมูล (Information Classification, Labelling and Handling Guideline)

6.3 **การจัดการสื่อบันทึกข้อมูล** (Media Handling)

6.3.1 **การบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยกหรือพกพาได้** (Management of removable media)

สื่อบันทึกข้อมูลที่ถอดแยกหรือพกพาได้ ต้องมีการจัดการข้อมูลสารสนเทศที่อยู่ในสื่อบันทึกนั้นๆ โดยปฏิบัติตามแนวปฏิบัติการจัดระดับชั้นความลับ การติดป้าย และการจัดการข้อมูล (Information Classification, Labelling and Handling Guideline)

6.3.2 **การทำลายสื่อบันทึกข้อมูลที่ไม่ใช้แล้ว** (Disposal of media)

สื่อบันทึกข้อมูลที่ล้าสมัยและไม่ใช้งานแล้วจะต้องถูกทำลายทิ้งตามมาตรฐานในการกำจัดสื่อบันทึกข้อมูลที่ได้กำหนดไว้

6.3.3 **การนำส่งสื่อสำรองข้อมูลออกไปยังภายนอกบริษัท** (Physical Media Transfer)

สื่อบันทึกข้อมูลที่นำออกไปใช้ภายนอกบริษัท ต้องได้รับการป้องกันอย่างเหมาะสม และผู้นำส่งสื่อบันทึกข้อมูล ต้องเป็นบุคคลหรือหน่วยงานที่ได้รับการรับรองและเชื่อถือได้

7. ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)

7.1 พื้นที่ที่มีความมั่นคงปลอดภัย (Secure areas)

กำหนดให้พื้นที่ทางกายภาพมีการออกแบบเพื่อป้องกันการเข้าถึง ทำลาย ก่อกวน หรือแทรกแซงโดยไม่ได้รับอนุญาต

7.1.1 ความมั่นคงปลอดภัยอาณาเขตและบริเวณล้อมรอบ (Physical security perimeter)

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

(1) พื้นที่หวงห้าม คือ พื้นที่ที่มีระดับความสำคัญสูงสุด โดยเป็นพื้นที่ที่เก็บอุปกรณ์สำคัญ พื้นที่ในส่วนนี้ได้แก่ พื้นที่ศูนย์คอมพิวเตอร์ ห้องจ่ายกระแสไฟฟ้า เป็นต้น

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

(3) การรักษาความมั่นคงปลอดภัยจะต้องมีการดำเนินงาน ดังนี้

1) จัดทำแผนผังที่ตั้งอาคารที่ใช้เป็นพื้นที่ในการปฏิบัติการ และแสดงระดับความสำคัญของพื้นที่

2) ประตูและหน้าต่างที่อยู่ในพื้นที่ด้านความมั่นคงปลอดภัยจะต้องทำจากวัสดุที่แข็งแรงเพื่อป้องกันการบุกรุกจากภายนอก

3) กำหนดให้พนักงานรักษาความปลอดภัยแลกบัตรของผู้มาติดต่อจากหน่วยงานภายนอก และจดบันทึกเพื่อใช้ในการตรวจสอบย้อนหลัง

4) จัดให้มีการติดตั้ง CCTV ให้ครอบคลุมพื้นที่หวงห้ามเด็ดขาดและทางเข้า-ออกบริเวณพื้นที่หวงห้าม โดยสามารถเรียกดูภาพบันทึกภาพย้อนหลังได้

7.1.2 การควบคุมการเข้าออกพื้นที่ (Physical entry controls)

ให้มีการควบคุมการเข้า-ออกพื้นที่ โดยมีแนวปฏิบัติดังนี้

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

(2) งดการออกบัตรหรือการใช้ข้อมูลอัตลักษณ์ (Biometric data) ในการเข้าถึงระบบสารสนเทศให้กับหน่วยงานภายนอกที่เข้าออกพื้นที่ชั่วคราว ยกเว้นมีเหตุจำเป็นโดยต้องได้รับการอนุมัติอย่างเป็นทางการ

(3) กำหนดให้หน่วยงานภายนอกที่เข้าถึงพื้นที่ของกลุ่มเทคโนโลยีสารสนเทศจะต้องติดบัตรผู้มาติดต่อในตำแหน่งที่เห็นได้ง่าย

(4) พนักงานที่อยู่ต่างฝ่าย และหน่วยงานภายนอกที่มีความประสงค์เข้าพื้นที่หวงห้ามจะต้องแจ้งความประสงค์ล่วงหน้า และมีผู้ติดตามระหว่างเข้าถึงพื้นที่ตลอดเวลา โดยบันทึกการเข้า-ออกทุกครั้ง

7.1.3 **ความมั่นคงปลอดภัยของพื้นที่ปฏิบัติงาน** (Securing offices, rooms, and facilities)

ห้องปฏิบัติงาน ห้องที่มีทรัพย์สินและอุปกรณ์ มีความมั่นคงปลอดภัย โดยครอบคลุมประเด็นสำคัญ ดังนี้

(1) อาคารหรือพื้นที่ที่มีความสำคัญ เช่น ศูนย์คอมพิวเตอร์ ฯลฯ มีความแข็งแรงและปลอดภัย ไม่สามารถรุกล้ำเข้าไปได้โดยง่าย ไม่ติดกระจกใสให้มองเห็นกิจกรรมภายในได้โดยง่าย ไม่แสดงป้ายชื่อหรือรายละเอียดกิจกรรมภายในห้อง

(2) หลีกเลี่ยงการวางอุปกรณ์เทคโนโลยีสารสนเทศที่สำคัญไว้บริเวณพื้นที่ส่วนกลาง

(3) สำนักงาน ห้อง และสภาพแวดล้อมของการปฏิบัติงานจะต้องมีความมั่นคงปลอดภัย

7.1.4 **การป้องกันภัยคุกคามจากภายนอกและสภาพแวดล้อม** (Protecting against external and environmental threats)

ให้พื้นที่ติดตั้งระบบเทคโนโลยีสารสนเทศมีการออกแบบและสามารถป้องกันภัยทางธรรมชาติ ดังนี้

(1) อาคารพื้นที่ตั้งปลอดภัยจากภัยทางธรรมชาติ เช่น ดินถล่ม น้ำท่วม แผ่นดินไหว เป็นต้น

(2) สถานที่ปฏิบัติงานมีอุปกรณ์ดับเพลิงที่เหมาะสมและมีการตรวจสอบคุณภาพของอุปกรณ์ดับเพลิงอย่างสม่ำเสมอ

(3) ศูนย์คอมพิวเตอร์มีการติดตั้งระบบดับเพลิงอัตโนมัติที่ปลอดภัยต่อชีวิตและทรัพย์สิน

(4) มีการบำรุงรักษาพื้นที่โดยทั่วไปอย่างสม่ำเสมอเพื่อกำจัดขยะที่อาจติดไฟ

7.1.5 **การปฏิบัติงานในพื้นที่ที่มีความมั่นคงปลอดภัย** (Working in secure areas)

ให้พื้นที่ของการปฏิบัติงานด้านเทคโนโลยีสารสนเทศมีการออกแบบให้มีความมั่นคงปลอดภัย โดยมีแนวปฏิบัติดังนี้

(1) ห้ามพนักงานที่ไม่มีหน้าที่ในการปฏิบัติงานในพื้นที่ และหน่วยงานภายนอกเข้าพื้นที่หวงห้าม เพื่อป้องกันการดำเนินการใดๆ ที่ไม่ได้รับอนุญาต

(2) ต้องปิดล็อกประตูห้องที่ไม่มีการใช้งาน ปิดประตูและหน้าต่างทุกครั้งที่เลิกงาน หรือเมื่อไม่มีผู้ดูแล

(3) ไม่อนุญาตให้นำอุปกรณ์ถ่ายภาพ วิดีโอ เสียง หรืออุปกรณ์บันทึกอื่นๆ เข้ามาภายในศูนย์คอมพิวเตอร์ เว้นแต่จะได้รับอนุญาต

(4) ไม่อนุญาตให้นำหรือรับประทานอาหารและเครื่องดื่มในศูนย์คอมพิวเตอร์

(5) ห้ามนำสิ่งของหรืออุปกรณ์ใดๆ เข้าพื้นที่หวงห้าม ยกเว้นได้รับการอนุญาตอย่างเป็นทางการ

7.1.6 **พื้นที่ส่วนกลาง พื้นที่ส่งของ และพื้นที่ขนถ่ายสิ่งของ** (Delivery and loading areas)

ควรจัดให้มีพื้นที่ส่วนกลาง พื้นที่ส่งของ และพื้นที่ขนถ่ายสินค้า โดยมีแนวปฏิบัติดังนี้

(1) การนำสิ่งของเข้าไปส่งในพื้นที่หวงห้าม จะต้องมีการแจ้งล่วงหน้า

(2) ก่อนนำสิ่งของเข้าไปส่งในพื้นที่หวงห้ามจะต้องตรวจสอบสภาพ และวัตถุอันตรายก่อนเคลื่อนย้ายไปยังจุดที่ต้องการ

7.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment)

อุปกรณ์ที่ตั้งอยู่ในพื้นที่ที่มีความมั่นคงปลอดภัยต้องมีการป้องกันทางกายภาพเพื่อป้องกันการเข้าถึง ทำลาย ก่อกวน หรือแทรกแซงโดยไม่ได้รับอนุญาต

7.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment sitting and protection)

การวางอุปกรณ์ภายในศูนย์คอมพิวเตอร์จะต้องปฏิบัติตามข้อกำหนดดังต่อไปนี้

(1) ต้องใช้ชั้นวางอุปกรณ์ (Server Rack) สำหรับวางเซิร์ฟเวอร์และอุปกรณ์เครือข่ายที่สำคัญ

(2) ต้องติดตั้ง CCTV หน้าชั้นวางอุปกรณ์สำคัญเพื่อใช้ตรวจสอบผู้ใช้งานอุปกรณ์ในชั้นวาง

(3) ต้องเฝ้าระวังอุณหภูมิและความชื้นภายในพื้นที่หวงห้าม

7.2.2 อุปกรณ์สนับสนุน (Supporting utilities)

จัดให้มีการติดตั้งอุปกรณ์สนับสนุน ระบบปรับอากาศ ระบายอากาศ ระบบแสงสว่าง และระบบดับเพลิงให้กับอุปกรณ์ในพื้นที่หวงห้าม รวมถึงประสานงานกับฝ่ายอาคารในการสนับสนุนและจัดหาให้มีการติดตั้งและสนับสนุนระบบไฟฟ้าให้กับอุปกรณ์ในพื้นที่ ดังนี้

(1) ต้องใช้ระบบสำรองกระแสไฟฟ้าต่อเนื่อง (UPS) เพื่อให้กระแสไฟฟ้ามีความเสถียร และป้องกันอุปกรณ์เสียหายจากเหตุไฟตก/ไฟกระชาก

(2) ต้องติดตั้งระบบปรับอากาศเพื่อสร้างสภาพแวดล้อมที่เหมาะสมให้กับอุปกรณ์

(3) ต้องติดตั้งไฟฉุกเฉินเพื่อให้บริการแสงสว่าง

(4) ต้องติดตั้งระบบแจ้งเตือน (Tele-alarm) เพื่อแจ้งเตือนผู้ปฏิบัติงานเมื่อตรวจพบเหตุผิดปกติ

(5) ต้องติดตั้งระบบกำเนิดไฟฟ้าสำรองเพื่อให้กระแสไฟฟ้ามีความเสถียร

7.2.3 ความมั่นคงปลอดภัยในการติดตั้งสายเคเบิล (Cabling security)

ในการติดตั้งสายเคเบิลภายในพื้นที่หวงห้ามจะต้องปฏิบัติตามข้อกำหนดดังต่อไปนี้

(1) สายเคเบิลที่ใช้ในการสื่อสารข้อมูลอยู่ในท่อหรือราง

(2) มีการแยกสายไฟและสายเคเบิลเครือข่ายออกจากกันเพื่อป้องกันสัญญาณรบกวน

(3) ต้องติดป้ายเพื่อระบุต้นทางและปลายทางของสายเคเบิลที่ใช้เชื่อมต่อเข้ากับอุปกรณ์เทคโนโลยีสารสนเทศ

7.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

จัดให้มีการบำรุงรักษาอุปกรณ์ที่หน่วยงานเป็นผู้ดูแลอย่างสม่ำเสมอ โดยมีหัวข้อสำคัญดังนี้

(1) มีการบำรุงรักษาระบบอุปกรณ์และระบบสนับสนุนการทำงานของอุปกรณ์ตามคำแนะนำของผู้ผลิต

(2) อนุญาตเฉพาะบุคลากรที่ผ่านการฝึกอบรมและได้รับการมอบหมายให้ทำการซ่อมบำรุงรักษา

(3) ในกรณีที่ใช้บริการซ่อมบำรุงจากหน่วยงานภายนอกจะต้องกำหนดเงื่อนไข และรอบระยะเวลาในการบำรุงรักษาอย่างละเอียด

7.2.5 **ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานภายนอกสำนักงาน** (Security of equipment and assets off-premises)

การนำอุปกรณ์ออกนอกสำนักงานจะต้องได้รับอนุมัติจากเจ้าของอุปกรณ์ ผู้จัดการฝ่ายหรือผู้มีอำนาจในการอนุมัติ เมื่อมีความประสงค์ในการนำอุปกรณ์ออกนอกสำนักงาน โดยมีข้อกำหนด ดังนี้

(1) นำอุปกรณ์ติดตัวอยู่ตลอดเวลา และไม่ทิ้งอุปกรณ์ไว้โดยไม่มีผู้ดูแล

(2) กำหนดกระบวนการจัดการข้อมูลที่มีความสำคัญที่อยู่ในอุปกรณ์ หากอุปกรณ์ชำรุดหรือสูญหาย

(3) มีการดูแลรักษาอุปกรณ์ตามคำแนะนำของผู้ผลิต

(4) การจัดการข้อมูล ต้องเป็นไปตามมาตรฐานการจัดการข้อมูลตามระดับชั้นสูงสุดที่มีอยู่ภายในอุปกรณ์นั้น เช่น การทำ disk encryption หากเป็นข้อมูลระดับลับขึ้นไป

7.2.6 **การเคลื่อนย้ายทรัพย์สินออกนอกสำนักงาน** (Removal of assets)

การนำทรัพย์สินออกนอกอาคารสำนักงาน จะต้องได้รับการอนุญาตจากเจ้าของทรัพย์สินเพื่อป้องกันการเคลื่อนย้ายโดยไม่ได้รับอนุญาต โดยมีแนวปฏิบัติ ดังนี้

(1) กำหนดผู้มีสิทธิในการเคลื่อนย้ายทรัพย์สินสารสนเทศ หากผู้ที่เคลื่อนย้ายเป็นผู้ที่ได้รับมอบหมายและเป็นส่วนหนึ่งในหน้าที่ความรับผิดชอบ ให้ระบุหน้าที่ ลักษณะงานในข้อตกลง หรือสัญญาให้ชัดเจน

(2) มีการบันทึกและตรวจสอบทรัพย์สินทุกครั้งที่มีการนำเข้า-ออกสำนักงานอย่างเป็นลายลักษณ์อักษร

7.2.7 **การทำลายหรือนำอุปกรณ์กลับมาใช้ใหม่** (Secure disposal or reuse of equipment)

เมื่อใช้งานอุปกรณ์เสร็จหรือต้องการนำอุปกรณ์กลับมาใช้ใหม่ให้ปฏิบัติดังนี้

(1) บันทึกการลบ ทำลาย ซ่อม หรือนำกลับมาใช้ใหม่ของสื่อบันทึกข้อมูลที่สำคัญ

(2) ตรวจสอบลิขสิทธิ์ซอฟต์แวร์โดยมีการถอดถอนหรือยกเลิกการลงทะเบียนเพื่อให้สามารถนำซอฟต์แวร์ไปติดตั้งที่เครื่องอื่นได้

(3) เมื่อไม่ต้องการใช้ข้อมูลที่จัดเก็บอยู่ในอุปกรณ์ให้ทำการลบเพื่อป้องกันไม่ให้มีการเข้าถึง และสามารถนำข้อมูลมาใช้โดยไม่ได้รับอนุญาต โดยทำการลบ เขียนซ้ำ หรือทำลายข้อมูลอย่างถาวร

7.2.8 **อุปกรณ์ของผู้ใช้งานที่ทิ้งไว้โดยไม่มีผู้ดูแล** (Unattended user equipment)

อุปกรณ์ที่ทิ้งไว้ ณ ช่วงเวลาหนึ่งโดยไม่มีผู้ดูแล ผู้ใช้งานต้องดูแลและป้องกันอุปกรณ์อย่างเหมาะสม ดังนี้

(1) ผู้ใช้งานจะต้องเปิดใช้งานการล็อกหน้าจอเมื่อออกจากเครื่องคอมพิวเตอร์ โดยไม่มีใครดูแล

(2) ผู้ใช้งานจะต้องเปิดใช้งานการล็อกหน้าจอทุกครั้งเมื่อไม่ใช้งาน

(3) เครื่องคอมพิวเตอร์และเทอร์มินัลทั้งหมด จะต้องมีโปรแกรมรักษาหน้าจอที่ป้องกันด้วยรหัสผ่านหรือการควบคุมอื่นๆ ที่เปิดใช้งานหลังจากไม่มีการใช้งานเป็นระยะเวลาหนึ่ง (สูงสุด 15 นาที)

7.2.9 **การดูแลโต๊ะทำงานให้ปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์** (Clear desk and clear screen policy)

(1) ข้อมูลที่จัดเก็บในสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ จะต้องได้รับการป้องกันจำแนกตามประเภทของข้อมูลที่กำหนดไว้ ในแนวปฏิบัติการจัดระดับชั้นความลับ การติดป้ายและการจัดเก็บข้อมูล

(2) ผู้ใช้งานไม่ควรวางเอกสารสำคัญบนโต๊ะทำงานและตั้งค่าตามแนวปฏิบัติป้องกันหน้าจอคอมพิวเตอร์เพื่อป้องกันการเข้าถึงข้อมูลทางกายภาพต่อเอกสารและข้อมูลสำคัญของบริษัท

(3) คอมพิวเตอร์ที่ใช้งานจะต้องตั้ง screen saver ที่มีรหัสผ่านเพื่อป้องกันการใช้ หรือมีมาตรการอื่นๆ ควบคุมเช่น การสแกนนิ้วมือ เป็นต้น โดยให้เริ่มล็อกหน้าจอเมื่อไม่ได้ใช้งานคอมพิวเตอร์นานเกิน 5 นาที

(4) เมื่อไม่อยู่ที่โต๊ะทำงาน ต้องกดล็อกหน้าจอทันที ก่อนออกไปจากโต๊ะ

(5) ควรจัดเก็บเอกสารข้อมูลที่สำคัญของบริษัทไว้ในที่มิดชิด รวมถึงสื่อบันทึกข้อมูลควรมีการเข้ารหัสป้องกันโดยเอกสารและสื่อที่เก็บข้อมูลควรเก็บไว้ในที่มิดชิด หรือใส่ตู้ที่มีกุญแจล็อก

(6) จะต้องไม่ติด user name/password ไว้ที่หน้าจอ

(7) ตรวจสอบทุกครั้งว่าไม่มีเอกสารใดๆ ค้างอยู่ที่เครื่องถ่ายเอกสาร หรือเครื่องส่งแฟกซ์ หลังจากถ่ายสำเนา หรือส่งแฟกซ์เสร็จแล้ว

(8) ไม่มีเอกสารสำคัญ หรือ เอกสารลับ ค้างไว้ที่เครื่องถ่ายสำเนา หรือ เครื่องส่งแฟกซ์

(9) โทรศัพท์มือถือ(ที่เป็นของบริษัท) ควรตั้งรหัสผ่านหน้าจอ

(10) อุปกรณ์ที่สำคัญอื่นๆ เช่น USB thump drive/External HDD/ etc. ไม่ควรวางทิ้งไว้บนโต๊ะ

(11) กรณีใช้ notebook หลังเลิกงาน ควรเก็บไว้ในลิ้นชัก ถ้าไม่เก็บ ให้พับหน้าจอและมีสายล็อกเครื่องไว้

8. ความมั่นคงปลอดภัยสำหรับการปฏิบัติงาน (Operations security)

8.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational procedure and responsibilities)

8.1.1 **กระบวนการในการปฏิบัติงานซึ่งกำหนดไว้เป็นลายลักษณ์อักษร** (Documented operating procedures)

ต้องจัดทำขั้นตอนการปฏิบัติงานของระบบที่ใช้ในการปฏิบัติงานทั้งหมดเพื่อให้มั่นใจว่าจะมีการใช้งานอย่างเหมาะสมและปลอดภัย ขั้นตอนการปฏิบัติงานควรระบุถึงหัวข้อต่างๆ ที่เกี่ยวข้อง ดังต่อไปนี้

(1) ขั้นตอนการปฏิบัติในการเปิดเครื่องและปิดเครื่อง พร้อมทั้งระบุหน้าที่รับผิดชอบ

(2) กำหนดขั้นตอนการปฏิบัติงาน ควรแสดงรอบระยะเวลา/เกณฑ์ที่ต้องมีการดำเนินการ และ/หรือวิธีการจัดการข้อผิดพลาดที่พบ รวมถึงระบุความเชื่อมโยงหรือความเกี่ยวข้องกับระบบอื่นๆ ที่สำคัญ

(3) มีการควบคุมและลงทะเบียนเอกสาร รวมถึงมีการทบทวนเอกสารให้เป็นปัจจุบันอยู่เสมอ

8.1.2 **การบริหารการเปลี่ยนแปลง** (Change management)

การเปลี่ยนแปลงใดๆ ของระบบ/ขั้นตอนการปฏิบัติงานต้องสอดคล้องกับกระบวนการบริหารการเปลี่ยนแปลงในการปฏิบัติงาน และมีแนวปฏิบัติที่สำคัญ ดังนี้

(1) มีการขออนุมัติการเปลี่ยนแปลงก่อนดำเนินการทุกครั้ง

(2) หลีกเลี่ยงการดำเนินงานในช่วงเวลาที่มีการใช้งานเป็นจำนวนมาก เพื่อหลีกเลี่ยงผลกระทบที่อาจเกิดขึ้นกับผู้ใช้งาน

(3) ประเมินผลกระทบจากการเปลี่ยนแปลงและกำหนดแผนสำรองเพื่อใช้กู้คืน หากการดำเนินงานไม่สัมฤทธิ์ผล

8.1.3 **การบริหารจัดการความสามารถของระบบ** (Capacity management)

ต้องจัดให้มีการบริหารทรัพยากรสารสนเทศให้เพียงพอกับความต้องการใช้งานของระบบ

(1) ควรมีการวางแผนระดับความต้องการทรัพยากรของระบบอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าทรัพยากรของระบบที่ใช้งานอยู่เพียงพอที่จะรองรับปริมาณการใช้งานที่เพิ่มขึ้น

(2) ควรกำหนดระดับการเตือนและระดับแจ้งเตือนเพื่อใช้เป็นจุดอ้างอิงในการปรับแต่งระบบต่อไป

8.1.4 **การแบ่งแยกสภาพแวดล้อมสำหรับการปฏิบัติงาน การพัฒนา และการทดสอบ** (Separation of development, testing and operational environments)

(1) ควรแยกซอฟต์แวร์ในการปฏิบัติงาน การพัฒนา และการทดสอบให้อยู่ในโดเมนหรือไดเรกทอรี่ที่ต่างกันออกไป

(2) สภาพแวดล้อมในการปฏิบัติ การทดลอง และการพัฒนาต้องถูกแยกด้านตรรกะออกจากกัน และสภาพแวดล้อมของผู้ใช้ควรทำการดูแลแบบแยกส่วนกัน

(3) ต้องลบบัญชีทดลอง และบัญชีผู้พัฒนาออกจากสภาพแวดล้อมการปฏิบัติงาน

8.2 **การป้องกันซอฟต์แวร์ประสงค์ร้าย** (Protection from malware)

เครื่องคอมพิวเตอร์จะต้องติดตั้งและเปิดใช้งานซอฟต์แวร์ตรวจจับไวรัสที่ผ่านการอนุมัติแล้ว โดยจะต้องมีการปรับปรุงข้อมูลไวรัสให้ทันสมัยอย่างสม่ำเสมอ

(1) พนักงานทุกคนจะต้องได้รับความรู้และคำแนะนำเกี่ยวกับการป้องกันและจัดการไวรัส

(2) ผู้ใช้จะต้องติดตั้งซอฟต์แวร์ที่ได้รับการอนุมัติแล้วเท่านั้น หากซอฟต์แวร์นั้น ไม่อยู่ในเอกสารรายชื่อซอฟต์แวร์ที่ได้รับการอนมุติ ผู้ติดตั้งต้องดำเนินการขออนุญาตต่อผู้บริหารก่อนทำการติดตั้ง

(3) ผู้ใช้งานจะต้องตรวจสอบให้แน่ใจว่าไฟล์อัปเดตโปรแกรมแอนตี้ไวรัสเป็นข้อมูลล่าสุดก่อนที่จะดาวน์โหลดไฟล์ภายนอกหรือเชื่อมต่อบริการอินเทอร์เน็ต

(4) ผู้ใช้งานจะต้องไม่พยายามเปิดไฟล์ที่ไม่ได้ร้องขอหรือน่าสงสัย ผ่านอีเมลอิเล็กทรอนิกส์ การส่งข้อความแชตหรือระบบเครือข่ายสังคมอื่น ๆ พวกเขาควรพยายามขอคำชี้แจงเกี่ยวกับวัตถุประสงค์ของไฟล์กับผู้ส่งก่อนที่จะทำการเปิด

(5) ผู้ใช้งานจะต้องสแกนสื่อบันทึกข้อมูลภายนอก ซึ่งเคยเชื่อมต่อกับระบบสารสนเทศอื่นที่ไม่ใช่ของบริษัทเพื่อตรวจสอบไวรัส

(6) ผู้ใช้งานจะต้องไม่ท่องเว็บไซต์ที่ไม่คุ้นเคยหรือน่าสงสัย และไม่ควรปิดการทำงานของฟังก์ชัน การป้องกันพ็อปอัป (pop-up) หรือฟิชชิงของโปรแกรมอินเทอร์เน็ตเบราว์เซอร์เมื่อเข้าใช้งานเว็บไซต์ที่ไม่คุ้นเคย

(7) หากอุปกรณ์คอมพิวเตอร์ที่ผู้ใช้งานดูแลติดไวรัสและไม่สามารถจัดการได้ด้วยตนเองให้ดำเนินการ ดังนี้

(1) ตัดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์และระบบเครือข่าย

(2) ติดต่อผู้ดูแลระบบให้เร็วที่สุด

(3) ไม่พยายามลบหรือแก้ไขไฟล์ระบบ (System Files) ด้วยตนเอง

(4) ให้ความร่วมมือผู้ดูแลระบบในการแก้ไขปัญหาจนกว่าผู้ดูแลระบบจะตรวจสอบว่าไวรัสทั้งหมดถูกลบออกแล้ว

(5) หากการดูแลระบบไม่สามารถลบไวรัสทั้งหมดในระบบที่ติดไวรัส ซอฟต์แวร์และไฟล์ทั้งหมดในคอมพิวเตอร์ จะต้องถูกลบรวมถึงข้อมูลการบูตเครื่องหากจำเป็น และซอฟต์แวร์จะได้รับการติดตั้งใหม่และสแกนหาไวรัสอีกครั้ง

8.3 การสำรองข้อมูล (Backup)

(1) จะต้องมีการสำรองข้อมูลเป็นประจำตามแนวทางในการสำรองข้อมูล

(2) ควรมีการกำหนดขั้นตอนในการสำรองข้อมูลที่จะนำมาใช้งาน

(3) ข้อมูลแต่ละส่วนควรมีช่วงเวลาแนะนำในการเก็บรักษาข้อมูลที่เป็นไปตามข้อกำหนดทางธุรกิจ

(4) กลยุทธ์การสำรองข้อมูลต้องเป็นไปตามช่วงเวลาการเก็บรักษาข้อมูลเฉพาะที่ระบุในตารางการเก็บรักษาข้อมูล

(5) ข้อมูลที่เก็บบนระบบสารสนเทศและข้อมูลที่เก็บบนสื่อบันทึกสำรองต้องเป็นไปตาม หรือมากกว่าที่ระบุไว้ในช่วงเวลาการเก็บรักษาข้อมูล

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

8.4 การบันทึกข้อมูลและการเฝ้าระวัง (Logging and monitoring)

8.4.1 การติดตามตรวจสอบการใช้งานของผู้ใช้งานระบบ

กลุ่มเทคโนโลยีสารสนเทศ และเจ้าของระบบกำหนดให้ผู้ดูแลระบบสารสนเทศและระบบเครือข่ายมีการตรวจสอบการใช้งานระบบอย่างสม่ำเสมอ หรืออย่างน้อยปีละ 2 ครั้ง โดยกำหนดให้ใช้เกณฑ์ในการติดตามดังนี้

(1) ความพยายามเข้าใช้งานที่ไม่สำเร็จ

(2) การแก้ไขการตั้งค่าโดยไม่ได้รับอนุญาต

(3) การเข้าถึงโดยไม่ได้รับอนุญาต

(4) ทรัพยากรที่มีการเข้าถึงโดยไม่ได้รับอนุญาต

(5) IP ที่ไม่รู้ที่มาหรือไม่ได้ลงทะเบียน

(6) การเข้าถึงในช่วงเวลาผิดปกติ

(7) เหตุผิดปกติหรือเหตุต้องสงสัยอื่นๆ

หากพบว่ามีเหตุผิดปกติหรือเหตุต้องสงสัย ผู้ดูแลระบบจะต้องดำเนินการวิเคราะห์ ตรวจสอบ ดำเนินก แก้ไข รวมถึงรายงานไปยังผู้เกี่ยวข้องทันที

8.4.2 การบันทึกข้อมูลผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

ในการตรวจสอบผู้ใช้งานระบบ จะต้องมีการเปิดบันทึกข้อมูลผู้ใช้งาน(logs) ซึ่งแบ่งออกเป็นระดับระบบปฏิบัติการและระดับแอปพลิเคชัน โดยจะต้องประกอบไปด้วยข้อมูลอย่างน้อยดังต่อไปนี้

(1) รหัสประจำตัวผู้ใช้

(2) วันที่และช่วงเวลาที่เข้าใช้งานและออกจากการใช้งาน

(3) เครื่องหรือตำแหน่งที่ใช้ในการเข้าใช้งาน หากสามารถระบุได้

(4) บันทึกการพยายามเข้าใช้งานระบบทั้งที่ประสบความสำเร็จและที่ถูกปฏิเสธ

(5) บันทึกการพยายามเข้าใช้งานแอพลิเคชั้นทั้งที่ประสบความสำเร็จและที่ถูกปฏิเสธ หากสามารถทำได้

(6) บันทึกการพยายามเข้าใช้งานข้อมูลและทรัพยากรอื่นๆ ทั้งที่ประสบความสำเร็จและที่ถูกปฏิเสธ

(7) การเปิดบันทึกจะต้องสามารถตรวจสอบกิจกรรมที่เกิดขึ้นจากผู้ใช้แต่ละคนได้ ซึ่งรวมไปถึงเจ้าหน้าที่ดูแลระบบที่มีหน้าที่ดูแลจัดการเครื่องแม่ข่าย

(8) ต้องมีการบันทึกการดำเนินการของผู้ดูแลระบบและผู้ใช้งาน

(9) ต้องมีการบันทึกการใช้งานผ่านสิทธิพิเศษของผู้ดูแลระบบ

(10) ต้องมีการบันทึก (logs) ผู้ใช้งานจัดทำโดยผู้ดูแลระบบ

(11) ควรมีการตั้งเวลาของระบบทั้งหมดให้ตรงกันเพื่อช่วยในการวิเคราะห์ลำดับการเกิดขึ้นของเหตุการณ์

(12) ต้องมีการป้องกันบันทึกข้อมูลการใช้งาน (logs) จากการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและมีการจัดเก็บบันทึกการเข้าใช้งาน (logs) ไว้อย่างน้อย 90 วัน

8.4.3 การตั้งเวลาให้ตรงกัน

กำหนดให้ระบบเทคโนโลยีสารสนเทศ เครื่องคอมพิวเตอร์ และอุปกรณ์ที่สามารถตั้งเวลาได้มีการเชื่อมต่อสัญญาณนาฬิกาไปที่แหล่งตั้งเวลาที่เชื่อถือได้ เพื่อให้เวลาตรงกันและช่วยในการวิเคราะห์ลำดับการเกิดขึ้นของเหตุการณ์

8.4.4 การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of operational software)

(1) มีการควบคุมซอฟต์แวร์ที่ใช้ในการปฏิบัติงาน

(2) การปรับปรุงรายการซอฟต์แวร์ดำเนินงานซึ่งสนับสนุนหน้าที่สำคัญต่างๆ ต้องกระทำโดยเจ้าหน้าที่ ที่ได้รับมอบหมายเท่านั้น และต้องบันทึกความเคลื่อนไหวทั้งหมดของรายการซอฟต์แวร์ที่ใช้ในการดำเนินงาน

(3) ต้องกำหนดกระบวนการติดตั้งซอฟต์แวร์ที่ใช้ในการดำเนินงาน

8.4.5 **การบริหารจัดการช่องโหว่ทางเทคนิค** (Technical vulnerability management)

(1) มีการระบุบทบาทและหน้าที่ความรับผิดชอบ รวมไปถึงการเฝ้าระวังช่องโหว่ การประเมินความเสี่ยง การปิดช่องโหว่ การติดตามทรัพย์สิน และการประสานงานอื่นๆที่จำเป็น

(2) กำหนดขั้นตอนการจัดการตัวแก้ไขซอฟต์แวร์เพื่อการบริหารตัวปรับปรุงประสิทธิภาพด้านความปลอดภัยของระบบปฏิบัติการโปรแกรม

8.4.6 **สิ่งที่ต้องพิจารณาในการตรวจสอบระบบ** (Information systems audit considerations)

(1) มีการควบคุมการตรวจสอบระบบข้อมูล

(2) ขอบเขตการตรวจสอบระบบต้องได้รับความเห็นชอบและการควบคุมเพื่อให้มั่นใจว่า การเข้าใช้งานเพื่อตรวจสอบจะถูกจำกัดขอบเขตตามขอบเขตงานที่ตกลงกัน

(3) การตรวจสอบระบบต้องดำเนินการตามความคิดเห็นทางด้านการตรวจสอบระบบ กระบวนการข้อกำหนด และหน้าที่ความรับผิดชอบในการตรวจสอบระบบต้องทำอย่างเป็นทางการ

(4) ต้องวางแผนถึงข้อกำหนดในการตรวจสอบระบบ และกิจกรรมต่างๆที่เกี่ยวข้องกับการตรวจเช็คซอฟต์แวร์และข้อมูลปฏิบัติการ ทั้งนี้ต้องได้รับความเห็นชอบจากผู้บริหารที่เกี่ยวข้องก่อนเพื่อลดความเสี่ยงของเหตุไม่พึงประสงค์ที่อาจเกิดขึ้นได้ ข้อกำหนดสำหรับการดำเนินการพิเศษ หรือเพิ่มเติมใดๆ ต้องระบุไว้ในแผนการตรวจสอบและได้รับความเห็นชอบเช่นกัน

(5) ขอบเขตการตรวจเช็คระบบต้องได้รับความเห็นชอบและควบคุม เพื่อที่จะมั่นใจได้ว่าการเข้าถึงการตรวจสอบนั้นอยู่ภายใต้ขอบเขตที่วางไว้

(6) ต้องมีการระบุทรัพยากรเทคโนโลยีสารสนเทศที่ใช้ในการตรวจสอบระบบ และต้องพร้อมใช้งานเสมอ

(7) ทำการตรวจสอบระบบด้วยซอฟต์แวร์และข้อมูลอ่านอย่างเดียวเท่านั้น ไม่สามารถแก้ไขและบันทึกทับได้

(8) การอนุญาตให้เข้าถึงไฟล์ที่นอกเหนือจากไฟล์อ่านอย่างเดียวนั้น สามารถทำได้ในการแยกสำเนาของไฟล์ระบบเท่านั้น ที่จะถูกลบทันทีเมื่อการตรวจสอบเสร็จสิ้น

(9) การเข้าถึงระหว่างมีการตรวจสอบระบบนั้น จะต้องมีการเฝ้าระวัง และ บันทึกไว้เพื่ออ้างอิง

9. ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

9.1 การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network security management)

9.1.1 การควบคุมเครือข่าย (Network controls)

(1) ควรมีการป้องกันเครือข่ายจากการบุกรุกโดยไม่ได้รับอนุญาตผ่านทางการจัดรูปแบบของเครือข่าย (Topology) การเลือกเส้นทางของข้อมูล (Routing) ความสามารถในการเชื่อมต่อ (Connectivity) และการควบคุมการเข้าใช้งาน (Access Control)

(2) ควรจัดทำเอกสารแสดงผังการเชื่อมต่อของเครือข่าย (Network Diagram) และปรับปรุงให้ทันสมัยอยู่เสมอเมื่อมีการเปลี่ยนแปลงเครือข่าย

(3) อนุญาตให้เฉพาะเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่เกี่ยวข้องกับการดำเนินงานของบริษัทที่ได้รับอนุญาตเท่านั้นในการเชื่อมต่อกับระบบเครือข่าย

(4) เฝ้าระวังและจัดเก็บบันทึกการเข้าใช้งาน (logs) ที่เกิดขึ้นจากการใช้บริการเครือข่าย

9.1.2 **ความมั่นคงปลอดภัยในการให้บริการเครือข่าย** (Security of network services)

(1) การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(2) ต้องมีการยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกบริษัท (user authentication for external connections) และต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกบริษัทสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของบริษัทได้

(3) การแบ่งแยกเครือข่าย ต้องมีการจัดแบ่งกลุ่มเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(4) บุคคลภายนอกสามารถเข้าถึงบริการในเครือข่ายบริการสาธารณะได้แต่ไม่มีสิทธิเข้าถึงทรัพยากรภายในของบริษัท

(5) ไม่อนุญาตให้บุคคลภายนอกเชื่อมต่อกับเครือข่ายสำนักงานโดยไม่ได้รับอนุญาตอย่างเป็นทางการจากเจ้าของระบบ ในกรณีที่การเชื่อมต่อได้รับการอนุมัติ ควรตรวจสอบกิจกรรมบนเครือข่ายของบุคคลภายนอก

(6) ต้องใช้เฉพาะอุปกรณ์ต่อพ่วงไร้สายที่ได้รับการอนุญาตให้ติดตั้งภายในสำนักงาน รวมถึงห้องเซิร์ฟเวอร์และห้องอุปกรณ์

9.2 **การถ่ายโอนสารสนเทศ** (Information transfer)

9.2.1 **แนวปฏิบัติและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนข้อมูลสารสนเทศ** (Information transfer policies and procedures)

เพื่อให้การแลกเปลี่ยนข้อมูลสารสนเทศทั้งในและนอกบริษัท มีความมั่นคงปลอดภัยเป็นไปตามระดับชั้นความลับของข้อมูล จึงได้จัดทำข้อกำหนดในการแลกเปลี่ยนข้อมูลสารสนเทศ ดังนี้

(1) การแลกเปลี่ยนข้อมูลสารสนเทศในบริษัท

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

(2) การแลกเปลี่ยนข้อมูลสารสนเทศระหว่างองค์กร

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงต้องกำกับให้จัดหา กำหนดมาตรการ และใช้งานระบบสารสนเทศทางธุรกิจที่มีความเชื่อมโยงกัน โดยมีแนวปฏิบัติ ดังนี้

a. วิเคราะห์ความเสี่ยงและกำหนดมาตรการจัดการความเสี่ยงที่เกิดจากการใช้งานระบบสารสนเทศที่เชื่อมโยงกันระหว่างหน่วยงาน โดยการประเมินความเสี่ยงของการเข้ามาใช้ข้อมูลจากหน่วยงานภายนอก โดยพิจารณาประเด็นต่างๆ ดังต่อไปนี้
   - รูปแบบของการเข้าถึงข้อมูลสารสนเทศ
   - ประเภทของข้อมูลสารสนเทศที่ต้องการใช้ในการแลกเปลี่ยน
   - มาตรฐานทางเทคนิคในการบันทึกและอ่านข้อมูลสารเทศ ตลอดจนซอฟต์แวร์ที่เกี่ยวข้อง
   - ข้อมูลหรือซอฟต์แวร์ที่ต้องการจะส่ง หรือมาตรการ/ กระบวนการในการแลกเปลี่ยนสื่อบันทึกข้อมูล
   - มาตรการอื่นๆ ที่จำเป็นในการป้องกันข้อมูลที่สำคัญ เช่น การใช้กุญแจในการเข้ารหัสข้อมูล เป็นต้น
   - ทบทวนมาตรการ (Controls) ตามที่ได้กำหนดไว้สำหรับการเข้าออกสถานที่ตลอดจนการเข้าถึงระบบ หากมีความจำเป็นอาจเพิ่มมาตรการเพื่อลดความเสี่ยงที่มีแนวโน้มว่าจะเกิดขึ้น ทั้งนี้มาตรการทั้งหมดควรต้องได้รับการวางแผนและนำมาใช้อย่างเป็นทางการต่อไป
b. กำหนดให้มีการเผยแพร่ข้อมูลที่เกี่ยวข้องผ่านทางระบบเทคโนโลยีสารสนเทศ เช่น อีเมล ปฏิทินส่วนกลาง (Public Calendar) อินทราเน็ต ฯลฯ ตามความจำเป็น
c. ให้ปฏิบัติตามระเบียบ แนวปฏิบัติ และข้อกำหนดของบริษัท ในการใช้งานระบบเทคโนโลยีสารสนเทศ
d. แบ่งแยกระบบที่มีข้อมูลสำคัญออกจากโซนการใช้งานทั่วไป หรือจำกัดสิทธิการเข้าถึงเฉพาะพนักงานที่มีความจำเป็นเท่านั้น
e. ต้องมีสัญญาหรือข้อตกลงเพื่อระบุความรับผิดชอบของฝ่ายที่รับข้อมูล รวมทั้งระบุมาตรฐานในการบรรจุเอกสารหรือข้อมูล และการส่งอย่างชัดเจน

(3) การเผยแพร่ข้อมูลสู่สาธารณะ

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงจัดให้เว็บไซต์ที่ใช้เผยแพร่ข้อมูลสู่สาธารณะ (www.jts.co.th) มีแนวปฏิบัติในการบริหารจัดการ ดังนี้

a. มีการดูแลข้อมูลทะเบียนโดเมนเทียบเท่ากับทรัพย์สินมีค่าอื่นๆ
b. เนื้อหาแต่ละส่วนที่อยู่ในเว็บไซต์จะต้องได้รับการอนุมัติโดยผู้บริหารระดับสูงที่เกี่ยวข้องก่อนที่จะมีการเผยแพร่ออกสู่สาธารณะ
c. จัดเก็บบันทึกการทบทวนเนื้อหาและข้อมูลอนุมัติการเผยแพร่ข้อมูลออกสู่สาธารณะอย่างเป็นทางการ
d. มีการเฝ้าระวังเนื้อหาในเว็บไซต์เพื่อให้มั่นใจได้ว่า ข้อมูลที่เผยแพร่เป็นข้อมูลที่เกี่ยวข้อง เป็นประโยชน์ และถูกต้อง
e. มีการเฝ้าระวังและตรวจสอบความถูกต้องของข้อมูลไม่ให้มีการเปลี่ยนแปลง แก้ไข โดยไม่ได้รับอนุญาต

9.2.2 **ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ** (Agreement on information transfer)

การถ่ายโอนสารสนเทศระหว่างบริษัทกับหน่วยงานภายนอกทั้งหมด จะต้องมีการร่วมลงนามในสัญญาว่าด้วยข้อกำหนดด้านความมั่นคงปลอดภัยในการแลกเปลี่ยนข้อมูลสารสนเทศ รวมถึงการจัดส่งข้อมูล และ/หรือ ซอฟต์แวร์ และการจัดการแลกเปลี่ยนสื่อบันทึกข้อมูล

9.2.3 **การใช้งานระบบจดหมายอิเล็กทรอนิกส์** (Electronic messaging)

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

(2) ห้ามส่งข้อมูลลับไปยังหน่วยงานอื่น ทั้งภายในและภายนอกหากไม่ได้รับอนุญาตอย่างเป็นทางการ และข้อมูลต้องได้รับการป้องกันตามแนวทางการจัดการตามระดับชั้นสูงสุดของข้อมูลนั้น

(3) อีเมลทั้งหมดควรมีการบันทึกถึงข้อตกลงการรักษาความลับ และระบุข้อความการปฏิเสธความรับผิดชอบหากมีการนำอีเมลไปใช้งานโดยไม่ได้รับอนุญาต

(4) ไม่อนุญาตให้ทำการปลอมแปลงต้นทางของการสื่อสารอิเล็กทรอนิกส์ การเปลี่ยนแปลงข้อมูลของระบบที่ใช้ในการระบุที่มาของข้อความ หรือปิดบังต้นทางของการสื่อสาร

(5) ห้ามมิให้เข้าถึงระบบเพื่อพยายามในการเฝ้าติดตาม อ่าน คัดลอก ลบ หรือเจาะเข้าไปในการสื่อสารทางอิเล็กทรอนิกส์ของบุคคลอื่นโดยไม่ได้รับความยินยอมจากบุคคลนั้น (ยกเว้นบุคลากรระบบเครือข่ายที่ได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร)

(6) ไม่ควรใช้ระบบอีเมลเก็บข้อมูลสะสมไว้เป็นเวลานาน

(7) ห้ามใช้ฟังก์ชัน Automatic Forward เพื่อการส่งอีเมลต่อไปให้คอมพิวเตอร์ที่ไม่ใช่ของบริษัท

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

9.2.4 การใช้งานระบบอินเทอร์เน็ตและเครือข่ายออนไลน์อย่างปลอดภัย

(1) ผู้ใช้งานจะต้องใช้อินเทอร์เน็ต และการส่งข้อความแชต เพื่อวัตถุประสงค์ในการปฏิบัติงานเท่านั้น

(2) เฉพาะเจ้าหน้าที่ที่ได้รับอนุญาตเท่านั้นที่สามารถเป็นตัวแทนบริษัท เพื่อการสื่อสารบนเครือข่ายออนไลน์ได้

(3) ผู้ใช้งานจะต้องปฏิบัติตามกฎหมายลิขสิทธิ์และอ้างอิงแหล่งที่มาอย่างเหมาะสม เมื่อโพสต์เนื้อหาในโซเชียลมีเดีย

(4) ผู้ใช้งานจะต้องไม่เผยแพร่ โพสต์หรือปล่อยข้อมูลใด ๆ ที่ถือว่าเป็นความลับหรือไม่เปิดเผยต่อสาธารณะ

(5) ห้ามใช้โลโก้และเครื่องหมายการค้าของบริษัท โดยไม่ได้รับความยินยอมเป็นลายลักษณ์อักษร

(6) การโพสต์ข้อความใดๆ ที่เกี่ยวข้องกับบริษัทจะต้องได้รับอนุญาตอย่างเป็นทางการก่อน

(7) ห้ามเผยแพร่ข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากเจ้าของข้อมูลอย่างถูกต้อง

(8) ผู้ใช้งานที่เยี่ยมชมเว็บไซต์ลามกอนาจาร อาจจะถูกลงโทษทางวินัยและอาจถูกเลิกจ้าง

ผู้ใช้งานควรใช้งานระบบ internet, Intranet และ E-Mail ด้วยความรอบคอบและมีวิจารณญาณ โดยให้ระลึกเสมอว่าพนักงานคือตัวแทนของบริษัทในการทำธุรกิจ

9.2.5 ข้อตกลงในการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or non-disclosure agreements)

ให้ผู้บริหาร พนักงานทุกคน รวมถึงพนักงานจากหน่วยงานทั้งภายในและภายนอกบริษัทที่ใช้ระบบสารสนเทศ ต้องทำข้อตกลงการรักษาความลับของข้อมูล โดยให้มีข้อความระบุไม่ให้เปิดเผยความลับไปยังผู้ที่ไม่เกี่ยวข้องและให้ลงลายมือชื่อรับทราบ โดยข้อความควรประกอบด้วยหัวข้อ ดังนี้

(1) ห้ามเปิดเผยความลับไปยังผู้ที่ไม่เกี่ยวข้อง รวมถึงบทลงโทษหรือสิ่งที่จะดำเนินการหากพบว่ามีการละเมิด

(2) ปฏิบัติตามแนวปฏิบัติความมั่นคงปลอดภัยที่เกี่ยวข้องในการไม่เปิดเผยความลับ เพื่อป้องกันไม่ให้ข้อมูลมีการรั่วไหลไปยังผู้ที่ไม่เกี่ยวข้อง

(3) การให้ความร่วมมือในการตรวจสอบกิจกรรมหากพบข้อสงสัยหรือข้อร้องเรียน

10. การควบคุมการเข้าถึง (Access Control)

10.1 ข้อกำหนดทางธุรกิจเรื่องการควบคุมการเข้าถึง (Business requirement of access control)

การเข้าถึงข้อมูลไม่ว่าเกิดจากช่องทางใดก็ตาม จำเป็นต้องมีการควบคุมการเข้าถึงเพื่อให้สอดคล้องกับข้อกำหนดทางธุรกิจและมีความมั่นคงปลอดภัย

10.1.1 แนวปฏิบัติในการควบคุมการเข้าถึง

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงกำกับให้มีการใช้แนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

(1) การเข้าถึงระบบสารสนเทศทั้งในส่วนของพนักงานและบุคคลภายนอก ต้องสอดคล้องตามมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศและคำนึงถึงการรักษาความปลอดภัยของข้อมูลอยู่เสมอ

(2) ระดับการเข้าถึงสอดคล้องกับระดับชั้นความลับของข้อมูลที่สามารถเข้าถึงได้

(3) การอนุญาตให้เข้าถึง ให้ใช้เกณฑ์พิจารณาดังต่อไปนี้

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

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

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

(4) การกำหนดหลักเกณฑ์ในการอนุญาตการเข้าถึง

(4.1) การกำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้องต้องกำหนดสิทธิที่สามารถใช้งานในขอบเขตขั้นต่ำ ดังนี้

- อ่านอย่างเดียว
- สร้างข้อมูล
- แก้ไข
- ประมวลผล
- ไม่มีสิทธิ

(4.2) การกำหนดเกณฑ์การระงับสิทธิ มอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งานที่กำหนดไว้

(4.3) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูงหรือผู้ดูแลระบบที่ได้รับมอบหมาย

(5) การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับของข้อมูลที่สามารถเข้าถึงได้

(5.1) ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับของข้อมูล

(5.2) เจ้าของข้อมูล จะต้องมีการตรวจสอบความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าสิทธิต่างๆที่ให้ไว้ยังคงมีความเหมาะสม

(5.3) วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบ ต้องกำหนดรายชื่อผู้ใช้งานและรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละระดับชั้นความลับของข้อมูล

10.2 การจัดการการเข้าถึงของผู้ใช้งาน (User access management)

กำหนดให้มีกระบวนการเพื่อใช้ในการจัดการลงทะเบียนและเพิกถอนสิทธิผู้ใช้งาน การให้สิทธิการเข้าถึง เพื่อเป็นการป้องกันไม่ให้มีการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

10.2.1 การลงทะเบียนผู้ใช้งาน

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงกำกับให้มีขั้นตอนการลงทะเบียนผู้ใช้งาน การโยกย้าย และการสิ้นสุดความจำเป็นต้องใช้งาน โดยมีแนวปฏิบัติดังนี้

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

(2) บัญชีของผู้ใช้แต่ละคนจะต้องไม่ซ้ำกันและสามารถอ้างอิงกลับไปยังผู้ที่เป็นเจ้าของได้ ในกรณีที่ไม่สามารถหลีกเลี่ยงการใช้บัญชีผู้ใช้ซ้ำ ให้ระบุชื่อผู้ที่ใช้งานร่วมกันและมีการทบทวนรายชื่อผู้ใช้อย่างสม่ำเสมอ

(3) การให้สิทธิสอดคล้องกับแนวปฏิบัติด้านความมั่นคงปลอดภัยของบริษัท

(4) ไม่กำหนดชื่อบัญชีผู้ใช้ที่สื่อถึงหน้าที่ความรับผิดชอบในการปฏิบัติงาน

10.2.2 การบริหารจัดการสิทธิ

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงกำกับให้มีการกำหนดสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศตามความจำเป็นที่ต้องใช้งาน โดยมีแนวปฏิบัติดังนี้

(1) สิทธิที่ให้กับพนักงานและหน่วยงานภายนอกไม่ทำให้ความมั่นคงปลอดภัยด้านสารสนเทศลดลง

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

(3) จำกัดบุคคลที่มีสิทธิผู้ดูแล (Administrator) ซึ่งหากมีความจำเป็นชั่วคราวที่ต้องใช้สิทธิดังกล่าว ให้กำหนดระยะเวลาที่อนุญาตและมีการทบทวนการให้สิทธิอย่างสม่ำเสมอ

(4) ต้องบันทึกสิทธิที่ให้ในแต่ละบัญชีผู้ใช้งานและมีการทบทวนความเหมาะสมของสิทธิที่ได้อย่างสม่ำเสมอ

10.2.3 การบริหารจัดการรหัสผ่านของผู้ใช้งาน

กำหนดให้ผู้ดูแลระบบมีแนวปฏิบัติในการบริหารจัดการรหัสผ่านให้กับผู้ใช้งาน และแนวปฏิบัติของผู้ใช้งานดังนี้

(1) แจ้งรหัสผ่านให้กับผู้ใช้งานโดยตรงโดยไม่มีบุคคลที่สามรับทราบ

(2) กำชับให้ผู้ใช้เปลี่ยนแปลงรหัสผ่านทันที หรือเปลี่ยนครั้งแรกที่มีการใช้งาน

(3) กำหนดให้ผู้ดูแลระบบสอบถามข้อมูลเพื่อยืนยันตัวบุคคลผู้ใช้ทุกครั้งที่ได้รับการร้องขอให้เปลี่ยน/รีเซตรหัสผ่าน ตัวอย่างคำถามของข้อมูลเพื่อยืนยันตัวบุคคล ได้แก่ หมายเลขโทรศัพท์ภายใน รหัสประจำตัวพนักงาน ฯลฯ

(4) รหัสผ่านจะถูกเปลี่ยนอย่างน้อยทุกๆ 90 วันหรือเมื่อใดก็ตามที่มีข้อบ่งชี้ว่าอาจมีการรั่วไหลของข้อมูล

(5) รหัสผ่านที่ใช้ร่วมกัน (share password) จะใช้สำหรับการทดสอบระบบเท่านั้นและได้รับการดูแลรักษาโดยเจ้าของระบบหรือผู้ดูแลระบบที่ได้รับมอบหมาย

(6) รหัสผ่านจะต้องไม่ถูกเก็บไว้ในระบบประมวลผลข้อมูลหรือสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ใด ๆ โดยไม่มีการเข้ารหัสข้อมูลไว้

(7) รหัสผ่านจะไม่ถูกบันทึกไว้ เว้นแต่จะสามารถจัดเก็บได้อย่างปลอดภัย

(8) ผู้ใช้งานจะต้องรับผิดชอบต่อบัญชีผู้ใช้งานและรหัสผ่านของตน และจะไม่เปิดเผยต่อผู้ใดโดยไม่คำนึงถึงสถานการณ์

(9) ผู้ใช้งานจะต้องเปลี่ยนรหัสผ่านทันทีที่เข้าใช้งานครั้งแรก และการกำหนดรหัสผ่านต้องเป็นรหัสผ่านที่มั่นคงปลอดภัย หากมีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพได้

(10) โดยการสร้างรหัสผ่านต้องมีองค์ประกอบดังนี้

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

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

(10.2) ผู้ใช้งานจะต้องพิจารณาสิ่งต่อไปนี้ เมื่อสร้างรหัสผ่านเพื่อเพิ่มความคาดเดายากของรหัสผ่าน:

- ห้ามใช้คำในภาษาสแลง ภาษาถิ่น ฯลฯ
- ห้ามใช้ข้อมูลส่วนบุคคล เช่น ชื่อ (ชื่อของญาติ ชื่อของสัตว์เลี้ยง ฯลฯ) หรือวันที่เช่นวันเกิด วันหยุดและวันครบรอบ (เช่น" 09Aug2009")
- ห้ามใช้คำวลีหรือตัวย่อที่เกี่ยวข้องกับองค์กร (เช่น" JtsiTgs01")
- ห้ามใช้ข้อกำหนดคำสั่งเว็บไซต์ชื่อคอมพิวเตอร์หรือแอปพลิเคชันซอฟต์แวร์ (เช่น" winipcfg", " yahoodotcom")
- ห้ามใช้คำหรือรูปแบบตัวเลข (เช่น" 12345678"," abcdefgh")
- ไม่ควรเพิ่มรหัสผ่านด้วยการเติม/ต่อท้ายอักขระด้วยลำดับเลขที่ (เช่น "oldpassword1", " 1oldpassword")

(11) การเปลี่ยนรหัสผ่านต้องไม่ซ้ำกับ 5 รหัสผ่านเดิมที่เคยตั้งไว้

(12) เนื่องจากการโจมตีแบบฟิชชิงได้แพร่หลายอย่างมากในปัจจุบัน ผู้ใช้งานพึงทราบ บริษัทจะไม่ขอข้อมูลส่วนบุคคลหรือรหัสผ่านใด ๆ จากคุณผ่านสื่ออิเล็กทรอนิกส์หรือเสียง (เช่น facebook, whatsapp, line, อีเมลและโทรศัพท์) ในกรณีที่ได้รับคำขอดังกล่าว พนักงานควรลบข้อความทันทีหรือวางสายโดยไม่สื่อสารต่อเนื่องกับผู้ส่ง / ผู้โทร หากพนักงานมีข้อสงสัยโปรดตรวจสอบความถูกต้องของคำขอกับหน่วยงานด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง (Cyber management)

10.2.4 การทบทวนสิทธิการใช้งาน

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงกำกับให้มีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ โดยมีแนวปฏิบัติดังนี้

(1) การยืนยันความถูกต้องจากหน่วยงานต้นสังกัด ผู้บังคับบัญชา หรือจากเจ้าของทรัพย์สิน

(2) ทบทวนสิทธิอย่างน้อยปีละ 1 ครั้ง ทั้งนี้อาจกำหนดความถี่ให้มากขึ้นสำหรับระบบที่มีความสำคัญสูง

(3) แก้ไขและเปลี่ยนแปลงสิทธิให้ตรงตามผลที่ได้จากการทบทวน

10.3 หน้าที่และความรับผิดชอบของผู้ใช้งาน

กำหนดให้มีการป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตด้วยการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยให้กับผู้ใช้งาน

10.4 การควบคุมการเข้าใช้งานระบบปฏิบัติการ

เพื่อให้มีการควบคุมไม่ให้มีการใช้งานระบบปฏิบัติการโดยไม่ได้รับอนุญาต จึงกำหนดให้มีการพิสูจน์ตัวตน จัดเก็บบันทึกการใช้งาน และเวลาที่อนุญาตให้เข้าถึงระบบสารสนเทศและระบบเครือข่าย

10.4.1 กระบวนการเข้าถึงระบบอย่างมั่นคงปลอดภัย

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงกำกับให้มีการออกแบบวิธีการเข้าถึงระบบต่างๆ ให้ผ่านขั้นตอนการเข้าใช้งานที่มีความมั่นคงปลอดภัยเพื่อลดโอกาสการเข้าถึงโดยไม่ได้รับอนุญาต โดยกำหนดแนวปฏิบัติ ดังนี้

(1) ไม่อนุญาตให้แสดงรายชื่อบัญชีผู้ใช้ที่มีทั้งหมดปรากฏในหน้าแรกการล็อกออน

(2) ไม่ส่งข้อมูลรหัสผ่านในรูปแบบ Clear Text

(3) จำกัดจำนวนครั้งที่ล็อกออนไม่ผ่านเกินกว่า 5 ครั้ง บัญชีใช้งานจะถูกปิดการใช้งานทันที

10.4.2 การระบุและการพิสูจน์ตัวตน

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงกำกับ ส่งเสริมให้มีการบริหารจัดบัญชีผู้ใช้งาน โดยมีแนวปฏิบัติดังนี้

(1) กำหนดให้มีการพิสูจน์ตัวตนในระบบที่อนุญาตให้มีผู้ใช้หลายคน (Multi-user Application) โดยการใช้รหัสผ่านของผู้ใช้งานทุกครั้งในการเข้าสู่ระบบ

(2) ผู้ใช้งานแต่ละคนจะต้องมีบัญชีผู้ใช้ไม่ซ้ำกัน ไม่สามารถใช้ร่วมกัน หรือโอนให้กันได้

(3) ในกรณีที่จำเป็นต้องสร้างบัญชีผู้ใช้กลุ่มเพื่อใช้งานร่วมกันจะต้องได้รับการอนุมัติอย่างเป็นทางการจากผู้บังคับบัญชาของผู้ร้องขอ และจากผู้จัดการฝ่ายที่เกี่ยวข้องที่ดูแลระบบนั้นๆ และมีการควบคุมการใช้งานอย่างเคร่งครัด เช่น กำหนดและบันทึกช่วงเวลาที่ใช้งาน

10.4.3 ระบบบริหารจัดการรหัสผ่าน

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงกำกับ ส่งเสริมให้มีการใช้รหัสผ่านที่มีคุณภาพ โดยมีแนวปฏิบัติดังนี้

(1) ระบบบังคับหรือกำหนดให้ผู้ใช้งานเปลี่ยนแปลงรหัสผ่านทันทีที่เข้าใช้งานครั้งแรก และการกำหนดรหัสผ่านต้องเป็นรหัสผ่านที่มั่นคงปลอดภัย

(2) ตั้งค่าให้ระบบยอมรับเฉพาะรหัสผ่านตามลักษณะของรหัสผ่านที่มีคุณภาพ ตามแนวทางปฏิบัติความปลอดภัยของระบบเทคโนโลยีสารสนเทศสำหรับผู้ใช้งาน

(3) ระบบยินยอมให้ผู้ใช้งานเลือกและเปลี่ยนรหัสผ่านได้ด้วยตนเอง

(4) ระบบบังคับหรือกำหนดให้ผู้ใช้งานไม่สามารถตั้งรหัสผ่านย้อนหลังได้ 5 รหัสผ่านเดิม

(5) ระบบบังคับหรือกำหนดให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน 5 ครั้ง ภายในระยะเวลา 15 นาที หากเกินกำหนดบัญชีใช้งานจะถูกปิดการใช้งานทันที และหลังจาก 15 นาทีจึงจะกลับมาใช้งานได้อีกครั้ง แต่หากการใส่รหัสผิดเกิน 5 ครั้ง ภายในระยะเวลาเกิน 15 นาที บัญชีใช้งานจะถูกปิดการใช้งานทันที และต้องติดต่อผู้ดูแลระบบเพื่อทำการคืนสถานะการใช้งานบัญชี

(6) ระบบบังคับหรือกำหนดให้เปลี่ยนรหัสผ่านอย่างน้อยทุก 90 วัน ยกเว้นกรณีเป็นบัญชีบริการ (Service Account) หรือเป็นข้อจำกัดการเปลี่ยนรหัสผ่านของบัญชีชื่อที่มีการใช้งานที่จำเป็นของระบบสารสนเทศ สำหรับการเชื่อมต่อการทำงานของระบบสารสนเทศต่างๆ

10.4.4 การใช้งานโปรแกรมประเภทอรรถประโยชน์

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงกำกับให้มีแนวปฏิบัติในการใช้งานอรรถประโยชน์ ดังนี้

(1) ห้ามติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ของบริษัท

(2) กำหนดให้มีการจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ โดยซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับต้องมีการลงทะเบียนเพื่อใช้งาน ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ และตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไม่

(3) รายชื่อโปรแกรมประเภทอรรถประโยชน์ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งาน ต้องได้รับการจัดทำเป็นเอกสาร และได้รับการอนุมัติโดยผู้บริหารของสายงานเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าซอฟต์แวร์เหล่านี้มีลิขสิทธิ์ถูกต้องครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ในการทำงานของบริษัทเท่านั้น

(4) ไม่อนุญาตให้ใช้งานโปรแกรมประเภทอรรถประโยชน์ที่ลัดขั้นตอนการพิสูจน์ตัวตน

(5) หากมีความจำเป็นต้องใช้งานโปรแกรมอรรถประโยชน์ที่ลัดขั้นตอนการพิสูจน์ตัวตน จำเป็นต้องมีการประเมินความเสี่ยงที่เกิดจากการใช้งานโปรแกรมอรรถประโยชน์ดังกล่าว มีการอนุมัติอย่างเป็นลายลักษณ์อักษร และเปิดใช้บันทึกเหตุการณ์เสมอ

10.4.5 การหมดเวลาในการใช้งาน

ผู้ดูแลระบบตั้งค่าให้หมดเวลาในการใช้งาน เมื่อไม่มีกิจกรรมการดำเนินงานกับระบบสารสนเทศกำหนดให้ยุติการใช้งานระบบสารสนเทศทุก 15 นาที (Session time-out)

10.4.6 การจำกัดระยะเวลาเชื่อมต่อระบบ

กำหนดให้มีการจำกัดช่วงเวลาในการเชื่อมต่อระบบสารสนเทศจากภายนอกอย่างเหมาะสม โดยกำหนดให้มีการพิสูจน์ตัวตนก่อนทุกครั้งในการเข้าใช้งาน

10.5 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

กำหนดให้มีการควบคุมโปรแกรมหรือแอปพลิเคชันและข้อมูลที่ใช้งานในระบบเทคโนโลยีสารสนเทศเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

10.5.1 การจำกัดการเข้าถึงข้อมูล

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงกำกับให้มีแนวปฏิบัติในการเข้าถึงข้อมูลและโปรแกรม ดังนี้

1) การเข้าถึงสารสนเทศสอดคล้องกับระดับชั้นความลับของข้อมูล

2) กำหนดสิทธิของผู้ใช้งานในโปรแกรม สำหรับสิทธิในการอ่าน เขียน ลบ ฯลฯ ข้อมูลที่อยู่ภายใน ตามหน้าที่ความรับผิดชอบ

3) เมนู/ฟังก์ชันในการใช้งานโปรแกรมสอดคล้องกับสิทธิที่ได้รับ

4) มาตรการควบคุมการเข้าถึงของผู้ใช้บริการ (Outsource) ต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่กำหนดให้เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนอื่น ก็ต้องมีการควบคุมหรือตรวจสอบการเข้าถึงของผู้ให้บริการ โดยให้ผู้ดูแลระบบควบคุมดูแลการทำงานของผู้ให้บริการอย่างใกล้ชิดในกรณีที่ผู้ให้บริการมาปฏิบัติหน้าที่ ที่บริษัท และให้ผู้ดูแลระบบตรวจสอบการทำงานของผู้ให้บริการอย่าง

ละเอียดในกรณีที่เป็นการให้บริการในลักษณะ Remote access และปิด Modem ทันทีที่การให้บริการเสร็จสิ้น

5) กำหนดให้ผู้บริการ (Outsource) ลงนามในสัญญารักษาความลับ

10.5.2 การแบ่งแยกระบบที่มีความสำคัญ

ผู้จัดการกลุ่มเทคโนโลยีสารสนเทศควบคุมให้มีการแบ่งแยกระบบที่มีความสำคัญดังนี้

1) จัดทำรายการระบบซึ่งไวต่อการรบกวน ที่มีผลกระทบและมีความสำคัญสูงต่อบริษัท และแยกระบบออกจากระบบเครือข่ายทั่วไป

2) มาตรการควบคุมการเข้าถึงของระบบซึ่งไวต่อการรบกวนและมีความสำคัญสูงต่อบริษัท จำกัดการเข้าถึงของพนักงาน อุปกรณ์คอมพิวเตอร์ หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้สามารถเข้าถึงได้ ทั้งนี้ไม่อนุญาตให้เข้าถึงและปฏิบัติงานจากภายนอกบริษัทผ่านอุปกรณ์คอมพิวเตอร์และเครื่องมือสื่อสารเคลื่อนที่

3) การดำเนินงานของระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญควรใช้เซิร์ฟเวอร์ที่แยกต่างหาก ในกรณีจำเป็นหากต้องใช้เซิร์ฟเวอร์เดียวกัน กำหนดให้ผู้ดูแลระบบประเมินความต้องการด้านทรัพยากรและออกแบบระบบให้รองรับกับความต้องการ

11. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information System Acquisition Development and Maintenance)

11.1 ข้อกำหนดด้านความปลอดภัยของระบบ (Security requirements of information system)

11.1.1 การวิเคราะห์และข้อกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ

ข้อกำหนดด้านความปลอดภัยสารสนเทศต้องมีการประเมินในระหว่างขั้นตอนการกำหนดความต้องการของผู้ใช้งาน ข้อกำหนดด้านความปลอดภัยอย่างต่ำควรประกอบด้วยด้านต่าง ๆ ต่อไปนี้

(1) การระบุและการตรวจสอบยืนยันตัวบุคคลของผู้ใช้งาน

(2) การควบคุมการเข้าถึงและการอนุญาตให้ใช้งาน

(3) การป้องกันความลับและความสมบูรณ์ครบถ้วนของรายการเปลี่ยนแปลงหรือข้อมูล (Integrity)

(4) ข้อกำหนดการตรวจสอบความถูกต้องของข้อมูลนำเข้า (Input validation)

(5) การจัดการกับข้อผิดพลาดในการประมวลผล (Error handling)

(6) การเข้ารหัสข้อมูล (Encryption) ตามระดับชั้นความลับของข้อมูล

(7) ข้อกำหนดของกฎหมาย หน่วยงานกำกับดูแล และการปฏิบัติให้เป็นไปตามกฎหมาย

11.1.2 ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ

(1) ควรมีมาตรการทางเทคนิคที่ใช้ในการจัดการความมั่นคงปลอดภัย เช่น การเข้ารหัสข้อมูล (encryption) การยืนยันตัวตน ฯลฯ

(2) ข้อตกลงควรจัดทำร่วมกันเพื่อให้ทุกฝ่ายที่เกี่ยวข้องเข้าใจถึงหน้าที่ความรับผิดชอบและข้อผูกพันการใช้ข้อมูลร่วมกันในการปฏิบัติงาน

(3) การเข้าถึงข้อมูลสารสนเทศควรมีการกำหนด ดูแล และควบคุม โดยจะต้องมีการพิจารณาระดับในการเข้าถึง (Authentication Level) ด้วยการประเมินความเสี่ยงจากความต้องการทางธุรกิจ

(4) ควรแบ่งแยกเครือข่ายของระบบสำคัญ ออกจากเครือข่ายสาธารณะ

11.2 การประมวลผลข้อมูลในโปรแกรม

ระบบหรือโปรแกรมที่มีการพัฒนาหรือปรับปรุงเพิ่มเติมจากที่มีการใช้งานอยู่ในปัจจุบัน จำต้องมีการออกแบบให้ตอบรับความต้องการความมั่นคงปลอดภัยตั้งแต่ข้อมูลนำเข้า ประมวลผล ความถูกต้องของข้อความ และข้อมูลนำออก

11.2.1 การตรวจสอบข้อมูลนำเข้า

ผู้จัดการกลุ่มเทคโนโลยีสารสนเทศกำกับ จัดหา ให้ระบบหรือโปรแกรมที่มีการพัฒนาหรือปรับปรุงจากระบบเดิมมีกลไกการตรวจสอบข้อมูลนำเข้า ในหัวข้อดังต่อไปนี้

(1) มีการตรวจสอบช่วงของข้อมูล ได้แก่

- การตรวจสอบลักษณะของข้อมูล เช่น ตัวอักษร ตัวเลข เป็นต้น
- การตรวจสอบความยาวของข้อมูล
- การตรวจสอบช่วงของข้อมูลที่ต้องการ หรือไม่ต้องการ เช่น จำนวนขั้นต่ำ ฯลฯ
- การตรวจสอบความครบถ้วนของข้อมูล
- การป้องกัน Uncontrolled Format Strings

(2) มีการกำหนดกระบวนการหรือกิจกรรมที่ต้องการหากพบความผิดปกติของข้อมูลนำเข้า

11.2.2 การควบคุมระหว่างการประมวลผล

ให้ระบบหรือโปรแกรมที่มีการพัฒนาหรือปรับปรุงจากระบบเดิม มีการควบคุมความเสี่ยงที่เกิดขึ้นจากการประมวลผลข้อมูลผิดพลาด ในด้านต่างๆ อย่างน้อยดังนี้

(1) การใช้ฟังก์ชันเพิ่ม แก้ไข และลบข้อมูล

(2) การกำหนดกลไกในการตรวจสอบและป้องกันไม่ให้มีการแก้ไขข้อมูลระหว่างการประมวลผล

(3) การป้องกัน Buffer Overflows

11.2.3 ความสมบูรณ์ครบถ้วนของข้อความ

ให้ระบบหรือโปรแกรมที่มีการพัฒนาหรือปรับปรุงจากระบบเดิมมีกลไกการตรวจสอบความถูกต้องของข้อความ โดยมีกระบวนการป้องกันไม่ให้ข้อความถูกแก้ไขจากต้นฉบับ หรือหากมีการแก้ไขข้อความนั้นต้องได้รับการพิสูจน์ตัวตนหรือตรวจสอบสิทธิในการเข้าใช้งานก่อน

11.2.4 การตรวจสอบข้อมูลนำออก

ให้ระบบหรือโปรแกรมที่มีการพัฒนาหรือปรับปรุงจากระบบเดิมมีกลไกการตรวจสอบข้อมูลนำออกให้มีผลลัพธ์เป็นไปตามข้อมูลนำเข้า และออกแบบโปรแกรมป้องกันไม่ให้มีการแก้ไขข้อมูลนำออกโดยไม่ได้รับอนุญาต

11.3 มาตรการการเข้ารหัส (Cryptography)

กำหนดให้มีแนวปฏิบัติในการควบคุมการเข้ารหัส หากมีความจำเป็นต้องใช้เทคโนโลยีดังกล่าวในการรักษาความถูกต้องสมบูรณ์ของข้อมูล และพิสูจน์ยืนยันตัวตนทั้งผู้รับและผู้ส่ง

11.3.1 การควบคุมการเข้ารหัส

ผู้จัดการกลุ่มเทคโนโลยีสารสนเทศกำกับให้มีการใช้เทคโนโลยีเข้ารหัสในระบบเทคโนโลยีสารสนเทศ และข้อมูลที่มีความสำคัญสูงโดยเลือกใช้เทคโนโลยีการเข้ารหัส หรืออัลกอริทึมที่ออกแบบเพื่อตอบสนองความต้องการด้านความมั่นคงปลอดภัยและสอดคล้องกับผลการประเมินความเสี่ยง

โดยมีแนวปฏิบัติ ดังนี้

(1) ห้ามไม่ให้มีการติดตั้งซอฟต์แวร์เข้ารหัสที่ไม่ได้รับอนุญาต

(2) การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล และเป็นการเข้ารหัส (Encryption) ที่ยังไม่มีการประกาศช่องโหว่ออกสู่สาธารณะ

(3) การเข้ารหัสไม่ควรต่ำกว่า 256 บิต

(4) เจ้าของข้อมูลที่เป็นความลับให้นำการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากลมาใช้

11.3.2 การบริหารจัดการกุญแจเข้ารหัสข้อมูล

ผู้จัดการกลุ่มเทคโนโลยีสารสนเทศ ควบคุมให้มีการใช้กุญแจเข้ารหัสข้อมูล ดังนี้

(1) มีการใช้กุญแจเข้ารหัสเพื่อสนับสนุนการทำงานของเทคโนโลยีเข้ารหัส

(2) มีการเปลี่ยนกุญแจเข้ารหัสอย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้งสำหรับระบบสารสนเทศที่สำคัญ และสำหรับระบบบริการภายในบริษัทจะมีการเปลี่ยนกุญแจเข้ารหัสอย่างน้อยทุก 3 ปี

(3) มีการเปลี่ยนกุญแจเข้ารหัส และทำลายรหัสเก่าเมื่อมีเหตุต้องสงสัยว่ามีบุคคลที่ไม่ได้รับอนุญาตรู้รหัสดังกล่าว

11.4 ความมั่นคงปลอดภัยของไฟล์ระบบ

กำหนดให้มีการควบคุมไฟล์ระบบ และมีการป้องกันไม่ให้เกิดการรั่วไหลของข้อมูลที่ใช้ในการทดสอบ

11.4.1 การควบคุมซอฟต์แวร์ที่ใช้ในการปฏิบัติงาน

กำหนดให้มีการควบคุมซอฟต์แวร์ที่อนุญาตให้ติดตั้งในเครื่องคอมพิวเตอร์และอุปกรณ์ ดังนี้

(1) ให้ติดตั้งเฉพาะซอฟต์แวร์ที่อยู่ในรายการที่ได้รับอนุญาตเท่านั้น

(2) การติดตั้งซอฟต์แวร์ดำเนินการโดยเจ้าหน้าที่ที่ได้รับการแต่งตั้งหรืออนุญาต

(3) มีการทบทวนรายการซอฟต์แวร์ เวอร์ชัน ที่ได้รับอนุญาตอย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้ง

(4) ไม่อนุญาตให้นำซอฟต์แวร์ที่ยังอยู่ในระหว่างการพัฒนาหรือการทดสอบมาใช้ ในสภาพแวดล้อมการดำเนินการจริง หรือหากมีความจำเป็นต้องใช้ ควรมีการประเมินความเสี่ยงและหามาตรการควบคุมที่เพียงพอ

(5) ไม่อนุญาตให้ใช้ระบบปฏิบัติการหรือซอฟต์แวร์ที่ผู้ผลิตยกเลิกการสนับสนุนการให้บริการ หรือหากมีความจำเป็นต้องใช้ ควรมีการประเมินความเสี่ยงและหามาตรการควบคุมที่เพียงพอ

11.4.2 การป้องกันข้อมูลที่ใช้ในการทดสอบ

กลุ่มเทคโนโลยีสารสนเทศกำหนดให้ควบคุมข้อมูลที่ใช้ในการทดสอบตามแนวปฏิบัติ ดังนี้

(1) ไม่ใช้ข้อมูลจริงในการทดสอบ โดยเฉพาะส่วนที่เป็นข้อมูลส่วนบุคคล ในกรณีที่มีความจำเป็นต้องใช้ให้ทำการสับเปลี่ยนข้อมูลเพื่อไม่ให้สามารถย้อนกลับไปยังข้อมูลต้นฉบับได้

(2) เมื่อมีความจำเป็นต้องคัดลอกข้อมูลที่ใช้ในการปฏิบัติงานจริงเพื่อทำการทดสอบ กำหนดให้มีบันทึกเพื่อระบุวัตถุประสงค์ และผู้ดำเนินการคัดลอกอย่างเป็นลายลักษณ์อักษร

(3) เมื่อใช้ข้อมูลทดสอบเสร็จสิ้นแล้วให้ลบข้อมูลออกจากระบบทดสอบทันที

11.4.3 การควบคุมการเข้าถึงซอร์สโค้ด

กลุ่มเทคโนโลยีสารสนเทศกำหนดให้ควบคุมการเข้าถึงซอร์สโค้ดตามแนวปฏิบัติ ดังนี้

(1) อนุญาตให้มีการเข้าถึงซอร์สโค้ดเฉพาะผู้มีสิทธิเท่านั้น โดยจัดทำบัญชีรายชื่อผู้ที่มีสิทธิการเข้าถึงอย่างเป็นลายลักษณ์อักษร

(2) มีการควบคุมเวอร์ชันของซอร์สโค้ด

(3) มีการเปิดบันทึกเหตุการณ์การเข้าถึงซอร์สโค้ด

11.5 ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in development and support processes)

กำหนดให้มีการควบคุมสภาพแวดล้อมของการพัฒนาและสนับสนุน โดยมีกระบวนการควบคุมการเปลี่ยนแปลงเพื่อป้องกันการละเมิดระบบและ/หรือสภาพแวดล้อมดังนี้

11.5.1 แนวทางการพัฒนาระบบให้มีความมั่นคงปลอดภัย

(1) นักพัฒนาระบบจำเป็นต้องศึกษาวงจรการพัฒนาระบบ และ เทคนิคในการเขียนระบบให้มีความปลอดภัยให้ดี

(2) บริษัทต้องนำหลักการของวงจรการพัฒนาระบบมาใช้ เพื่อทำให้มั่นใจได้ถึงคุณภาพของซอฟต์แวร์ในการพัฒนาระบบ

(3) การบริหารโครงการด้านเทคโนโลยีสารสนเทศ ต้องคำนึงถึงข้อกำหนดด้านความมั่นคงปลอดภัยในการพิจารณาและดำเนินกิจกรรมในโครงการในแต่ละช่วงของการบริหารโครงการเสมอ

11.5.2 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ

(1) การเปลี่ยนแปลงระบบ จะต้องถูกควบคุมโดยกระบวนการควบคุมการเปลี่ยนแปลงและมีการอนุมัติอย่างเป็นทางการ เพื่อลดปัญหาที่กระทบกับระบบโดยรวม

(2) คำร้องขอการเปลี่ยนแปลงระบบหรือซอฟต์แวร์ทุกคำร้องต้องได้รับการอนุมัติจากเจ้าของระบบ หรือบุคคลที่ได้รับการแต่งตั้งก่อนเริ่มทำการเปลี่ยนแปลง

(3) มีการควบคุมเวอร์ชันของซอฟต์แวร์ที่ดำเนินการ

(4) การเปลี่ยนแปลงระบบปฏิบัติการต้องเข้าสู่กระบวนการบริหารการเปลี่ยนแปลง

(5) จัดทำ/ปรับปรุงเอกสาร คู่มือ เพื่อให้สอดคล้องกับซอฟต์แวร์ที่มีการเปลี่ยนแปลงแก้ไข

11.5.3 การทบทวนโปรแกรมทางด้านเทคนิคหลังจากมีการเปลี่ยนแปลงระบบปฏิบัติการ

เมื่อมีการเปลี่ยนแปลง แก้ไข หรือมีการปรับปรุงประสิทธิภาพของระบบปฏิบัติการ ควรแจ้งให้ผู้ที่เกี่ยวข้องทราบล่วงหน้า เพื่อให้มีเวลาพอสำหรับทบทวนและทดสอบระบบโปรแกรมก่อนใช้งานจริง และให้มั่นใจว่าไม่มีผลกระทบร้ายแรงต่อการทำงานของผู้ใช้งานหรือส่งผลกระทบต่อความมั่นคงปลอดภัย

11.5.4 การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป

(1) ห้ามทำการเปลี่ยนแปลงใดๆ บนซอฟต์แวร์สำเร็จรูป หากมีความจำเป็นต้องมีการดำเนินการให้อยู่ภายใต้การควบคุมตามกระบวนการบริหารการเปลี่ยนแปลง (Change Management Procedure) อย่างเข้มงวด

(2) จะต้องได้รับคำยินยอมจากผู้ขายก่อนทำการเปลี่ยนแปลงใดๆ เพื่อให้มั่นใจว่าไม่มีการละเมิดทรัพย์สินทางปัญญา

(3) ต้องไม่ทำการแก้ไขโปรแกรมสำเร็จรูปจากผู้ขายถ้าไม่จำเป็น

11.5.5 แนวทางการพัฒนาระบบโดยหน่วยงานภายนอก

(1) ซอฟต์แวร์ที่พัฒนาโดยหน่วยงานภายนอกต้องเป็นไปตามรายละเอียดข้อกำหนดผู้ใช้ และมีการสนับสนุนด้านสินค้าอย่างเหมาะสม

(2) ต้องมั่นใจว่ามีการปรึกษาและทำการตกลงร่วมกันระหว่างบริษัทและหน่วยงานภายนอกในเรื่องการสนับสนุนจากหน่วยงานภายนอก และการปฏิบัติตามกฎหมายอย่างต่อเนื่อง การจัดการใบอนุญาตกรรมสิทธิ์ของโปรแกรม และทรัพย์สินทางปัญญา

(3) การทดสอบด้านความมั่นคงปลอดภัยของระบบ ต้องมีการดำเนินการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบในระหว่างที่ระบบอยู่ในช่วงการพัฒนา

11.5.6 การตรวจรับระบบ

(1) จะต้องมีเกณฑ์ในการตรวจรับระบบทุกระบบที่มีการพัฒนาขึ้นมาใหม่หรือมีการปรับปรุงประสิทธิภาพเพิ่มเติม โดยเกณฑ์ที่ใช้ในการตรวจรับจะต้องเป็นเกณฑ์ที่กำหนดอย่างชัดเจน ผ่านการอนุมัติ มีการจัดทำเป็นเอกสาร และผ่านการทดสอบการใช้งานมาแล้ว

(2) การทดสอบเพื่อตรวจรับระบบจะต้องไม่ทำโดยทีมที่เป็นผู้พัฒนาระบบนั้นเอง

11.6 **ข้อมูลสำหรับการทดสอบ** (Test data)

11.6.1 **การป้องกันข้อมูลสำหรับการทดสอบ**

(1) ต้องได้รับการอนุญาตก่อนนำสำเนาข้อมูลปฏิบัติการไปใช้ในการทดสอบระบบทุกครั้ง

(2) ต้องมีการเปลี่ยนแปลงข้อมูลบางส่วนสำหรับข้อมูลที่นำไปทดสอบ ไม่ให้เหมือนข้อมูลต้นทาง เพื่อป้องกันข้อมูลรั่วไหลและถูกนำไปใช้โดยไม่ได้รับอนุญาต

(3) ต้องดำเนินการให้สิทธิขั้นต่ำ (Least privilege) หมายถึง จำกัดผู้ใช้ที่ทำงาน ข้อมูลและระบบข้อมูลเฉพาะที่จำเป็นในการทำงานเท่านั้น

12. **ความสัมพันธ์กับผู้ให้บริการภายนอก** (Supplier relationships)

12.1 **ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก** (Information security in supplier relationship)

12.1.1 **ความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก**

บริษัทต้องคำนึงถึงและนำมาตรการด้านความมั่นคงปลอดภัยมากำกับหรือควบคุมในการให้บริการของผู้ให้บริการภายนอก ดังนี้

(1) ในระยะการวางแผน บริษัทควรระบุความต้องการจัดจ้างคนภายนอก, ความเสี่ยงที่จะเกิดขึ้นในการจ้างคนภายนอก และปัจจัยที่สามารถเป็นไปได้ในการลดการจัดจ้างคนภายนอก รายละเอียดเหล่านี้จะต้องทำเป็นลายลักษณ์อักษรในส่วนของการบริหารจัดการโครงการ

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

(3) การนำไปปฏิบัติ บริษัทต้องพัฒนาการรักษาความมั่นคงปลอดภัยสารสนเทศ และตารางสมรรถนะโดยอ้างอิงตามสัญญาและเงื่อนไขที่กำหนดไว้ ตารางนั้นจะต้องมีการเฝ้าระวังและทบทวนเป็นประจำ

(4) การแก้ไข/เปลี่ยนแปลง บริษัทอาจพิจารณาให้มีการเพิ่มเติมข้อกำหนดหรือวิธีการปกป้องใดๆ ในเอกสารสัญญาการบริการ เพื่อรักษาด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งนี้ขึ้นอยู่กับลักษณะงานที่ทำการว่าจ้างและผลการประเมินความเสี่ยง

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

(6) เมื่อสิ้นสุดการให้บริการ บริษัทต้องเตรียมให้ผู้ให้บริการส่งหน้าที่ความรับผิดชอบกลับมายังบริษัทหรือผู้ให้บริการรายใหม่ บริษัทต้องมั่นใจได้ว่าข้อมูลของบริษัททั้งหมดต้องได้กลับคืนจากผู้ให้บริการรายเดิม รายละเอียดเหล่านี้จะต้องทำเป็นลายลักษณ์อักษรในส่วนของการบริหารจัดการโครงการ

(7) เมื่อผู้ให้บริการหรือหน่วยงานภายนอกส่งมอบงานเสร็จสิ้น ข้อมูลการพัฒนาระบบ โปรแกรม และคู่มือต่างๆ ถือเป็นลิขสิทธิ์หรือทรัพย์สินของบริษัท ห้ามเปิดเผยหรือนำไปใช้โดยไม่ได้อนุญาต

12.1.2 การระบุปัญหาด้านความปลอดภัยในข้อตกลงกับหน่วยงานภายนอก

ข้อตกลงกับหน่วยงานภายนอกจะต้องระบุถึงการให้ความสำคัญกับความปลอดภัยที่เกี่ยวข้อง ดังต่อไปนี้

(1) การจัดหมวดหมู่ข้อมูลและการจัดการกับข้อมูล

(2) ระดับเป้าหมายของการให้บริการที่ยอมรับได้

(3) ความรับผิดของทั้งสองฝ่าย

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

(5) การจัดหาการควบคุมการเข้าใช้งานทั้งแบบเข้าถึงตัวเครื่องและแบบผ่านทางระบบเครือข่าย

(6) สิทธิในการตรวจสอบความรับผิดชอบตามสัญญาหรือการตรวจสอบที่ดำเนินการโดยบุคคลที่สาม

(7) การเกี่ยวข้องของหน่วยงานภายนอกโดยกับผู้รับจ้างช่วงอื่น

(8) ข้อกำหนดในการเก็บรักษาไว้ซึ่งรายชื่อของผู้ที่ได้รับอนุญาตใช้บริการ และสิทธิอื่นๆ

(9) สิทธิในการเฝ้าระวังและยกเลิกกิจกรรมของผู้ใช้งาน

(10) ข้อกำหนดในการทำสำเนา และเปิดเผยข้อมูลบริษัท

(11) การคืน หรือการทำลายข้อมูลต่างๆเมื่อสัญญาเสร็จสิ้น

(12) ข้อกำหนดในการป้องกันซอฟต์แวร์ประสงค์ร้าย

12.2 การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก

12.2.1 การติดตามและทบทวนบริการของผู้ให้บริการภายนอก

(1) การส่งมอบบริการโดยบุคคลที่สามจากภายนอกควรจะมีการตกลงทำสัญญารักษาความปลอดภัย คำนิยามของบริการ และระดับของการส่งมอบบริการรวมอยู่ในสัญญาส่งมอบบริการจากหน่วยงานภายนอก

(2) ควรจัดให้มีการตรวจสอบติดตามและประเมินผลการบริการจากหน่วยงานภายนอกเป็นประจำเพื่อให้มั่นใจว่าได้มีการปฏิบัติตามข้อตกลงในการรักษาความมั่นคงปลอดภัยของข้อมูล และเพื่อให้ได้มีการจัดการกับปัญหาทางด้านความปลอดภัยอย่างเหมาะสม

(3) สร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยด้านไซเบอร์เท่าที่จำเป็นต่อผู้ปฏิบัติงานที่เกี่ยวข้อง

(4) สื่อสารกระบวนการและขั้นตอนในการจัดการเหตุการณ์ละเมิดความปลอดภัยหรือเหตุการณ์ฉุกเฉิน

(5) ติดตาม/เฝ้าระวังผู้ให้บริการภายนอกให้ปฏิบัติตามแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยทางไซเบอร์

12.2.2 การบริหารการเปลี่ยนแปลงในบริการจากผู้ให้บริการภายนอก

(1) บริษัทจะปรับปรุงเงื่อนไขในสัญญาการให้บริการเมื่อมีการเปลี่ยนแปลงข้อกำหนดในการให้บริการ ซึ่งรวมถึงการดูแลและปรับปรุงแนวปฏิบัติ ขั้นตอนปฏิบัติ และการควบคุมด้านความมั่นคงปลอดภัยของข้อมูลที่มีอยู่เดิม

(2) ระหว่างทำการเปลี่ยนแปลงการให้บริการ ต้องมีการบริหารความเสี่ยงที่อาจเกิดขึ้นจากการเปลี่ยนแปลงการให้บริการ

13. การบริหารจัดการเหตุละเมิดด้านความมั่นคงปลอดภัยสารสนเทศ (Information security management)

13.1 การบริหารจัดการเหตุละเมิดด้านความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security and improvements)

13.1.1 หน้าที่รับผิดชอบและแนวทางตอบสนอง

(1) ต้องมีการกำหนดขั้นตอนการจัดการเหตุการณ์และจุดอ่อนด้านความปลอดภัยข้อมูล เพื่อจัดการเหตุการณ์ในหลายๆ ลักษณะที่เกิดขึ้น เช่น

- ระบบข้อมูลขัดข้อง และใช้บริการไม่ได้
- โปรแกรมประสงค์ร้ายต่อระบบ
- การถูกโจมตีที่ทำให้เครื่องเป้าหมายไม่สามารถให้บริการได้
- ความผิดพลาดอันเป็นผลจากข้อมูลทางธุรกิจที่ไม่สมบูรณ์หรือไม่ถูกต้อง
- การล่วงละเมิดความลับและความครบถ้วนสมบูรณ์ของข้อมูล
- การใช้ระบบข้อมูลโดยมิชอบ

(2) การตอบสนองต่อเหตุละเมิดด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยทางไซเบอร์ โดยทีมตอบสนองต่อเหตุละเมิดด้านความมั่นคงปลอดภัย (Security Incident Response Team) ควรดำเนินการดังนี้

- รวบรวมและวิเคราะห์ข้อมูลเพื่อตรวจหาเหตุการณ์ละเมิดความปลอดภัย
- จัดแบ่งประเภทและลำดับเหตุการณ์เพื่อพิจารณาว่าเหตุการณ์นั้นควรส่งต่อทีมอื่นในการดำเนินการหรือไม่
- วิเคราะห์ข้อมูลที่เกี่ยวข้องกับเหตุการณ์ กำหนดกลยุทธ์การตอบสนองและแก้ไข ประสานงานหรือสื่อสารข้อมูลที่เหมาะสมไปยังบุคคลที่เกี่ยวข้อง

- ประเมินผลมาตรการแก้ไขและประเมินความเสี่ยง เพื่อทบทวนมาตรการและปรับปรุงการบริหารจัดการเหตุการณ์ต่างๆ ให้มีประสิทธิภาพมากขึ้น เพื่อป้องกันการเกิดเหตุการณ์ละเมิดความปลอดภัยในอนาคต

(3) ผู้ใช้งานจะต้องรายงานเหตุการณ์และ/หรือจุดอ่อนด้านความมั่นคงปลอดภัยไปยังเจ้าหน้าที่ที่เกี่ยวข้องในการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยทันที ตามแนวปฏิบัติในการรายงานเหตุละเมิดด้านความมั่นคงปลอดภัย

(4) ห้ามผู้ใช้งานตอบคำถามที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยและความผิดพลาดของระบบกับสื่อใดๆ เองโดยเด็ดขาด การสื่อสารข้อมูลกับหน่วยงานภายนอกทั้งหมดเป็นหน้าที่ของคณะทำงานที่ได้รับมอบหมายในการสื่อสารเท่านั้น

13.1.2 การรายงานเหตุการณ์ทางด้านความมั่นคงปลอดภัยของข้อมูล

ต้องกำหนดช่องทางที่ใช้รายงานเหตุการณ์ทางด้านความปลอดภัย และแจ้งให้ผู้ใช้งานทุกคนทราบ ทุกเหตุการณ์ทางด้านความปลอดภัยต้องรายงานขึ้นไปตามกระบวนการรายงานเหตุการณ์และจุดอ่อนทางด้านความปลอดภัยสารสนเทศและความปลอดภัยทางไซเบอร์

13.1.3 การรายงานจุดอ่อนทางด้านความมั่นคงปลอดภัยสารสนเทศ

ต้องกำหนดช่องทางที่ใช้รายงานจุดอ่อนทางด้านความปลอดภัย และแจ้งให้ผู้ใช้งาน ทุกคนทราบจุดอ่อนทางด้านความปลอดภัยต้องรายงานขึ้นไปตามกระบวนการรายงานเหตุการณ์และจุดอ่อนทางด้านความปลอดภัย โดยผู้ใช้งานต้องไม่พยายามแก้ไขจุดอ่อนที่ต้องสงสัยออกเพื่อประโยชน์ในการตรวจสอบจากผู้ดูแลหรือผู้เชี่ยวชาญเว้นแต่จะได้รับอนุญาต

13.1.4 การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

ควรมีการทบทวนเหตุการณ์และจุดอ่อนทางด้านความปลอดภัยสารสนเทศและความปลอดภัยทางไซเบอร์ โดยพิจารณา ทบทวนมาตรการแก้ไขและประเมินความเสี่ยง เพื่อทบทวนมาตรการการป้องกันให้เหมาะสม รวมถึงการปรับปรุงการบริหารจัดการเหตุการณ์ต่างๆ ให้มีประสิทธิภาพมากขึ้น เพื่อป้องกันการเกิดเหตุการณ์ละเมิดความปลอดภัยในอนาคต

13.1.5 การเก็บรวบรวมหลักฐาน

ต้องมีการเก็บรักษาหลักฐานสนับสนุนอื่นๆ อาทิ อีเมล ผู้ดูแล การเข้าถึง ข้อยกเว้น ไฟร์วอลล์ และระบบตรวจจับการบุกรุก และที่เกี่ยวข้องอื่นๆ โดยวิธีการเก็บรวบรวมหลักฐานควรจะสอดคล้องกับแนวปฏิบัติการจัดเก็บและจัดการสารสนเทศที่ใช้เป็นหลักฐาน

14. มุมมองด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารความต่อเนื่องของธุรกิจ (Information security aspects of business continuity management)

14.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity)

14.1.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

การวางแผนความต่อเนื่องทางธุรกิจ เพื่อพัฒนาและรักษาความต่อเนื่องของธุรกิจทั่วทั้งบริษัท ประกอบด้วย เทคโนโลยีสารสนเทศ การบริหารจัดการ และด้านอื่นๆ ของฝ่ายต่างๆ

(1) การประเมินต้องคำนึงถึงกระบวนการทางธุรกิจทั้งหมด และไม่จำกัดอยู่เพียงระบบประมวลผลเท่านั้น

(2) ควรทำการวิเคราะห์ผลกระทบทางธุรกิจเพื่อระบุเหตุการณ์ที่สามารถทำให้กระบวนการทางธุรกิจหยุดชะงักลงได้

14.1.2 การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

(1) ต้องมีการปฏิบัติตามแผนความต่อเนื่องทางธุรกิจ หากเกิดเหตุภัยพิบัติ การให้บริการทางธุรกิจที่สำคัญของบริษัทจะสามารถดำเนินการได้ภายใต้กรอบเวลาที่กำหนดไว้

(2) ข้อพิจารณาของข้อกำหนดทางความมั่นคงปลอดภัยสารสนเทศ

(3) สภาพแวดล้อมทางกายภาพของระบบคอมพิวเตอร์สำรองฉุกเฉินจะต้องปฏิบัติตามความมั่นคงปลอดภัยขั้นต่ำ คือ การกำหนดความรับผิดชอบในการเข้าถึงระบบคอมพิวเตอร์สำรองฉุกเฉิน

(4) การเตรียมระบบคอมพิวเตอร์สำรองฉุกเฉินต้องมีสถาปัตยกรรมเครือข่ายเช่นเดียวกับสภาพแวดล้อมปกติ โดยที่ความสามารถในการทำงานซ้ำซ้อนอาจลดลงได้

(5) การเตรียมระบบสารสนเทศต้องมีความปลอดภัยตามแนวทางการดำเนินการของบริษัท

(6) ต้องมีการจัดการข้อมูลตลอดเวลาโดยผู้ควบคุมที่ถูกกำหนดไว้และผู้ใช้

(7) ต้องมีการจัดการสื่อบันทึกโดยผู้ได้รับอนุญาต และทำการจัดเก็บในตู้ที่ถูกล็อกอย่างดี

(8) ในกรณีที่มีการให้บริการจากหน่วยงานภายนอก ต้องมีเอกสารรายชื่อบุคคลผู้มีอำนาจเพื่อที่จะสามารถเริ่มและยุติการให้บริการ

14.1.3 การพัฒนาและจัดทำแผนการบริหารความต่อเนื่องของธุรกิจรวมทั้งความมั่นคงปลอดภัยของข้อมูล

แผนการบริหารความต่อเนื่องของธุรกิจควรประกอบด้วยสิ่งต่อไปนี้

(1) การระบุกระบวนการทางธุรกิจที่มีความสำคัญ และการใช้งานร่วมกันหรือความต่อเนื่องกันของกระบวนการเหล่านี้

(2) ลำดับความสำคัญของกระบวนการต่างๆ ที่ต้องกู้กลับมา

(3) การระบุความรับผิดชอบทั้งหมดและการเตรียมการสำหรับกรณีฉุกเฉิน

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

(5) เอกสารเกี่ยวกับขั้นตอนต่างๆ ที่ได้ตกลงกันแล้ว

(6) แผนการบริหารความต่อเนื่องของธุรกิจต้องครอบคลุมถึงความต่อเนื่องของกระบวนการทางธุรกิจและบริการที่มีความสำคัญ ข้อกำหนดการดำเนินงาน และการกู้บริการด้านคอมพิวเตอร์คืนจากภัยพิบัติ

(7) พนักงานควรได้รับการฝึกอบรมเกี่ยวกับขั้นตอนการกู้ระบบคืนตามที่ตกลงกัน และจะต้องทำการทดสอบเป็นประจำเพื่อให้มั่นใจว่าพนักงานรู้ว่าต้องตอบสนองอย่างไรเพื่อคงความต่อเนื่องของธุรกิจต่อไป

14.1.4 **การทดสอบ การบำรุงรักษา และการประเมินแผนการบริหารความต่อเนื่องของธุรกิจ**

(1) ควรจะมีการทดสอบด้านความต่อเนื่องของธุรกิจอย่างน้อยปีละหนึ่งครั้ง

(2) จะต้องกำหนดวิธีทดสอบก่อนการทดสอบจริง

(3) จะต้องติดตามข้อบกพร่องที่ระบุได้ในระหว่างการทดสอบความต่อเนื่องของธุรกิจ

14.1.5 **การเตรียมการอุปกรณ์ประมวลผลสำรอง** (Redundancies)

(1) สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ

การเตรียมความพร้อมในการสำรองอุปกรณ์ ควรพิจารณาถึงเงื่อนไขดังนี้

- ระบบต้องปฏิบัติตามกฎหมาย ข้อบังคับ และข้อผูกพันตามสัญญากับลูกค้า
- ระบบมีระดับการวิเคราะห์ผลกระทบทางธุรกิจสูง
- ระบบที่พึ่งพาระบบอื่นที่มีระดับการวิเคราะห์ผลกระทบทางธุรกิจสูง

(2) ตามข้อจำกัดทางภูมิศาสตร์ ความต้องการทางธุรกิจ และช่องโหว่ทางธุรกิจมีที่อยู่ การทำงานชุดสำรองควรพิจารณาถึงสิ่งเหล่านี้

- ความพร้อมในการบริหารจัดการพลังงาน
- ความพร้อมในการเชื่อมโยงเครือข่ายสู่สภาพแวดล้อมภายนอก
- ความพร้อมในการเชื่อมโยงเครือข่ายภายใน
- ความพร้อมในการเปิดระบบ
- ความพร้อมในการเก็บรักษาอุปกรณ์

15. **ความสอดคล้อง** (Compliance)

15.1 **ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง** (Compliance with legal and contractual requirements)

15.1.1 **การระบุกฎหมายและความต้องการในสัญญาจ้างที่เกี่ยวข้อง**

(1) เจ้าของระบบต้องมั่นใจว่าระบบของตนเป็นไปตามข้อกำหนดของกฎหมายหรือ ระเบียบ ข้อบังคับของหน่วยงานที่กำกับดูแลในประเทศนั้นๆ

(2) เจ้าของระบบต้องระบุความต้องการทั้งหมดที่เกี่ยวข้องกับข้อกำหนดกฎหมาย ระเบียบข้อบังคับ สัญญาจ้าง เป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ

(3) เจ้าของระบบแต่ละรายต้องปฏิบัติตามข้อกำหนดในสัญญาที่ทำกับลูกค้า และข้อตกลงเกี่ยวกับระดับการให้บริการที่ให้แก่ลูกค้า

15.1.2 **สิทธิในทรัพย์สินทางปัญญา**

ต้องมีการควบคุมและมีขั้นตอนปฏิบัติที่เหมาะสม สอดคล้องกับกฎหมาย ระเบียบข้อบังคับ ในการใช้งานผลิตภัณฑ์ซอฟต์แวร์ที่มีกรรมสิทธิ์ที่ถูกต้อง

15.1.3 **การป้องกันบันทึกต่าง ๆ**

บันทึกต่างๆ ที่มีความสำคัญของบริษัทต้องได้รับการป้องกันจากการสูญหาย การทำลาย และการปลอมแปลง

15.1.4 **ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล**

ข้อมูลที่เป็นข้อมูลส่วนบุคคลที่บริษัทเก็บหรือดูแลไว้ ต้องมีการดำเนินการให้สอดคล้องกับกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

16. การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information security reviews)

16.1 การทบทวนด้านความมั่นคงปลอดภัยของข้อมูลโดยอิสระ

(1) จะต้องมีการตรวจสอบความมั่นคงปลอดภัยของข้อมูลอย่างน้อยปีละครั้งเพื่อหาจุดที่ไม่เป็นไปตามมาตรฐาน

(2) ผู้ตรวจสอบที่ได้รับมอบหมายให้ทำการตรวจสอบความมั่นคงปลอดภัยของข้อมูลจะต้องไม่เป็นผู้ตรวจสอบงานของตนเอง

16.2 การปฏิบัติให้เป็นไปตามแนวปฏิบัติและมาตรฐานด้านความปลอดภัย

(1) ผู้บังคับบัญชาต้องมีความรับผิดชอบในการดูแล และกำกับการทำงานของพนักงานในทีมเพื่อให้เป็นไปตามแนวปฏิบัติ ขั้นตอน และมาตรฐานด้านความปลอดภัยที่เกี่ยวข้อง ในกรณีที่เจอเหตุละเมิดด้านความมั่นคงปลอดภัยจากการปฏิบัติงานของทีมงาน ให้ดำเนินการร้องขอ ให้ทำการสอบสวน เพื่อให้เข้าสู่ขั้นตอนของกระบวนการแก้ไขปัญหา

(2) ผู้บังคับบัญชาต้องมีหน้าที่รับผิดชอบในการปฏิบัติตามแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศ

16.3 การตรวจสอบความสอดคล้องทางเทคนิค

ต้องมีการประเมินเครือข่ายและมาตรการความมั่นคงปลอดภัยของระบบสารสนเทศอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง โดยบุคลากรทางเทคนิคและด้านความปลอดภัยที่เหมาะสม เพื่อตรวจสอบการควบคุมด้านความปลอดภัยต่างๆ ให้เพียงพอต่อปัจจัยเสี่ยงในปัจจุบัน

17. บทลงโทษทางวินัย

บทลงโทษทางวินัยนั้นจะอิงตามบทลงโทษของพนักงานที่ฝ่าย HR กำหนดไว้ ซึ่งจะมีคณะกรรมการพิจารณาระดับโทษ โดยมีรายละเอียดดังนี้

(1) ตักเตือนด้วยวาจา

(2) ตักเตือนเป็นลายลักษณ์อักษร

(3) พักงานสถานเบา 1-7 วัน โดยไม่จ่ายค่าจ้าง

(4) พักงานสถานหนัก 8-15 วัน โดยไม่จ่ายค่าจ้าง

(5) เลิกจ้าง โดยไม่จ่ายค่าชดเชยใดๆ ทั้งสิ้น