นโยบายการจัดการเทคโนโลยีสารสนเทศและความปลอดภัยด้านไซเบอร์ 2025
(Information Technology Management and Cyber Security Policy)

บริษัท ฐิติกร จำกัด (มหาชน) และบริษัทย่อย
(พ.ศ. 2568)

สารบัญ

เรื่อง	หน้า
หลักปฏิบัติในระดับคณะกรรมการ	3
หลักปฏิบัติในระดับบริหารงาน	3
หลักปฏิบัติในระดับการดำเนินงาน	4
นโยบายและแนวทางปฏิบัติ	5
วัตถุประสงค์	5
ขอบเขต	6
ความหมายและการกำจัดความ	6
นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท	7
การทบทวนนโยบาย	7
การปฏิบัติตามนโยบาย	7
1. ความปลอดภัยที่เกี่ยวข้องกับบุคลากร	8
2. การบริหารจัดการทรัพย์สินด้านสารสนเทศ	9
3. การจัดระดับชั้นความลับของข้อมูล	10
4. การควบคุมการเข้าถึง	13
5. การบริหารจัดการการเข้ารหัสข้อมูล	14
6. การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม	15
7. การรักษาความปลอดภัยในการปฏิบัติงาน	16
8. การรักษาความปลอดภัยของระบบสื่อสาร	19
9. การจัดหา การพัฒนาและการดูแลระบบ	20
10. การบริหารจัดการผู้ให้บริการภายนอก	21
11. การจัดการเหตุการณ์ผิดปกติด้านความปลอดภัย	22
12. การบริหารจัดการด้านการดำเนินธุรกิจอย่างต่อเนื่อง	22
13. ความปลอดภัยในการใช้สื่อสังคมออนไลน์	23
14. ความปลอดภัยในการใช้บริการ	25

15. การใช้ e-mail 25

16. การปฏิบัติตามข้อกำหนด 26

17. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ 27

18. การจ้างงานภายนอกบริการเทคโนโลยี 27

นโยบายการจัดการเทคโนโลยีสารสนเทศและความปลอดภัยด้านไซเบอร์ 2025
Information Technology Management and Cyber Security Policy

บริษัทมีนโยบายการปฏิบัติตามหลักการกำกับดูแลกิจการที่ดี โดยเผยแพร่ข้อมูลและข่าวสารด้านจัดการเทคโนโลยีสารสนเทศและความปลอดภัยด้านไซเบอร์ (Cyber Security) เพื่อให้มีการควบคุมในการดำเนินงานของบริษัท ซึ่งรวมถึงการกำหนดระเบียบปฏิบัติเกี่ยวกับจริยธรรมทางธุรกิจและจรรยาบรรณให้สอดคล้องกับข้อพึงปฏิบัติที่ดี ซึ่งมีสาระสำคัญของการกำกับดูแลกิจการด้านความปลอดภัยด้านไซเบอร์ (Cyber Security) ดังนี้

1. หลักปฏิบัติในระดับคณะกรรมการ

คณะกรรมการจัดให้มีกรอบการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร ที่สอดคล้องกับความต้องการของบริษัทด้านการบริหารความเสี่ยงและด้านความปลอดภัยด้านไซเบอร์ (Cyber Security) เพื่อให้บริษัทสามารถบรรลุวัตถุประสงค์และเป้าหมายหลักของบริษัท

1.1 คณะกรรมการจะดูแลให้การบริหารความเสี่ยงขององค์กรครอบคลุมถึงการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและความปลอดภัยด้านไซเบอร์ (Cyber Security)

1.2 คณะกรรมการจะจัดให้มีนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งนี้ กรอบการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศและความปลอดภัยด้านไซเบอร์ (Cyber Security) ระดับองค์กร ได้แก่

(1) บริษัทได้ทำตามกฎหมาย ระเบียบ ข้อบังคับและมาตรฐานต่าง ๆ ที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศและด้านความปลอดภัยด้านไซเบอร์

(2) บริษัทมีระบบการรักษาความปลอดภัยของข้อมูล ในการรักษาความลับ (Confidentiality) การรักษาความน่าเชื่อถือ (Integrity) และความพร้อมใช้ของข้อมูล (Availability) รวมทั้งป้องกันมิให้มีการนำข้อมูลไปใช้ในทางมิชอบ หรือมีการแก้ไขเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

(3) บริษัทได้พิจารณาความเสี่ยงด้านเทคโนโลยีสารสนเทศ และมีมาตรการในการบริหารจัดการความเสี่ยงดังกล่าวในด้านต่าง ๆ เช่น การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management) การบริหารจัดการเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Incident Management) การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management) เป็นต้น

2. หลักปฏิบัติในระดับบริหารงาน

ผู้บริหารจัดให้มีแผนการดำเนินงานจัดการเทคโนโลยีสารสนเทศระดับองค์กร ที่สอดคล้องกับความต้องการของบริษัทด้านการบริหารความเสี่ยงและด้านความปลอดภัยด้านไซเบอร์ (Cyber Security) เพื่อให้บริษัทสามารถบรรลุวัตถุประสงค์และเป้าหมายหลักของบริษัท

2.1 ผู้บริหารมีการกำหนดหลักเกณฑ์และระเบียบปฏิบัติ ดูแลให้การบริหารครอบคลุมถึงการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและความปลอดภัยด้านไซเบอร์ (Cyber Security)

2.2 ผู้บริหารมีการกำหนดแผนการดำเนินงานและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และความปลอดภัยด้านไซเบอร์ (Cyber Security) ระดับองค์กร ได้แก่

(1) มีการกำหนด บทบาท หน้าที่ และความรับผิดชอบ คณะกรรมการบริหารความเสี่ยงระบบสารสนเทศ และความปลอดภัยด้านไซเบอร์ (Cyber Security)

(2) จัดทำแผนปฏิบัติการด้านการบริหารความเสี่ยงระบบสารสนเทศระบบสารสนเทศและความปลอดภัยด้านไซเบอร์ (Cyber Security) โดยมีการทบทวนและมีการปรับปรุงจากข้อบกพร่องในอดีต รวมถึงโอกาสของภัยคุกคามทางไซเบอร์ในอนาคต

2.3 ผู้บริหารมีการติดตามการนำนโยบายมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และความปลอดภัยด้านไซเบอร์ (Cyber Security) ที่ได้รับการอนุมัติจากคณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมาย ไปปฏิบัติและมีการทบทวนนโยบายและแนวปฏิบัติปีละหนึ่งครั้งและการนำเสนอข้อเปลี่ยนแปลงอย่างมีนัยสำคัญให้คณะกรรมการฯ ทราบ

2.4 ผู้บริหารมีการจัดทำกระบวนการหรือขั้นตอนในการประเมินความเสี่ยงและจัดการความเสี่ยง การกำหนดดัชนีชี้วัดความเสี่ยงของระบบสารสนเทศและความปลอดภัยด้านไซเบอร์ (Cyber Security Risk indicator) รวมถึงจัดให้มีการติดตาม และรายงานผลดัชนีชี้วัดความเสี่ยงดังกล่าวต่อผู้ที่มีหน้าที่รับผิดชอบ เพื่อให้สามารถบริหารจัดการความเสี่ยงได้อย่างเหมาะสมและทันต่อเหตุการณ์ เช่น การรายงานความเสี่ยงของระบบสารสนเทศและความปลอดภัยด้านไซเบอร์ (Risk reporting) กำหนดระดับความเสี่ยงที่ยอมรับได้ (IT risk appetite) นำเสนอวิธีการหรือเครื่องมือในการบริหารและจัดการความเสี่ยงของระบบสารสนเทศและความปลอดภัยด้านไซเบอร์ ให้อยู่ในระดับที่ยอมรับได้ รวมถึงเกณฑ์การประเมินความเสี่ยงของระบบสารสนเทศและความปลอดภัยด้านไซเบอร์ โดยครอบคลุมระดับของผลกระทบ และระดับของโอกาสการเกิดเหตุการณ์ เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง

3. หลักปฏิบัติในระดับการดำเนินงาน

พนักงานระดับปฏิบัติงานได้ดำเนินการตามแผนด้านการบริหารความเสี่ยงและด้านความปลอดภัยด้านไซเบอร์ (Cyber Security) เพื่อให้บริษัทสามารถบรรลุวัตถุประสงค์และเป้าหมายหลักของบริษัท ดังนี้

3.1 พนักงานระดับปฏิบัติงานดำเนินตามหลักเกณฑ์และระเบียบปฏิบัติ และแผนการดำเนินงานการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและความปลอดภัยด้านไซเบอร์ (Cyber Security)

3.2 มีการจัดทำแนวปฏิบัติการจัดชั้นสารสนเทศ (Information classification) ที่เหมาะสมตามชั้นความลับ และความสำคัญของสารสนเทศขององค์กร โดยมีรายละเอียดครอบคลุม

(1) การรักษาความมั่นคงปลอดภัยของข้อมูล ทั้งในการรับส่งข้อมูลผ่านเครือข่ายสื่อสาร การจัดเก็บข้อมูลในระบบงานหรือสื่อบันทึกข้อมูลต่าง ๆ สอดคล้องตามการจัดชั้นข้อมูล

(2) ปฏิบัติการทำลายข้อมูลที่เหมาะสมกับชั้นความลับ

(3) มีแนวปฏิบัติควบคุมการเข้าถึงชั้นข้อมูลที่เหมาะสมตามชั้นความลับและความสำคัญของข้อมูลขององค์กร

3.3 พนักงานระดับปฏิบัติงานดำเนินการตามแนวทางในการกำกับดูแลและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และความปลอดภัยด้านไซเบอร์ (Cyber Security) ระดับองค์กร ได้แก่

(1) การควบคุมการเข้าถึงข้อมูลหรือระบบ (Access Control) โดยมีการกำหนดรอบระยะเวลาการทบทวนปรับปรุงสิทธิการใช้งาน

(2) การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT continuity) และซ้อมปฏิบัติเป็นประจำทุกปี

(3) การบริหารจัดการทรัพย์สินสารสนเทศ (IT asset management)

(4) การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)

(5) การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations security) เช่น การเข้าถึงระบบ การใช้งาน และการประมวลผล

(6) มีการจัดการข้อมูลและการบริหารจัดการกุญแจเข้ารหัส (Key Management) มาตรฐานการเข้ารหัสซึ่งเชื่อถือได้ตามมาตรฐานสากล

(7) มีการควบคุมการเข้าและออกระบบสารสนเทศ และมีการบันทึกและจัดเก็บประวัติข้อมูลการเข้าและออก

(8) มีกระบวนการหรือชั้นตอนการเข้าถึงระบบเครือข่าย และระบบสารสนเทศจากระยะไกล (remote access) โดยจะต้องได้รับการอนุมัติจากผู้มีอำนาจและมีหลักฐาน

(9) มีกระบวนการบริหารจัดการการเปลี่ยนแปลง (Change management) และควบคุมการเปลี่ยนแปลงอย่างรัดกุมและเพียงพอ ทั้งการนำระบบขึ้นใช้งานจริง (System Deployment) และการตั้งค่าระบบ (System Configuration)

(10) มีการบริหารจัดการขีดความสามารถของระบบ (capacity management) เพื่อให้มีการจัดสรรทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอและมีการวางแผนรองรับการใช้งานในอนาคต

(11) มีกระบวนการในการควบคุมการติดตั้งเพื่อปรับปรุงซอฟต์แวร์ (Patch) ให้เป็นรุ่นที่ยอมรับในความปลอดภัยด้านไซเบอร์ของระบบที่ใช้งานจริง

(12) มีมาตรฐานและระเบียบวิธีปฏิบัติในการติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม เพื่อให้มีการติดตาม ดูแลความปลอดภัยของระบบอย่างต่อเนื่อง โดยใช้ซอฟต์แวร์ป้องกัน Malware, Anti-Virus และ Anti-Ransomware ติดตั้งครบทั้งระบบโครงสร้างพื้นฐาน

(13) มีการจัดการช่องโหว่ระบบ ด้วยการจัดซื้อซอฟต์แวร์ค้นหาช่องโหว่และทำการสำรวจหาช่องโหว่ระบบ โดยดำเนินการปิดช่องโหว่ที่มีระดับความเสี่ยงสูงและปานกลาง

(14) มีการทดสอบเจาะระบบ (Penetration Test) เพื่อหาจุดอ่อนของระบบ และมีดำเนินการปรับปรุงแก้ไขจุดอ่อนต่างๆ โดยจะมีแผนดำเนินการในปีนี้

(15) กำหนดแนวทางในการตอบสนองและสื่อสาร เพื่อดำเนินการแก้ไขเหตุการณ์หรือสถานการณ์จากภัยคุกคามทางไซเบอร์ โดยมีขั้นตอนรายงานเป็นลำดับชั้นตามระดับความเสี่ยง นอกจากนี้ยังมีมาตรการในการฟื้นฟูความเสียหายจากภัยคุกคามไซเบอร์ พร้อมทั้งมีการซักซ้อมหรือทดสอบประจำทุกปี

นโยบายและแนวทางปฏิบัติ

วัตถุประสงค์

เพื่อกำหนดนโยบายและแนวทางในการใช้ระบบเทคโนโลยีสารสนเทศให้เป็นไปอย่างเหมาะสม สอดคล้องกับกฎหมายตลอดจนข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้อง และปกป้องพนักงาน และทรัพย์สินของบริษัทฯ ให้พ้นจากความเสี่ยงด้านความมั่นคงปลอดภัย หรือการใช้งานที่ไม่ถูกต้อง

รวมถึงรักษาไว้ซึ่งความสามารถในการดำเนินธุรกิจได้อย่างต่อเนื่อง โดยการทำงานแบ่งตามองค์ประกอบหลักของบริษัทฯ ได้เป็น 4 ส่วนคือ

1. ข้อมูล : ข้อมูลของบริษัทฯ คือทรัพย์สินที่มีความสำคัญมากที่สุด และต้องได้รับการปกป้องให้คงไว้ซึ่ง
    - ความลับ (Confidentiality)
    - ความถูกต้องครบถ้วน (Integrity)
    - ความพร้อมใช้งาน (Availability)
2. ระบบสารสนเทศ : การดำเนินธุรกิจของบริษัทฯจำเป็นต้องอาศัยคอมพิวเตอร์ ระบบเครือข่าย และข้อมูลอิเล็กทรอนิกส์ ดังนั้นจึงถือเป็นหน้าที่ของพนักงานและผู้ที่เกี่ยวข้องทุกคน ในการรักษาความมั่นคงปลอดภัยให้แก่ระบบเทคโนโลยีสารสนเทศของบริษัทฯ อย่างสุดความสามารถ
3. สำนักงาน : สำนักงานของบริษัทฯ คือพื้นที่ปฏิบัติงานของพนักงาน และผู้ที่เกี่ยวข้อง ซึ่งพื้นที่เหล่านี้อาจถูกล่วงละเมิดความมั่นคงปลอดภัยได้ หากไม่ได้รับการปกป้องคุ้มครองอย่างเหมาะสม

4. พนักงาน : พนักงานทุกคนต่างมีความรับผิดชอบต่อข้อมูลของบริษัทฯ ดังนั้น พนักงานจึงจำเป็นต้องทราบถึงวิธีการปกป้องข้อมูลให้พ้นจากการถูกล่วงละเมิด ทั้งในขณะปฏิบัติงานภายในและนอกสถานที่ทำงาน รวมไปถึงการทำงานที่บ้าน

ขอบเขต

นโยบายฉบับนี้ครอบคลุมการบริหารจัดการทางด้านการรักษาความปลอดภัยของระบบสารสนเทศของบริษัทฯ และครอบคลุมถึง

- ข้อมูลทั้งหมด (ทั้งที่อยู่ในรูปเอกสาร และอิเล็กทรอนิกส์) ที่ได้รับการจัดเก็บ ได้รับการใช้งาน หรือใช้ในการสื่อสารเพื่อดำเนินกิจการของบริษัทฯ
- บุคคลทั้งหมดที่มีส่วนเกี่ยวข้องในการใช้งานระบบสารสนเทศ ซึ่งได้แก่ ผู้บริหาร พนักงาน หุ้นส่วน ตัวแทนธุรกิจ บุคคลภายนอกที่ถูกว่าจ้างโดยบริษัทฯ บริษัทคู่ค้า บริษัทหรือบุคคลที่เป็นคู่สัญญา และ ผู้ให้บริการ
- ทรัพย์สินทั้งหมดที่เกี่ยวข้องกับข้อมูล และที่ใช้ในการจัดเก็บ ส่งผ่าน หรือประมวลผลข้อมูล ซึ่งได้แก่ อุปกรณ์ เครื่องเซิร์ฟเวอร์ เครื่องคอมพิวเตอร์ ซอฟต์แวร์ โปรแกรม เอกสารอิเล็กทรอนิกส์ เอกสารตีพิมพ์ เครื่องมือ สิ่งอำนวยความสะดวก ตลอดจนบริการที่ได้รับ

ความหมายและการกำจัดความ

“บริษัท” หมายถึง บริษัท ฐิติกร จำกัด (มหาชน) และบริษัทย่อย

“ผู้ใช้งาน” หมายถึง กรรมการ /พนักงาน หรือผู้ที่ได้รับอนุญาตให้ใช้ระบบคอมพิวเตอร์หรือระบบเครือข่ายของบริษัท

“คณะกรรมการฯ” หมายถึง พนักงานที่ได้รับแต่งตั้งให้เป็นคณะกรรมการดูแลระบบสารสนเทศ

“ทีมงานรักษาความปลอดภัยเทคโนโลยีสารสนเทศ” หมายถึง หน่วยงานที่ดูแลระบบสารสนเทศ

“หน่วยงาน” หมายถึง หน่วยงานต่างๆ ในองค์กร

“ผู้ดูแลระบบ” หมายถึง พนักงานที่ถูกแต่งตั้งให้ดูแลระบบสารสนเทศ

“เจ้าของข้อมูล” หมายถึง ผู้ได้รับมอบหมายจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดความเสียหาย

“ทรัพย์สินด้านสารสนเทศ” ได้แก่ ฐานข้อมูล ไฟล์ข้อมูล ซอฟต์แวร์ เครื่องมือในการพัฒนา อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์สื่อสาร สื่อบันทึกข้อมูลภายนอก และอุปกรณ์ต่อพ่วงทุกชนิด

“ระบบสารสนเทศ” หมายถึง ระบบที่มีการนำเอาฮาร์ดแวร์ ซอฟต์แวร์ บุคลากร แนวปฏิบัติ และข้อมูล ซึ่งทำงานประสาน กันเพื่อจัดเตรียมสารสนเทศที่จำเป็นให้กับบริษัท

“สารสนเทศ” หมายถึง ข้อมูลต่างๆ ที่ได้ผ่านการเปลี่ยนแปลงประมวลผลหรือวิเคราะห์สรุปผลด้วยวิธีการต่างๆ แล้วเก็บรวบรวมไว้ เพื่อนำมาใช้ประโยชน์ตามต้องการ การประมวลผล เป็นการนำข้อมูลจากแหล่งต่างๆ ที่เก็บรวบรวมไว้มาผ่านกระบวนการต่างๆ เพื่อแปรสภาพข้อมูลให้เป็นระบบที่อยู่ในรูปแบบที่ต้องการ

“บุคคลภายนอก” หมายถึง บุคคล นิติบุคคล ซึ่งบริษัทหรือหน่วยงานในบริษัทอนุญาตให้มีสิทธิ์ในการเข้าถึงข้อมูลหรือระบบสารสนเทศ โดยได้รับสิทธิ์ตามประเภทการใช้งาน และต้องรับผิดชอบในการไม่เปิดเผยความลับของบริษัทโดยไม่ได้รับอนุญาต

“ผู้รับการว่าจ้าง” หมายถึง บุคคล บริษัท หรือหน่วยงานภายนอก ซึ่งได้รับการว่าจ้างจากบริษัทให้ทำงานให้ในช่วงระยะเวลาหนึ่ง หรือทำงานในฐานะเป็นผู้ใช้งานของบริษัท ซึ่งรวมถึงลูกจ้างชั่วคราว โดยทั่วไปการว่าจ้างจะมีการทำสัญญาจ้างเพื่อควบคุมให้ผู้รับจ้างปฏิบัติตามเงื่อนไข หรือข้อตกลงการจ้างงานนั้น

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท

พนักงานทุกคนต้องปฏิบัติตามนโยบายการรักษาความปลอดภัยของระบบสารสนเทศในการปกป้องข้อมูลจากเหตุละเมิดต่างๆ ซึ่งอาจส่งผลกระทบต่อความลับของข้อมูล (Confidentiality) ความถูกต้องและสมบูรณ์ครบถ้วนของข้อมูล (Integrity) หรือความมีพร้อมใช้งานของข้อมูล (Availability) โดยบริษัทมีนโยบายดังนี้

- ข้อมูลที่สำคัญของบริษัทฯ จะต้องได้รับการปกป้องจากการเข้าถึงโดยไม่ได้รับอนุญาต
- ข้อมูลที่สำคัญของบริษัทฯ จะต้องได้รับการรักษาความลับอย่างเหมาะสม
- ข้อมูลที่สำคัญของบริษัทฯ จะต้องมีความถูกต้องและสมบูรณ์ครบถ้วน
- ข้อมูลที่สำคัญของบริษัทฯ จะต้องมีพร้อมใช้งานอยู่เสมอ
- กฎหมาย กฎระเบียบ และข้อบังคับที่เกี่ยวข้องต่างๆ จะต้องได้รับการปฏิบัติตามอย่างถูกต้องครบถ้วน
- พนักงานทุกคนจะต้องได้รับการฝึกอบรมด้านการรักษาความมั่นคงของข้อมูล
- จัดให้มีการบริหารจัดการความเสี่ยง (Risk management) ที่เกี่ยวข้องกับความมั่นคงของข้อมูลขึ้นในบริษัทฯ
- จัดทำแผนการจัดการเพื่อให้ธุรกิจดำเนินได้อย่างต่อเนื่อง พร้อมทั้งทำการดูแลรักษา และทดสอบแผนอย่างเหมาะสม
- จัดให้มีชุดเอกสารนโยบายด้านความมั่นคงของข้อมูล และเอกสารสนับสนุนที่เกี่ยวข้อง เพื่อกำหนดระเบียบปฏิบัติตลอดจนแนวทางการปฏิบัติงานและการใช้งานข้อมูลอย่างมั่นคงปลอดภัย
- จัดให้มีกระบวนการในการรายงาน สืบสวน รับมือ และจัดการกับเหตุละเมิดความมั่นคงอย่างเหมาะสม โดยเหตุละเมิดความมั่นคง ตลอดจนสิ่งผิดปกติ และเหตุการณ์ที่น่าสงสัยอื่นๆ จะต้องได้รับการรายงานไปที่ผู้จัดการด้านความมั่นคง หรือทีมงาน เพื่อดำเนินการตรวจสอบ และแก้ไข
- จัดให้มีการกำหนดสิทธิในการเข้าถึงข้อมูล การประมวลผล และเผยแพร่ข้อมูลอย่างรอบคอบและรัดกุม

การทบทวนนโยบาย

นโยบายการรักษาความปลอดภัยของระบบสารสนเทศจะต้องได้รับการทบทวนโดยคณะกรรมการฯ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญที่มีผลต่อนโยบายฉบับนี้ เพื่อให้มั่นใจได้ว่าเนื้อหาของนโยบาย ยังคงไว้ซึ่งความสมบูรณ์ มีประสิทธิภาพ และสามารถนำไปใช้งานได้อย่างเหมาะสม

การปฏิบัติตามนโยบาย

การละเมิด ฝ่าฝืน ละเลย หรือไม่ปฏิบัติตามนโยบาย วิธีการปฏิบัติงาน และเอกสารสนับสนุน ที่เกี่ยวข้อง ไม่ว่าโดยเจตนาหรือไม่ก็ตาม ถือเป็นความผิดทางวินัย ซึ่งต้องถูกพิจารณาลงโทษทางวินัยของทางบริษัท และหากการละเมิดหรือฝ่าฝืนนโยบายนั้นเข้าข่ายการกระทำที่ผิดกฎหมาย ผู้ละเมิดก็ต้องได้รับการดำเนินคดีตามที่กฎหมาย

กรณีที่มีระบบงานที่ไม่สามารถปฏิบัติตามนโยบายการรักษาความปลอดภัยของระบบสารสนเทศได้ให้เจ้าของระบบงานและหน่วยงานที่รับผิดชอบในขอบเขตงานที่ขอยกเว้น ทำการประเมินความเสี่ยงพร้อมทั้งกำหนดแนวทางควบคุมความเสี่ยง นำเสนอให้ทีมงานรักษาความปลอดภัยเทคโนโลยีสารสนเทศพิจารณา และขอความเห็นชอบจากคณะกรรมการฯ

การรักษาความปลอดภัยเของระบบสารสนเทศ ครอบคลุมหัวข้อดังต่อไปนี้

1. ความปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resource Security)
2. การบริหารจัดการทรัพย์สินด้านสารสนเทศ (Asset Management)
3. การรักษาความปลอดภัยของข้อมูล (Information Security)
4. การควบคุมการเข้าถึง (Access Control)

5. การบริหารจัดการการเข้ารหัสข้อมูล (Cryptography)
6. การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)
7. การรักษาความปลอดภัยในการปฏิบัติงาน (Operations Security)
8. การรักษาความปลอดภัยของระบบเครือข่ายสื่อสาร (Communications Security)
9. การจัดหา การพัฒนาและการดูแลระบบ (System acquisition, development and maintenance)
10. การบริหารจัดการผู้ให้บริการภายนอก (Supplier relationships)
11. การจัดการเหตุการณ์ผิดปกติด้านความปลอดภัย (Information security incident management)
12. การบริหารจัดการด้านการดำเนินธุรกิจอย่างต่อเนื่อง (Information security aspects of business continuity management)
13. ความปลอดภัยในการใช้สื่อสังคมออนไลน์ (Social Media)
14. ความปลอดภัยในการใช้บริการ Cloud Computing
15. การใช้ e-mail
16. การปฏิบัติตามข้อกำหนด (Compliance)
17. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)
18. การจ้างงานภายนอกบริการเทคโนโลยี (Technology Service Outsourcing)

1. ความปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resource Security)

วัตถุประสงค์

เพื่อกำหนดและคัดสรรบุคคลก่อนที่จะเข้ามาทำงาน เพื่อลดความเสี่ยงจากความผิดพลาด การขโมย การปลอมแปลง และการนำข้อมูลไปใช้ในทางที่ไม่เหมาะสม

1.1 การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)

- หน่วยงานบริหารทรัพยากรบุคคล ต้องตรวจสอบประวัติรวมไปถึงคุณสมบัติของผู้สมัครงาน โดยระมัดระวังที่จะไม่ละเมิดต่อกฎหมาย ระเบียบ หรือข้อบังคับที่เกี่ยวข้องกับความเป็นส่วนบุคคล การจ้างงาน หรือแรงงาน
- หน่วยงานบริหารทรัพยากรบุคคลต้องทำการพิจารณา ตรวจสอบเอกสาร ข้อมูล หรือบุคคลอ้างอิงของผู้สมัครงาน ข้อมูลหลักฐานแสดงตนของผู้สมัครงาน และประวัติอาชญากรรมของผู้สมัครงานเฉพาะตำแหน่งงานที่เข้าถึงข้อมูลที่สำคัญ

1.2 การกำหนดเงื่อนไขการจ้างงาน (Terms and Conditions of Employment)

- พนักงานใหม่ต้องลงนามในสัญญาการว่าจ้างและเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) และ/หรือ เอกสารอื่นๆ ที่เกี่ยวข้อง เพื่อเป็นการยอมรับว่าข้อมูลต่างๆ ที่ได้รับทราบและใช้งานในระหว่างการจ้างงาน เป็นทรัพย์สินของบริษัทฯ และไม่สามารถนำไปใช้เพื่อการอื่นโดยมิได้รับอนุญาต ทั้งนี้ ในการใช้งานข้อมูลทั้งหลายในบริษัทฯ จะถือว่าทุกคนรับทราบและยินยอมปฏิบัติตามเงื่อนไขของนโยบายนี้ รวมไปถึงระเบียบปฏิบัติด้านความมั่นคงทางเทคโนโลยีสารสนเทศทุกประการ
- เพื่อให้การบริหารจัดการบัญชีผู้ใช้ (User ID) เป็นไปอย่างถูกต้องและเป็นปัจจุบัน หน่วยงานบริหารทรัพยากรบุคคลต้องแจ้งให้หน่วยงานเทคโนโลยีสารสนเทศทราบในทันทีที่มีข้อสรุปที่แน่นอน หรือไม่เกิน 30 วัน เมื่อมีเหตุการณ์ดังนี้
  - การว่าจ้างงาน
  - การเปลี่ยนแปลงสภาพการว่าจ้างงาน
  - การสิ้นสุดการเป็นพนักงานหรือสิ้นสุดสัญญาจ้าง

- การโยกย้ายหน่วยงาน
- การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

1.3 การสร้างความความปลอดภัยสารสนเทศขณะเป็นพนักงาน (During Employment)

- จัดให้มีการอบรมให้ความรู้เกี่ยวกับการรักษาความปลอดภัยด้านสารสนเทศ (Information Security Awareness) แก่พนักงาน
- พนักงานทุกคนมีหน้าที่รับผิดชอบในการดูแลและปกป้องทรัพย์สินสารสนเทศ รวมทั้งข้อมูลของบริษัท
- พนักงานทุกคนต้องไม่เข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัทโดยไม่ได้รับอนุญาต ต้องไม่ดำเนินการใด ๆ ที่ส่งผลกระทบต่อผู้อื่นและระบบงานของบริษัท จนทำให้ไม่สามารถปฏิบัติงานได้หรือทำให้เกิดความเสียหายต่อทรัพย์สินสารสนเทศของบริษัท
- พนักงานทุกคนต้องไม่มอบสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศให้กับพนักงานผู้อื่นโดยไม่ได้รับอนุญาต จากผู้บังคับสูงสุดของหน่วยงานที่สังกัดและผู้ดูแลระบบที่ได้รับมอบหมาย

1.4 การลาออก ยกเลิกการจ้างงาน หรือเปลี่ยนแปลง (Termination /Change of Employment)

- หน่วยงานบริหารทรัพยากรบุคคลหรือหน่วยงานต้นสังกัดของพนักงาน ต้องแจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เมื่อมีการลาออก แต่งตั้งโยกย้าย ปลดหรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบของพนักงาน เพื่อทำการปรับปรุง ระงับ ยกเลิกบัญชีผู้ใช้ และยกเลิกสิทธิ์ในการเข้าถึงระบบและข้อมูล

1.5 การคืนทรัพย์สิน (Return on Assets)

- พนักงานบริษัทซึ่งพ้นสภาพจากการจ้างงาน ต้องคืนทรัพย์สินทั้งหมดซึ่งเกี่ยวข้องกับระบบงานคอมพิวเตอร์ เครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วง คู่มือ เอกสารต่าง ๆ และข้อมูลของบริษัท ให้แก่ผู้บังคับบัญชา เมื่อสิ้นสุดหรือพ้นสภาพการเป็นพนักงาน

1.6 การยกเลิก / ปรับปรุงสิทธิ์การเข้าถึง (Removal or adjustment of access rights)

- เมื่อมีการยกเลิกหรือเปลี่ยนแปลงตำแหน่งการเป็นพนักงานของบริษัท หน่วยงานบริหารทรัพยากรบุคคลจะต้องแจ้งต่อหน่วยงานที่เกี่ยวข้องทราบ และหน่วยงานต้นสังกัดต้องแจ้งต่อ ลูกค้า บริษัทคู่ค้า ผู้ให้บริการภายนอก ให้รับทราบตามความเหมาะสม เพื่อระงับหรือยกเลิกการเข้าถึงพื้นที่และข้อมูลต่าง ๆ ของพนักงาน

2. การบริหารจัดการทรัพย์สินด้านสารสนเทศ (Asset Management)

วัตถุประสงค์

เพื่อให้บริษัทมีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างครบถ้วนและควบคุมดูแลทรัพย์สินด้านเทคโนโลยีสารสนเทศให้มีความพร้อมใช้งาน และสามารถรองรับการดำเนินธุรกิจได้อย่างต่อเนื่อง

2.1 ความเป็นเจ้าของทรัพย์สิน (Owner of Assets)

- จัดให้มีเจ้าหน้าที่ผู้รับผิดชอบในการจัดทำปรับปรุงทะเบียนรายการทรัพย์สินด้านระบบสารสนเทศ และบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ รวมทั้งวางแผนรองรับทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้จะสิ้นสุดตามอายุการใช้งาน (end of life) หรือสิ้นสุดการให้บริการ (end of support)

2.2 ทะเบียนทรัพย์สินด้านสารสนเทศ (Inventory of Assets)

- มีการจัดทำทะเบียนรายการทรัพย์สินด้านสารสนเทศ ของฮาร์ดแวร์ (hardware) และซอฟต์แวร์ (software) และข้อมูล (Information) เพื่อบริหารจัดการด้านการรักษาความปลอดภัย
- มีการทบทวน ปรับปรุงทะเบียนรายการทรัพย์สินให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง

2.3 การยกเลิกและเรียกคืนทรัพย์สิน (Return asset)

- ทำการเรียกคืนทรัพย์สินในทันทีจากพนักงานบริษัทเมื่อสิ้นสุดการใช้งานหรือสิ้นสุดการเป็นพนักงาน และกรณีที่ผู้ให้บริการภายนอกมีการใช้ทรัพย์สินให้เรียกคืนทันทีเมื่อมีการยกเลิกสัญญาจ้าง

3. การจัดระดับชั้นความลับของข้อมูล (Information Classification)

วัตถุประสงค์

เพื่อให้บริษัทมีการรักษาความปลอดภัยและความลับของข้อมูล อย่างเหมาะสมตามระดับชั้นความลับของข้อมูล ครอบคลุมการรับส่งข้อมูล ผ่านเครือข่ายสื่อสาร การจัดเก็บหรือใช้งานบนระบบและสื่อบันทึกข้อมูลต่าง ๆ

3.1 หลักเกณฑ์การจัดชั้นความลับของข้อมูล (information classification)

- เจ้าของข้อมูลต้องจำแนกชั้นความลับของข้อมูลทั้งหมดที่อยู่ในความรับผิดชอบของตน โดยพิจารณาจากความจำเป็นในการเข้าถึงข้อมูลเพื่อการปฏิบัติงาน ข้อกำหนดหรือกฎระเบียบที่เกี่ยวข้องในการปกป้องข้อมูล และผลกระทบทางธุรกิจอื่นๆ ที่เกี่ยวข้อง ทั้งนี้ ข้อมูลของบริษัทฯ ถ้าไม่มีการระบุชั้นความลับไว้ให้ถือเป็น "Internal Use Only" ทั้งหมด

3.2 กำหนดให้มีเจ้าของข้อมูล (information owner)

- เจ้าของข้อมูลต้องรับผิดชอบในการกำหนดผู้ใช้งาน สิทธิ์การเข้าถึงและการใช้งานข้อมูลอย่างปลอดภัย

3.3 การจำแนกชั้นความลับของข้อมูล

- ชั้นความลับของข้อมูลแบ่งออกเป็น 4 ประเภท ดังนี้

Secret	คุณลักษณะ:
	• มีความสำคัญต่อบริษัทฯในระดับสูง<u>มาก</u> • หากข้อมูลสูญหาย หรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลเสียหายต่อบริษัทฯในระดับสูง<u>มาก</u> • เกี่ยวข้องกับแผนกลยุทธ์ และทิศทางหลักในการดำเนินธุรกิจ • มีความสำคัญอย่างมากต่อความสำเร็จทางเทคนิค หรือทางการเงินของผลิตภัณฑ์ • จำเป็นต้องมีมาตรการควบคุมการเผยแพร่ข้อมูลที่เข้มงวด โดยพิจารณา<u>จำกัดรายชื่อผู้ได้รับอนุญาตให้เข้าถึงข้อมูล</u>ที่บริษัทฯกำหนดเท่านั้น
	ตัวอย่าง:
	• แผนกลยุทธ์ และทิศทางในการดำเนินธุรกิจ • ข้อมูลสำคัญขององค์ประกอบ และเทคโนโลยีในการพัฒนาผลิตภัณฑ์
Confidential	คุณลักษณะ:
	• มีความสำคัญต่อบริษัทฯในระดับสูง • หากข้อมูลสูญหาย หรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลเสียหายต่อบริษัทฯ • เกี่ยวข้องกับทิศทางการปฏิบัติงานของบริษัทฯ (มีผลเฉพาะในช่วงระยะเวลาหนึ่ง

	• จำเป็นต้องมีมาตรการควบคุมการเผยแพร่ข้อมูลที่เข้มงวด โดยจำกัดการเข้าถึงให้กับกลุ่มบุคคลที่บริษัทฯกำหนดเท่านั้น และต้องได้รับการปกป้องอย่างเหมาะสม
	ตัวอย่าง:
	• ข้อมูลเกี่ยวกับรายได้ ต้นทุน กำไร หรือข้อมูลทางการเงินอื่นๆ • แผนการปฏิบัติงาน แผนผลิตภัณฑ์ ข้อกำหนดทางการตลาด • ขั้นตอนการปฏิบัติงาน แผนงานของโครงการ งานออกแบบ และข้อกำหนดต่างๆ • เอกสารเกี่ยวกับความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ • ข้อมูลเกี่ยวกับลูกค้า และพันธมิตรทางธุรกิจ • ข้อมูลส่วนตัวของพนักงาน
Internal Use Only	คุณลักษณะ:
	• ข้อมูลทางธุรกิจ ข้อมูลที่ใช้งานภายในบริษัทฯ และไม่ได้รับอนุญาตให้นำไปใช้งานภายนอกบริษัทฯ • หากข้อมูลสูญหาย หรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลเสียหายต่อบริษัทฯในระดับต่ำ • ไม่ควรทำสำเนา หรือนำออกจากบริษัทฯโดยไม่ได้รับอนุญาต • เป็นชั้นความลับปริยายของบริษัทฯ (Default)
	ตัวอย่าง:
	• ข้อมูลในระบบ Intranet • ระเบียบ ประกาศภายในบริษัทฯ บันทึกข้อความภายในบริษัทฯ รายงานของโครงการ บันทึกการประชุม
Public	คุณลักษณะ:
	• ข้อมูลที่ไม่จำเป็นต้องได้รับการคุ้มครองความมั่นคงปลอดภัย หรือ • ข้อมูลสำหรับการเผยแพร่ต่อสาธารณะ ผ่านช่องทางที่เหมาะสมซึ่งบริษัทฯพิจารณาอนุมัติแล้ว • หากข้อมูลสูญหาย หรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะไม่ส่งผลเสียหายใดๆต่อบริษัทฯ
	ตัวอย่าง:
	• ข้อมูลบนระบบ Intranet ข้อมูลเพื่อการประชาสัมพันธ์ • ข้อมูลจากการแถลงข่าว หรือรายงานประจำปีของบริษัทฯ

3.4 กำหนดแนวทางการรักษาความปลอดภัยของข้อมูล สอดคล้องตามหลักเกณฑ์การจัดชั้นความลับของข้อมูล

- ข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (data in use) ต้องมีการป้องกันและจัดการอย่างเหมาะสม

- ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (data in motion) ต้องมีการดำเนินการให้มีการรับส่งข้อมูลผ่านเครือข่ายที่มีความปลอดภัย
- ข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (data at rest) ให้มีการดำเนินการให้มั่นใจว่าข้อมูลถูกจัดเก็บอย่างปลอดภัย มีการกำหนดสิทธิ์ในการเข้าใช้งานอย่างเหมาะสม

3.5 การจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (management of removable media)

- สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Removable Media) ที่นำมาใช้งานภายในบริษัท ต้องได้รับการพิจารณาอนุมัติจากหน่วยงานต้นสังกัดและหน่วยงานเทคโนโลยีสารสนเทศต้องตรวจสอบไวรัสคอมพิวเตอร์ สปายแวร์ สแปมเมล์ ก่อนนำมาใช้งาน
- พนักงานต้องใช้งานสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ด้วยความระมัดระวัง หากการใช้งานสื่อบันทึกข้อมูลก่อให้เกิดความเสียหายต่อข้อมูล หรือระบบเทคโนโลยีสารสนเทศของบริษัทฯ พนักงานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น
- สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ ที่มีข้อมูลของบริษัทฯอยู่ภายใน ต้องไม่ถูกนำไปใช้งานร่วมกันกับผู้อื่น
- สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ต้องได้รับการเก็บรักษาในสถานที่มั่นคงปลอดภัยเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ทั้งนี้ พนักงานควรจะเก็บสื่อบันทึกข้อมูลไว้กับตัวตลอดเวลา
- ไม่อนุญาตให้เชื่อมต่อสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ของบุคคลภายนอกเข้ากับอุปกรณ์ หรือระบบเทคโนโลยีสารสนเทศของบริษัทฯ เว้นแต่ เป็นการดำเนินการโดยพนักงานของบริษัทฯ
- สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ ตลอดจนสื่อบันทึกแบบอื่นๆ (เช่น CD-ROM, Floppy Disk ,USB , Flash Drive) ที่มาจากแหล่งภายนอก หรือที่เคยถูกนำไปใช้งานภายนอกบริษัทฯ ต้องได้รับการตรวจหาไวรัสก่อนที่จะถูกนำมาใช้งานภายในบริษัทฯเสมอ หากไฟล์ในสื่อบันทึกถูกเข้ารหัส ผู้ใช้งานต้องทำการถอดรหัสข้อมูลก่อนการตรวจหาไวรัสทุกครั้ง
- สื่อบันทึกข้อมูลที่บริษัทฯส่งให้กับบุคคลภายนอกต้องไม่เคยถูกใช้งานมาก่อน หรือถูกลบข้อมูลออกจนหมดด้วยวิธีการที่มั่นคงปลอดภัย (Secure Delete) ก่อนที่จะบันทึกไฟล์ข้อมูลที่ต้องการรับ-ส่งเข้าไปแทนที่
- ห้ามนำสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ มาเชื่อมต่อโดยตรงกับเครื่อง Server หรืออุปกรณ์ เว้นแต่ได้รับอนุญาตจากหัวหน้าหน่วยงาน IT Infrastructure และต้องดำเนินการตรวจเช็คไวรัสก่อนการเชื่อมต่อระบบ

3.6 การควบคุมดูแลรักษาความปลอดภัยสื่อบันทึกข้อมูลระหว่างขนส่ง (physical media transfer)

- ต้องดำเนินการตามหลักเกณฑ์การจัดชั้นความลับของข้อมูล เพื่อให้มีการควบคุมการเข้าถึงสื่อที่มีข้อมูลสำคัญในระหว่างการขนส่ง
- พนักงานได้รับอนุญาตให้นำข้อมูล ทั้งในรูปแบบเอกสาร หรือแบบอิเล็กทรอนิกส์ ออกไปใช้งานนอกพื้นที่ บริษัทฯ ได้ ตามความจำเป็นในการปฏิบัติงาน อย่างไรก็ตาม ข้อมูลในรูปแบบอิเล็กทรอนิกส์นั้นต้องถูกใช้งาน กับเครื่องคอมพิวเตอร์ที่ได้รับการจัดหาให้โดยฝ่ายเทคโนโลยีสารสนเทศเท่านั้น

3.7 การทำลายข้อมูล (information disposal)

- มาตรฐานและระเบียบวิธีปฏิบัติการทำลายข้อมูล (information disposal) ให้ดำเนินการตามขั้นตอนการปฏิบัติงานการจัดระดับชั้นความลับของข้อมูล
- พิจารณาวิธีการทำลายข้อมูลให้สอดคล้องตามหลักเกณฑ์การจัดชั้นความลับของข้อมูล โดยมีกระบวนการควบคุมการทำลายข้อมูล ที่ครอบคลุมการอนุมัติจากหน่วยงานเจ้าของข้อมูลหรือผู้มีอำนาจอนุมัติก่อนดำเนินการ

- จัดให้มีการทำลายข้อมูลก่อนทุกครั้งเมื่อมีการยุติหรือยกเลิกการใช้งาน เช่น หมดอายุเสื่อมสภาพ หรือหมดสัญญา ส่งคืน หรือถ่ายโอน หรือบริจาค หรือจัดจำหน่ายต่อ หรือไม่ใช้งานแล้ว
- การทำลายข้อมูลในสื่อสำรองบันทึกข้อมูลด้านเทคโนโลยีสารสนเทศ ที่มีอายุใช้งานเกิน 10 ปี หรือตามที่กฎหมายกำหนด โดยต้องได้รับการอนุมัติจากเจ้าของข้อมูลก่อน

4. การควบคุมการเข้าถึง (Access Control)

วัตถุประสงค์

เพื่อให้บริษัทมีการบริหารจัดการบัญชีและสิทธิ์ของผู้ใช้งานอย่างมีประสิทธิภาพเป็นไปตามหลักความจำเป็นของการใช้งานและสอดคล้องกับหลักการแบ่งแยกหน้าที่ และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

4.1 การบริหารจัดการบัญชีผู้ใช้ระบบ (User Access Management)

- กำหนดให้มีกระบวนการและมีหน่วยงานที่รับผิดชอบในการเพิ่ม เปลี่ยนแปลง และลบ บัญชีและสิทธิ์ของผู้ใช้ระบบ
- ในการเข้าใช้ระบบงานทุกครั้ง จะต้องมีการระบุตัวตนและพิสูจน์ตัวตนด้วยวิธีการที่เหมาะสม เช่น การใช้บัญชีผู้ใช้ (Username ,Password)
- ในระบบงานที่มีความสำคัญ ควรมีการจัดทำตารางควบคุมการให้สิทธิ์ (Authorization Matrix) ที่สอดคล้องกับตำแหน่งหน้าที่งาน ตามหลักการตามความจำเป็นของหน้าที่รับผิดชอบ
- กำหนดให้มีขั้นตอนการขอสิทธิการเข้าใช้ระบบและมีการอนุมัติโดยผู้ที่มีอำนาจอนุมัติทุกครั้งที่มีการเพิ่ม ยกเลิก และ เปลี่ยนแปลง ทั้งบัญชีผู้ใช้และสิทธิ์ของผู้ใช้
- เมื่อมีพนักงานลาออกจากงานหรือเปลี่ยนหน้าที่ความรับผิดชอบ หน่วยงานต้นสังกัดและหน่วยงานทรัพยากรบุคคลต้องแจ้งหน่วยงานเทคโนโลยีสารสนเทศทราบ เพื่อทำการปรับปรุงหรือยกเลิกบัญชีผู้ใช้
- ให้ดำเนินการทบทวนสิทธิในการเข้าถึงระบบของพนักงาน (Review of user access rights) อย่างน้อยปีละ 1 ครั้ง หรือให้พิจารณาดำเนินการตามรอบระยะเวลาที่เหมาะสม

4.2 การบริหารจัดการรหัสผ่าน (Password Management)

- ผู้ใช้งานแต่ละคนต้องได้รับมอบ Unique user account เพื่อใช้ในการเข้าถึงระบบและบริการต่างๆ ของบริษัทฯ ทั้งนี้ การมอบสิทธิ์ดังกล่าวต้องสอดคล้องตามหลักการ “Need-to-Know” และ “Need-to-Use” อย่างเคร่งครัด รหัสผ่านต้องได้รับการเปลี่ยนเมื่อเข้าใช้งานครั้งแรก และเปลี่ยนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดไว้ในมาตรฐานการควบคุมรหัสผ่าน (Password Standard)
- การควบคุมรหัสผ่านต้องเป็นไปตามมาตรฐานการควบคุมรหัสผ่าน (Password Standard)
- รหัสผ่านถือเป็นข้อมูลลับ และเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านอย่างมั่นคงปลอดภัย ห้ามมิให้มีการใช้งาน User account ร่วมกันหรือให้ผู้อื่นเข้าใช้งาน User account ของตนโดยเด็ดขาด ทั้งนี้ รวมถึงสมาชิกในครอบครัวเมื่อผู้ใช้งานนำงานกลับไปทำที่บ้านด้วย
- ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่กระทำผ่าน User account และรหัสผ่านของตนทั้งหมด ทั้งในด้านกฎระเบียบของบริษัทและด้านกฎหมาย
- รหัสผ่านที่มีสิทธิพิเศษในระบบสำคัญของบริษัทฯต้องได้รับการควบคุมโดยผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายหน้าที่อย่างเป็นทางการ
- ผู้ใช้งานทุกคนต้องได้รับการฝึกอบรมเพื่อให้มีความรู้และความตระหนักในการใช้งานรหัสผ่านอย่างถูกต้อง และรับทราบเทคนิคต่างๆ ที่ใช้ในการหลอกลวงและนำไปสู่การโจรกรรมข้อมูล

- ระบบหรือการกระทำใดๆ ที่ไม่สอดคล้องกับนโยบายฉบับนี้ต้องได้รับการบันทึก ประเมิน และพิจารณาอนุมัติอย่างเหมาะสมเป็นกรณีไป เช่น ถ้าหากจำเป็นต้องมีการใช้งาน User account ร่วมกันโดยผู้ใช้งานตั้งแต่หนึ่งคนขึ้นไป ผู้ดูแลระบบต้องเก็บบันทึกรายชื่อผู้ที่มีสิทธิ์ใช้งาน User account ดังกล่าว และระบบทั้งหมดที่ User account นั้นมีสิทธิ์เข้าถึง
- User account ที่มีวัตถุประสงค์พิเศษ เช่น DEPT_USER อาจได้รับการสร้างขึ้นเพื่อเป็น user กลางของหน่วยงาน และ/หรือ เพื่อใช้งานร่วมกันโดยผู้ใช้งานมากกว่าหนึ่งคนขึ้นไป โดยต้องมีผู้ใช้งานหนึ่งคนที่ได้รับการแต่งตั้งให้ทำหน้าที่เป็นเจ้าของ user account นั้น
- ถ้าหากผู้ใช้งานสงสัยว่า User account หรือรหัสผ่านของตนถูกล่วงละเมิด ให้ผู้ใช้งานแจ้งเหตุต่อผู้ดูแลระบบ และทำการเปลี่ยนแปลงรหัสผ่านทั้งหมดทันที
- การขอ Reset Password โดยผู้ใช้งานต้องดำเนินการตามกระบวนการมาตรฐานของบริษัทฯเท่านั้น โดยผู้ใช้งานต้องแสดงตัวตน และสิทธิ์ความเป็นเจ้าของ User account นั้นๆ เจ้าหน้าที่ที่เกี่ยวข้องมีสิทธิ์ในการขอข้อมูลและพิสูจน์ตัวตนของผู้ใช้งานตามความเหมาะสม
- ในทางกลับกัน ผู้ใช้งานอาจได้รับการร้องขอจาก ผู้ดูแลระบบให้ทำการเปลี่ยนรหัสผ่านใหม่ ถ้าหากรหัสผ่านของผู้ใช้งานไม่มีความมั่นคงปลอดภัย สามารถถูกคาดเดา หรือถูกล่วงละเมิดได้ง่าย ทั้งนี้ ผู้ใช้งานต้องตรวจสอบความถูกต้องของแหล่งที่มาของคำร้องขอดังกล่าวด้วย เพื่อให้มั่นใจว่าการร้องขอนั้นไม่ได้เป็นการหลอกลวง

4.3 การบริหารจัดการเข้าถึงระบบงาน (System and application access control)

- การบริหารสิทธิการเข้าถึงระบบของผู้มีหน้าที่ดูแลระบบงาน ต้องมีการกำหนดสิทธิและแบ่งแยกหน้าที่ในการทำงานตามความจำเป็นและความเหมาะสม
- มีการระงับหรือยกเลิก Default Account ที่ไม่มีความจำเป็นในการใช้งานหรือไม่มีความจำเป็นต่อการทำงานของระบบ เช่น Guest Accounts เป็นต้น
- มีการเปลี่ยน Default Password ของบัญชีผู้ใช้ที่มากับระบบงานให้เป็นไปตามมาตรฐานรหัสผ่าน หากกรณีจำเป็นต้องใช้จะต้องกำหนดให้มีการทบทวน Log การเข้าถึงและการเข้าใช้งานของบัญชีผู้ใช้ที่มากับระบบงานด้วย
- ระบบต้องสามารถจัดเก็บประวัติการเข้าถึงได้ เพื่อใช้ในการสอบทาน
- การบริหารจัดการบัญชีผู้ใช้สิทธิสูง (High privilege user ID) ให้ดำเนินการดังนี้
  - มีการควบคุมดูแลการเบิกใช้บัญชีผู้ใช้งานที่มีสิทธิ์สูงสุด (Highest Privilege User) อย่างเหมาะสม
  - มีการจัดเก็บรหัสผ่านของบัญชีผู้ใช้ที่มีสิทธิ์สูงสุดโดยหน่วยงานที่มีความเป็นอิสระจากหน่วยงานของผู้ขอเบิกใช้ และทำการเปลี่ยนรหัสผ่านหลังการใช้งานและตามรอบระยะเวลา

5. การบริหารจัดการการเข้ารหัสข้อมูล (Cryptography)

วัตถุประสงค์

เพื่อให้บริษัทมีการรักษาความปลอดภัยและการจัดการความลับของข้อมูล

- การเข้ารหัสข้อมูล ให้ปฏิบัติตามหลักเกณฑ์การจัดชั้นความลับของข้อมูล (information classification)
- กรณีที่มีการส่งข้อมูลที่เป็นความลับหรือความสำคัญผ่านช่องทางอิเล็กทรอนิกส์ หรือเคลื่อนย้ายสื่อบันทึกข้อมูลที่มีความสำคัญ ผู้รับผิดชอบต้องเข้ารหัสข้อมูล เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงข้อมูลได้
- วิธีการเข้ารหัสข้อมูล ควรใช้มาตรฐานการเข้ารหัสข้อมูลที่เชื่อถือได้และเป็นมาตรฐานไทยและสากล โดยมีการทบทวนประสิทธิภาพของวิธีการเข้ารหัสข้อมูลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าวิธีการเข้ารหัสข้อมูลที่ใช้งานยังคงมีความปลอดภัยเพียงพอ

- มีการบริหารจัดการกุญแจเข้ารหัสข้อมูล (key management) ที่มีความปลอดภัย
    - กุญแจที่ใช้ในการเข้ารหัสข้อมูลของบริษัทฯจัดอยู่ในชั้นความลับ “Confidential” หรือ “Secret” เสมอ ทั้งนี้ การเข้าถึงกุญแจต้องถูกจำกัดตามหลักการ “Need-to-Know” โดยการเปิดเผยกุญแจต่อบริษัทที่ปรึกษา คู่สัญญา พนักงานชั่วคราว หรือบุคคลภายนอกใดๆ ต้องได้รับอนุญาตจากหัวหน้าฝ่ายก่อนเสมอ นอกจากนี้ กุญแจต้องได้รับการเข้ารหัสทุกครั้งเมื่อมีการส่งผ่านระบบเครือข่าย
    - อุปกรณ์ หรือวัสดุใดๆ ที่ใช้ในการสร้าง การเก็บรักษากุญแจ และการทำสำเนากุญแจ รวมถึงกุญแจที่ถูกบันทึกอยู่ในรูปของเอกสาร ต้องได้รับการปกป้องจากการสูญหาย เสียหาย ถูกเปลี่ยนแปลงแก้ไข หรือเข้าถึงโดยไม่ได้รับอนุญาต
    - กฎการเลือกกุญแจเข้ารหัสที่มั่นคงปลอดภัย ต้องเป็นไปตามหลักการเดียวกันกับกฎการเลือกรหัสผ่านที่มั่นคงปลอดภัย

6. การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

วัตถุประสงค์

เพื่อให้บริษัทมีการรักษาความปลอดภัยและความพร้อมใช้งานของศูนย์คอมพิวเตอร์ พื้นที่สำคัญที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการปฏิบัติงาน

6.1 การควบคุมการเข้าถึงพื้นที่สำนักงาน

- บุคคลภายนอกต้องทำการแลกบัตรประจำตัวของตนที่ออกให้โดยหน่วยงานรัฐ เช่น บัตรประชาชน ใบขับขี่ พาสปอร์ต ฯลฯ กับบัตรผู้มาติดต่อของบริษัทฯ ก่อนได้รับอนุญาตให้เข้าถึงพื้นที่สำนักงาน
- พนักงานและบุคคลภายนอกต้องติดบัตรพนักงานหรือบัตรผู้มาติดต่อตลอดเวลาที่อยู่ในพื้นที่สำนักงาน ทั้งนี้ บัตรพนักงานและบัตรผู้มาติดต่อไม่อนุญาตให้โอนกรรมสิทธิ์ หรือหยิบยืมกันใช้งาน
- พนักงานต้องไม่เปิดประตูสำนักงานทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่สำนักงานโดยเด็ดขาด เว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรพนักงานหรือบัตรผู้มาติดต่อได้ เพื่อเป็นการป้องกันการเข้าถึงพื้นที่สำนักงาน และพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับอนุญาต
- ผู้ใช้งานต้องแจ้งพนักงานรักษาความปลอดภัยทันที เมื่อพบเห็นบุคคลแปลกหน้าหรือบุคคลที่ไม่แขวนบัตรพนักงานหรือบัตรผู้มาติดต่อในพื้นที่สำนักงาน
- พนักงานควรติดตาม ควบคุมดูแล และให้คำแนะนำผู้ที่มาติดต่อกับตนตลอดเวลาที่ผู้มาติดต่อนั้นอยู่ในพื้นที่สำนักงาน
- พนักงานควรตรวจสอบความมั่นคงปลอดภัยของพื้นที่ทำงานของตนเป็นประจำทุกวันหลังเลิกงาน เพื่อให้มั่นใจว่าตู้เซฟ ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่างๆ ได้รับการปิดและล๊อค อย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย
- ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงาน ในห้องประชุม หรือในตู้ที่ไม่ได้ล๊อคกุญแจโดยเด็ดขาด
- ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะโดยไม่ได้รับการทำลายอย่างเหมาะสม การทำลายข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์เหล่านี้อ้างอิงได้จาก ข้อ *3. การจัดระดับชั้นความลับของข้อมูล (Information Classification)*
- พนักงานต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาด เว้นแต่บุคคลผู้นั้นเป็นเจ้าหน้าที่ที่ได้รับอนุญาตให้ดำเนินการ และเป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องเท่านั้น

- พนักงานต้องไม่เปิดเผยสถานที่ตั้งของ Data Center ต่อบุคคลภายนอกโดยเด็ดขาด เว้นแต่บุคคลภายนอกนั้นมีความจำเป็นต้องรับทราบเพื่อการปฏิบัติงาน
- มีพนักงานรักษาความปลอดภัย เพื่อควบคุมการเข้าถึงของบุคคลภายนอก และมีการรักษาความปลอดภัยของพื้นที่สำนักงานนอกเวลาทำการอย่างเหมาะสม
- มีการป้องกันการบุกรุกของบุคคลภายนอกผ่านทางประตูหนีไฟ
- ประตูทางเข้าออกสำนักงานต้องมีการติดตั้งกล้องวงจรปิด เพื่อดูแลความปลอดภัยของบริเวณสำนักงาน โดยมีเจ้าหน้าที่ควบคุม ดูแล และ ตรวจสอบภาพกล้องวงจรปิด ซึ่งสามารถเก็บบันทึกภาพย้อนหลังได้อย่างน้อย 30 วัน
- ห้ามนำอาหาร และเครื่องดื่มเข้าห้องคอมพิวเตอร์ และเครือข่ายโดยเด็ดขาด

7. การรักษาความปลอดภัยในการปฏิบัติงาน (Operations Security)

วัตถุประสงค์

เพื่อให้มีแนวทางในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศให้มีความปลอดภัย เพื่อให้มีกระบวนการควบคุมที่มีความรัดกุมปลอดภัยและเป็นไปตามมาตรฐานที่กำหนด

7.1 การบริหารจัดการการเปลี่ยนแปลง (Change Management)

- กำหนดมาตรฐานและขั้นตอนการปฏิบัติงาน การบริหารจัดการการเปลี่ยนแปลง เพื่อควบคุมการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศให้มีความรัดกุมเพียงพอ
- กำหนดบทบาทหน้าที่และความรับผิดชอบของผู้บริหารที่ได้รับมอบหมายหรือคณะทำงานจัดการการเปลี่ยนแปลง เพื่อทำหน้าที่ประเมินผลกระทบและพิจารณาเหตุผลความจำเป็นก่อนอนุมัติให้ดำเนินการเปลี่ยนแปลงระบบ ป้องกันการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและไม่ให้เกิดผลกระทบที่อาจเกิดกับระบบที่เกี่ยวข้อง
- ผู้ที่เกี่ยวข้องในกระบวนการบริหารจัดการการเปลี่ยนแปลง ควรมีการแบ่งแยกหน้าที่อย่างเหมาะสม (segregation of duties) เพื่อไม่ให้บุคคลใดบุคคลหนึ่งสามารถปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการ เช่น ผู้มีสิทธิ์ร้องขอ ผู้ที่มีอำนาจในการอนุมัติการเปลี่ยนแปลง ผู้ที่สามารถดำเนินการเปลี่ยนแปลงระบบ เป็นต้น
- คำขอการเปลี่ยนแปลง (change request) ควรได้รับการอนุมัติจากหน่วยงานเจ้าของระบบ (system owner) เพื่อให้มั่นใจได้ว่าการขอเปลี่ยนแปลงได้รับการพิจารณาความจำเป็นอย่างเหมาะสมจากหน่วยงานเจ้าของระบบ
- มีการประเมินผลกระทบหรือทำการทดสอบก่อนนำไปตั้งค่าบนระบบที่ให้บริการจริง เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น
- ควรมีการติดตามผลหลังการเปลี่ยนแปลงระบบ (post implementation review) เพื่อให้มั่นใจได้ว่าการเปลี่ยนแปลงนั้นเป็นไปตามวัตถุประสงค์ที่กำหนด

7.2 การบริหารจัดการการตั้งค่าระบบ (System Configuration Management)

- มีการจัดทำเอกสารการตั้งค่าของระบบงานเครื่องคอมพิวเตอร์ , Server , อุปกรณ์เครือข่ายสื่อสาร และมีการทบทวนปรับปรุงเอกสารให้เป็นปัจจุบันอย่างสม่ำเสมอ
- มีการตั้งค่าระบบที่มีความปลอดภัยของระบบงาน และอุปกรณ์เครือข่ายสื่อสารต่าง ๆ มีการสอบทานการตั้งค่าตามรอบระยะเวลา เพื่อให้สอดคล้องตามมาตรฐานของบริษัท
- ทำการตรวจสอบและเฝ้าระวังการทำงานของระบบงานหลักและระบบงานสนับสนุนสำหรับศูนย์ควบคุมคอมพิวเตอร์ (Data Center) ให้เป็นไปตามค่ามาตรฐานที่กำหนด พร้อมทั้งกำหนดให้มีการแจ้งเตือนในกรณีที่ระบบงานที่สำคัญทำงานผิดปกติ

- มีการบันทึกการปรับปรุงข้อมูลทุกๆครั้งโดยละเอียดเพื่อใช้ในการติดตามและตรวจสอบประวัติโดยส่งรายงานให้คณะกรรมการฯรับทราบเป็นประจำอย่างน้อยปีละ 1 ครั้ง

7.3 การบริหารจัดการ patch (Patch Management)

- มีการบริหารจัดการ patch เพื่อให้มีการควบคุมที่รัดกุมปลอดภัย และติดตั้งได้อย่างเหมาะสม
- กำหนดให้ผู้ดูแลระบบทำการติดตั้ง patch โดยประเมินจากการประเมินความเสี่ยงและการจัดความสำคัญของระบบ และจัดให้มีการทดสอบ patch ก่อนนำไปติดตั้งบนระบบที่ให้บริการจริงตามความจำเป็น
- มีการบันทึกการปรับปรุงข้อมูลทุกๆครั้งโดยละเอียดเพื่อใช้ในการติดตามและตรวจสอบประวัติโดยส่งรายงานให้คณะกรรมการฯรับทราบเป็นประจำอย่างน้อยปีละ 1 ครั้ง

7.4 การจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging)

- มีการจัดเก็บข้อมูลบันทึกเหตุการณ์ของเครื่อง Server ระบบงาน อุปกรณ์เครือข่ายสื่อสารที่สำคัญด้วยวิธีการที่ปลอดภัย กำหนดให้บันทึกกิจกรรมการใช้งานของผู้ใช้ การให้บริการของระบบ และเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับความปลอดภัย และจัดเก็บย้อนหลังเป็นระยะเวลาอย่างน้อย 90 วัน หรือตามที่กฎหมายกำหนด
- มีการใช้ระบบในการควบคุมค่าเวลาของเครื่อง Server ระบบงาน อุปกรณ์เครือข่ายสื่อสารให้ตรงกันโดยใช้ Network Time Protocol: NTP (clock synchronization) เพื่อให้ค่าเวลาในการบันทึกเหตุการณ์มีความถูกต้องในลักษณะ real-time ซึ่งต้องรับสัญญาณนาฬิกาจากแหล่งที่มีความน่าเชื่อถือ
- ข้อมูลการบันทึกเหตุการณ์ของอุปกรณ์สำคัญควรจัดเก็บไว้ที่เครื่อง Server ที่แยกเฉพาะ อย่างน้อยครอบคลุม access log และ activity log โดยมีการรักษาความปลอดภัยเพียงพอ
- ระบบต้องมีการบันทึกการเข้าถึง (access Log) และบันทึกการดำเนินงาน (activity log) ของผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศที่มีสิทธิ์สูง เช่น system administrator หรือ system operator เพื่อใช้ในการสอบทานการเข้าถึงของผู้ปฏิบัติงาน
- มีการนำ Log มาวิเคราะห์เพื่อหาช่องโหว่ของระบบหรือพฤติกรรมที่ผิดปกติ และส่งรายงานให้คณะกรรมการฯรับทราบเป็นประจำอย่างน้อยปีละ 1 ครั้ง

7.5 การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

- มีการประเมินและติดตามดูแลความเพียงพอของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่ครอบคลุมถึง ระบบคอมพิวเตอร์ ระบบฐานข้อมูล ระบบเครือข่ายสื่อสาร และระบบสาธารณูปโภคที่เกี่ยวข้องกับงานเทคโนโลยีสารสนเทศ
- มีการประเมินแนวโน้มการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศเพื่อวางแผนรองรับการใช้งานในอนาคต (capacity planning) โดยครอบคลุมทั้งระบบหลักและระบบสำรอง
- จัดทำรายงานความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศนำเสนอต่อผู้บริหารที่ได้รับมอบหมายที่เกี่ยวข้องรับทราบตามแผนงานของหน่วยงาน
    - เพื่อรายงานให้ทางผู้บริหารรับทราบก่อนจะมีการดำเนินการจัดทำงบประมาณประจำปี
    - เพื่อให้มีการกำกับดูแลความพร้อมและความเพียงพอของระบบในการรองรับการให้บริการทางธุรกิจได้อย่างต่อเนื่อง

7.6 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (Security Monitoring)

- ติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม เพื่อให้มีการติดตามดูแลความปลอดภัยของระบบอย่างต่อเนื่อง
- ทำการตรวจจับเหตุการณ์ผิดปกติที่กระทบต่อความปลอดภัยของระบบที่สำคัญและระบบเครือข่ายสื่อสาร เพื่อให้

รับทราบความผิดปกติหรือภัยคุกคาม และสามารถดำเนินการป้องกันหรือรับมือได้อย่างเหมาะสม

- ทำการวิเคราะห์และจัดการข้อมูลภัยคุกคามที่อาจเกิดขึ้นอย่างต่อเนื่อง ครอบคลุม ลักษณะการโจมตี ความเป็นไปได้ที่จะเกิดเหตุการณ์ภัยคุกคาม รวมถึงวิธีการรับมือกับภัยคุกคามนั้น เพื่อนำมาใช้สนับสนุนการรับมือต่อภัยคุกคามทางไซเบอร์
- กรณีที่พบเหตุการณ์หรือความผิดปกติ จะต้องรายงานให้ทางผู้บริหารทราบทันที

7.7 การบริหารจัดการช่องโหว่ (Vulnerability Management)

- ทำการประเมินช่องโหว่และทดสอบการเจาะระบบ สำหรับระบบที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) และระบบงานที่สำคัญอย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงค่าความปลอดภัยหรือมีการเปลี่ยนแปลงความเสี่ยงอย่างมีนัยสำคัญ
- รายงานผลการประเมินช่องโหว่และผลการทดสอบเจาะระบบ พร้อมทั้งแนวทางและแผนการดำเนินการปรับปรุงแก้ไขต่อหัวหน้าหน่วยงานเทคโนโลยีสารสนเทศ

7.8 การสำรองข้อมูล (Data Backup)

- กำหนดให้มีข้อมูลสำรองพร้อมใช้และมีความปลอดภัย ตามขั้นตอนการปฏิบัติงาน การสำรองข้อมูล (Back-up Procedure) มีกระบวนการสำรองทั้งระบบ (full backup) ทุกครั้ง ภายหลังจากที่มีการเปลี่ยนแปลงระบบปฏิบัติการ และระบบงานแบบมีนัยสำคัญ เพื่อให้ระบบสำรองมีความเป็นปัจจุบัน
- มีการจัดเก็บสื่อบันทึกข้อมูลสำรองไว้นอกศูนย์คอมพิวเตอร์หลักหรือนอกสถานที่ปฏิบัติงานหลัก โดยมีการรักษาสภาพแวดล้อมและการควบคุมความปลอดภัยในการเข้าถึงข้อมูลที่จัดเก็บไว้
- จัดให้มีการสอบทานการสำรองข้อมูล เพื่อให้มั่นใจว่ามีการสำรองข้อมูลครบถ้วนถูกต้อง พร้อมใช้งานและปลอดภัย

7.9 การรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint Security)

- ติดตั้งระบบปฏิบัติการและโปรแกรมพื้นฐานที่ใช้ในการปฏิบัติงานบนเครื่องคอมพิวเตอร์ ตามที่บริษัทกำหนดเท่านั้น โดยมีการควบคุมและติดตามไม่ให้ผู้ใช้งานสามารถติดตั้งโปรแกรมอื่น ๆ นอกเหนือจากที่กำหนด
- ติดตั้งโปรแกรมรักษาความปลอดภัย anti-Virus / anti-malware โดยมีการปรับปรุงประสิทธิภาพของการป้องกันโปรแกรมไม่ประสงค์ดี (Malware) ให้เท่าทันสำหรับการป้องกันภัยคุกคามใหม่ ๆ
- การจัดเก็บข้อมูลที่มีระดับชั้นความลับสูงสุดในเครื่องคอมพิวเตอร์ของผู้ใช้งาน ต้องมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ จำกัดสิทธิการเข้าถึงและมีการเข้ารหัสข้อมูล
- จำกัดการเข้าถึง shared drive หรือ shared folder ตามความจำเป็นในการใช้งานเท่านั้น โดยต้องได้รับการอนุญาตจากหน่วยงานเจ้าของข้อมูลก่อนการเข้าใช้งาน
- การใช้งานอุปกรณ์ส่วนบุคคล
    - มีการควบคุมการใช้อุปกรณ์ส่วนบุคคล ในการเข้าถึงระบบเครือข่ายสื่อสาร ระบบงานและข้อมูลของบริษัท โดยจัดเก็บรายการคำขอของเครื่องที่ขอใช้งาน โดยต้องได้รับการพิจารณาอนุมัติจากหัวหน้าหน่วยงานต้นสังกัดและผู้มีอำนาจอนุมัติของบริษัท เป็นกรณี ๆ ไป
    - ทำการตรวจสอบ อุปกรณ์ที่นำมาใช้งานในบริษัท โดยเครื่องคอมพิวเตอร์ต้องติดตั้ง anti-virus /anti-malware
    - ไม่อนุญาตให้อุปกรณ์โทรศัพท์เคลื่อนที่ (tablet, smartphone) ที่ถูกปรับแต่ง (rooted หรือ jail broken) ลงทะเบียนใช้งาน

8. การรักษาความปลอดภัยของระบบสื่อสาร (Communications Security)

วัตถุประสงค์

เพื่อให้บริษัทมีโครงสร้างของระบบเครือข่ายสื่อสารที่มั่นคงปลอดภัย มีการออกแบบระบบเครือข่ายสื่อสารที่เหมาะสม และมีการป้องกันหรือเฝ้าระวังการบุกรุกหรือภัยคุกคามในรูปแบบต่าง ๆ

8.1 การรักษาความปลอดภัยระบบเครือข่าย (Network Security Management)

- มีการจัดแบ่งเครือข่ายอย่างเหมาะสม โดยคำนึงถึงระดับความสำคัญของระบบงาน ระดับความสำคัญของข้อมูลที่ถูกประมวลผล รวมถึงความจำเป็นในการเชื่อมต่อจากระบบงานอื่นๆ หรือจากภายนอกบริษัท และจัดให้มีการควบคุมการเชื่อมต่อจากระบบงานต่าง ๆ มายังระบบงานที่มีความสำคัญอย่างเข้มงวด
- มีการแบ่งแยกเครือข่ายส่วนที่เป็น Private Network และ Public Network ออกจากกัน
- มีการจัดตั้งโซนเครือข่าย Demilitarized Zone (DMZ) เพื่อรองรับระบบงานที่ต้องมีการให้บริการ ติดต่อสื่อสาร หรือแลกเปลี่ยนข้อมูลกับภายนอก โดยไม่จัดวาง Server ที่เป็นระบบฐานข้อมูลสำคัญไว้ในโซนดังกล่าว
- ในจุดที่มีการแบ่งแยกเครือข่ายที่พิจารณาว่ามีความสำคัญและมีความเสี่ยง ควรติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่ายที่มีความสามารถในการควบคุมและคัดกรอง Traffic ที่ส่งผ่านระบบเครือข่าย การเฝ้าระวังการบุกรุก การป้องกันการบุกรุก และการตรวจจับไวรัส หรือมัลแวร์ต่างๆ ที่อาจบุกรุกเข้าสู่เครือข่าย
- มีการจำกัดให้เฉพาะบุคคลที่ได้รับมอบอำนาจเท่านั้นที่สามารถเข้าถึงระบบเครือข่าย โดยจำกัดสิทธิ์ในการเข้าถึงระบบเครือข่ายให้อยู่ในส่วนที่มีความจำเป็น และเหมาะสมตามหน้าที่การทำงานเท่านั้น
- การเปลี่ยนแปลงติดตั้งค่าต่างๆ ที่เกี่ยวกับอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย การเปลี่ยนแปลงต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงการตั้งค่าอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่ายอย่างเป็นขั้นตอน พร้อมทั้งได้รับการอนุมัติดำเนินการจากผู้มีอำนาจอนุมัติ
- มีการเปลี่ยน Default Password ของอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย ให้เป็นไปตามนโยบายการควบคุมรหัสผ่าน
- มีการติดตั้ง Software Updates หรือ Patch ที่จำเป็นให้กับอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย ตามคำแนะนำของผู้ผลิต โดยการติดตั้งต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management) อย่างเป็นขั้นตอน

8.2 การควบคุมการเชื่อมต่อกับระบบเครือข่ายสื่อสารของบริษัท

- ไม่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์อื่นใด ที่บริษัทมิได้จัดหาให้มาเชื่อมต่อและใช้งานในระบบเครือข่ายสื่อสารของบริษัท เว้นแต่ได้รับการพิจารณาอนุมัติจากหน่วยงานต้นสังกัด และ หัวหน้าหน่วยงานเทคโนโลยีสารสนเทศการใช้งานการเชื่อมต่อเครือข่ายของบริษัท ต้องใช้หมายเลข IP Address ที่ผู้ดูแลระบบกำหนดให้เท่านั้น
- เครื่องคอมพิวเตอร์ หรืออุปกรณ์อื่นใด ที่มีการเชื่อมต่อกับระบบเครือข่ายของบริษัท ต้องดำเนินการผ่านการควบคุมโดยระบบรักษาความปลอดภัยเครือข่ายของบริษัท
- กำหนดให้มีวิธีการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์ ก่อนที่จะอนุญาตให้เข้ามาใช้งานเครือข่ายของบริษัท
- การใช้งานโปรแกรมหรือข้อมูลบริษัทฯ อนุญาติให้ใช้ได้เฉพาะตัวพนักงานเท่านั้น ห้ามนำโปรแกรมหรือข้อมูลของบริษัทฯไปเปิดเผยกับบุคคลภายนอก ไม่ว่าทางใดทางหนึ่ง
- ห้ามติดตั้งและใช้งานโปรแกรมที่อาจจะมีผลต่อการทำงานของระบบคอมพิวเตอร์และระบบเครือข่าย

8.3 การควบคุมการเชื่อมต่อมาจากเครือข่ายจากระยะไกล (Remote Access)

- กรณีที่ต้องมีการเชื่อมต่อมาจากเครือข่ายจากระยะไกล ต้องมีการระบุและพิสูจน์ตัวตนของบุคคล และกระทำผ่านช่องทางที่มีความปลอดภัย เช่น SSH, VPN, SFTP หรือ SSL/TLS เป็นต้น
- ห้ามทำการเชื่อมต่อเพื่อเข้าถึงระบบเครือข่ายภายในบริษัทจากระยะไกลด้วยเครื่องคอมพิวเตอร์สาธารณะ

8.4 การควบคุมการเชื่อมต่อกับ Wireless Network

- หากคอมพิวเตอร์เครื่องใด ที่มีความจำเป็นต้องเปิดใช้บริการ Wireless Network ต้องใช้มาตรฐานความปลอดภัยที่น่าเชื่อถือได้และเป็นปัจจุบันตามมาตรฐานสากล ซึ่งทางบริษัทฯ ได้ทำการแบ่งกลุ่มย่อยของระบบ Wireless Network ภายใน ดังต่อไปนี้
    - Private

      ใช้สำหรับอุปกรณ์คอมพิวเตอร์ พกพาของพนักงานในบริษัทฯ และอุปกรณ์คอมพิวเตอร์ จะต้องได้รับการลงทะเบียนจากทางหน่วยงาน IT เท่านั้น จึงจะสามารถใช้งานเครือข่ายนี้ได้ โดยมีสิทธิ์ในการเข้าถึง เครื่อง Server ของบริษัทฯ และใช้ Internet ด้วยขอบเขตจำกัด
    - Guest

      ใช้สำหรับผู้ที่มาติดต่อธุรกิจกับบริษัทฯ โดยการใช้งานจะต้องลงทะเบียนเพื่อรับ user name และ password ก่อนใช้งานทุกครั้ง ซึ่งการใช้งานดังกล่าวจะไม่มีสิทธิ์ในการเข้าถึง เครื่อง Server ของบริษัทฯ แต่สามารถใช้ Internet ได้ด้วยขอบเขตและระยะเวลาใช้งานที่จำกัด

9. การจัดหา การพัฒนาและการดูแลระบบ (System Acquisition, Development and Maintenance)

วัตถุประสงค์

เพื่อให้มั่นใจได้ว่ากระบวนการจัดหาและการพัฒนาระบบ มีการควบคุมการรักษาความปลอดภัยอย่างรัดกุมและสอดคล้องตามหลักการควบคุมที่เป็นมาตรฐานสากล

9.1 การจัดหาระบบ (System Acquisition)

- หน่วยงานเทคโนโลยีสารสนเทศ ทำหน้าที่ควบคุมดูแลผู้ให้บริการปฏิบัติตามมาตรฐานและระเบียบวิธีปฏิบัติการออกแบบและพัฒนาระบบ
- หน่วยงานเทคโนโลยีสารสนเทศ ทำหน้าที่กำหนดเกณฑ์ในการตรวจสอบและส่งมอบระบบเทคโนโลยีสารสนเทศ

9.2 การพัฒนาระบบเทคโนโลยีสารสนเทศ (Information Technology System Development)

- กำหนดมาตรฐานและขั้นตอนปฏิบัติการควบคุมการเปลี่ยนแปลงและพัฒนาระบบ โดยคำนึงถึงการรักษาความปลอดภัย ครอบคลุมกระบวนการตั้งแต่จัดทำความต้องการ (requirement) การออกแบบ การพัฒนา และการทดสอบระบบก่อนใช้งานจริง
- กำหนดให้หน่วยงานธุรกิจที่เกี่ยวข้องสอบทานความถูกต้องครบถ้วนตามความต้องการของหน่วยงานธุรกิจ (business requirement) โดยครอบคลุมการรักษาความปลอดภัยตามนโยบายหรือมาตรฐานที่บริษัทกำหนด (security requirement)

9.3 การออกแบบระบบ (System design)

- จัดทำเอกสารรายละเอียดคุณสมบัติทางเทคนิค (Technical Specification) โดยครอบคลุมการรักษาความปลอดภัยตามนโยบายหรือมาตรฐานที่บริษัทกำหนด รวมทั้งจัดให้มีการสอบทานความถูกต้องครบถ้วน

9.4 การพัฒนาระบบ (System development)

- บทบาทหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการพัฒนาระบบควรเป็นไปตามหลักการแบ่งแยกหน้าที่อย่างเหมาะสม (segregation of duties) เพื่อไม่ให้บุคคลใดบุคคลหนึ่งสามารถปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการ เช่น ควรแยกผู้พัฒนาระบบ ออกจากผู้นำระบบขึ้นใช้งานจริง เป็นต้น
- ระบบงานที่มีความสำคัญ ควรมีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สาหรับการพัฒนา (development) การทดสอบ (testing) และระบบที่ให้บริการจริง (production) ออกจากกัน
- มีการควบคุมเวอร์ชั่นของคำสั่งในการเขียนโปรแกรม (source code version control)

9.5 การทดสอบระบบ (Commissioning)

- จัดทำขอบเขตการทดสอบให้ครอบคลุมฟังก์ชันและเงื่อนไขต่าง ๆ ด้านประสิทธิภาพ ตามความต้องการของหน่วยงานธุรกิจ (business requirement) รวมถึงการควบคุมความปลอดภัย
- สำหรับการเปลี่ยนแปลงระบบมีการใช้งานหรือเชื่อมโยงกับระบบอื่นจำนวนมาก ควรจัดให้มีการทดสอบประสิทธิภาพ (performance test) เพื่อให้มั่นใจได้ว่าระบบมีเสถียรภาพเพียงพอในการรองรับการทำงาน
- มีกระบวนการและเอกสารการ sign off ผลการทดสอบจากหน่วยงานที่เกี่ยวข้อง
- มีแนวทางการควบคุมการรักษาความปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ในการทดสอบ เช่น data masking เป็นต้น เพื่อป้องกันความเสี่ยงในการรั่วไหลของข้อมูลสำคัญดังกล่าว
- มีการจัดทำคู่มือและอบรมผู้ใช้งานและผู้ดูแลระบบ เพื่อให้มีความเข้าใจฟังก์ชันการทำงานและมีการใช้งานระบบอย่างปลอดภัย

9.6 การนำระบบขึ้นใช้งานจริง (system deployment)

- การนำระบบขึ้นใช้งานจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่บริษัทกำหนด เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

10. การบริหารจัดการผู้ให้บริการภายนอก (Supplier relationships)

วัตถุประสงค์

เพื่อให้บริษัทมีแนวทางการบริหารจัดการผู้ให้บริการภายนอก หรือพันธมิตรทางธุรกิจที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของบริษัทหรือสามารถเข้าถึงข้อมูลสำคัญของลูกค้าของบริษัท และกำหนดมาตรฐานในการบริหารจัดการผู้ให้บริการภายนอก เพื่อควบคุมให้มีการรักษาความปลอดภัยข้อมูลของบริษัทโดยอย่างน้อยครอบคลุมในเรื่องดังต่อไปนี้

- ก่อนใช้บริการ บริษัทดำเนินการวิเคราะห์ผลกระทบที่อาจเกิดขึ้นกับข้อมูลหรือระบบเทคโนโลยีสารสนเทศที่ผู้ให้บริการภายนอกสามารถเข้าถึง โดยอย่างน้อยควรพิจารณา ขอบเขต เหตุผลและความจำเป็นในการเข้าถึงข้อมูลหรือระบบเทคโนโลยีสารสนเทศ ข้อจำกัดหรือข้อตกลงในการเปลี่ยนแปลงผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจและการยกเลิกหรือสิ้นสุดสัญญา
- ข้อกำหนดในการรักษาความปลอดภัยของหน่วยงานภายนอก รวมถึง sub-contract ต้องปฏิบัติ โดยควรสอดคล้องตามนโยบายการรักษาความปลอดภัยที่บริษัทกำหนด
- ข้อตกลงการไม่เปิดเผยข้อมูล (non-disclosure agreement)
- ข้อตกลงด้านความมั่นคงปลอดภัย (security policy)

- สัญญาการให้บริการและเงื่อนไขระหว่างบริษัทและผู้ให้บริการภายนอก สอดคล้องตามนโยบายการรักษาความปลอดภัยที่บริษัทกำหนด เช่น การทำลายข้อมูลของบริษัทหรือลูกค้าทั้งหมด เมื่อสิ้นสุดการใช้บริการ ความรับผิดชอบต่อการรั่วไหลของข้อมูลอันเนื่องมาจากการนำข้อมูลไปใช้ นอกเหนือจากที่ระบุไว้ในสัญญาหรือข้อตกลงในการให้บริการ เป็นต้น
- มีกระบวนการติดตาม ประเมิน ทบทวน และรายงานผลการปฏิบัติงานของหน่วยงานภายนอก

11. การจัดการเหตุการณ์ผิดปกติด้านความปลอดภัย (Information security incident management)

วัตถุประสงค์

เพื่อให้บริษัทมีแนวทางในการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงเหตุการณ์ผิดปกติจากภัยคุกคามทางไซเบอร์อย่างเหมาะสมทันการณ์ ให้สามารถจัดการแก้ไข ปัญหาให้กลับสู่สภาพปกติได้อย่างรวดเร็วและจำกัดความเสียหายที่ส่งผลกระทบต่อธุรกิจของบริษัท และเพื่อให้มีกระบวนการติดตามหาสาเหตุที่แท้จริง ให้มีแนวทางป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติซ้ำในอนาคต

11.1 การบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT Incident Management)

- กำหนดมาตรฐานและขั้นตอนการปฏิบัติงาน การบริหารจัดการเหตุการณ์ผิดปกติด้านความปลอดภัยสารสนเทศ ครอบคลุมตั้งแต่กระบวนการหรือเครื่องมือในการบันทึกเหตุการณ์ผิดปกติ การกำหนดประเภท การจัดระดับความรุนแรง การวิเคราะห์หาสาเหตุ การดาเนินการแก้ไข การติดตามแก้ไข การรายงานเหตุการณ์ผิดปกติ
- จัดให้มีศูนย์รับแจ้งเหตุการณ์ผิดปกติ โดยทำหน้าที่ในการบันทึกและแก้ไขในเบื้องต้น หรือส่งต่อเหตุการณ์ผิดปกติไปยังหน่วยงานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง
- จัดทำแผนการรับมือกับเหตุการณ์ผิดปกติ ตามความสำคัญของเหตุการณ์ เพื่อให้สามารถรับมือและตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและทันการณ์ โดยอย่างน้อยแผนควรระบุกระบวนการรับมือและช่องทางประสานงานจากผู้เชี่ยวชาญทั้งภายในและภายนอก และมีแนวทางการตรวจสอบ วิเคราะห์หาสาเหตุ และประเมินผลกระทบ
- จัดทำรายงานเหตุการณ์ผิดปกติ เสนอต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย
- ในกรณีเกิดปัญหาหรือเหตุการณ์ผิดปกติที่เกิดจากการใช้งานเทคโนโลยีสารสนเทศ จนเป็นเหตุให้บริษัทไม่สามารถให้บริการพื้นฐาน แก่ลูกค้าในวงกว้าง หรือเกิดเหตุการณ์ที่มีนัยสำคัญซึ่งอาจส่งผลกระทบต่อชื่อเสียงของบริษัท รวมถึงกรณีเทคโนโลยีสารสนเทศที่สำคัญของบริษัท ถูกโจมตีหรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ และเป็นปัญหาหรือเหตุการณ์ที่ต้องรายงานต่อผู้บริหารในตำแหน่งสูงสุดของบริษัททราบ ให้หน่วยงานเทคโนโลยีสารสนเทศจัดทำรายงานปัญหาหรือเหตุการณ์ผิดปกติที่เกิดขึ้น ส่งไปยังสำนักงานคณะกรรมการการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย ตามข้อกำหนดของ คปภ.

12. การบริหารจัดการด้านการดำเนินธุรกิจอย่างต่อเนื่อง (Information security aspects of business continuity management)

วัตถุประสงค์

- เพื่อให้บริษัทมีแนวทางรองรับเหตุการณ์ผิดปกติที่ระบบเกิดหยุดชะงักหรือเกิดความเสียหาย โดยที่ธุรกิจสามารถดำเนินการได้อย่างต่อเนื่องและสามารถกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่ยอมรับได้
- มีการจัดทำแผนการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan : BCP) โดยต้องได้รับการอนุมัติจากคณะกรรมการ BCM และจัดให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

- การจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง ควรคำนึงถึงลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ เหตุการณ์ความเสียหายต่าง ๆ และความเสี่ยงที่เกี่ยวข้องในการดำเนินธุรกิจของบริษัท เช่น ด้านปฏิบัติการ ด้านชื่อเสียง และความเสี่ยงที่มีผลกระทบต่อบริษัท ผู้ใช้บริการ ผู้มีส่วนได้เสีย จัดให้มีการทดสอบแผนการดำเนินธุรกิจอย่างต่อเนื่อง อย่างน้อยปีละ 1 ครั้ง

13. ความปลอดภัยในการใช้สื่อสังคมออนไลน์ (Social Media)

วัตถุประสงค์

เพื่อเป็นแนวทางในการกำกับดูแลการเผยแพร่ข้อมูลและการเข้าถึงสื่อเครือข่ายสังคมออนไลน์ของ “องค์กร” รวมถึงบริการอิเล็กทรอนิกส์ตลอดจนการแสดงความคิดเห็นของบุคลากรในองค์กร ผ่านสื่อเครือข่ายสังคมออนไลน์ให้เป็นไปอย่างถูกต้องเหมาะสม มีความเป็นระเบียบเรียบร้อยและเกิดประโยชน์สูงสุด แบ่งออกเป็น 2 ส่วน

13.1 การปฏิบัติในสื่อสังคมออนไลน์

- แนวปฏิบัติ
  - องค์กรอนุญาตให้ใช้เครือข่ายสำหรับการเข้าถึงสังคมออนไลน์ประเภทเว็บไซด์ที่ไม่มีเนื้อหาขัดต่อกฎหมาย ศีลธรรม และหลักจรรยาบรรณองค์กร
  - หน่วยงานภายในองค์กร บุคลากร สามารถแสดงชื่อผู้ใช้งานในโลกออนไลน์ เพื่อประโยชน์ในการเผยแพร่ประชาสัมพันธ์ที่เกี่ยวข้องกับองค์กรติดต่อสื่อสารระหว่างกัน แต่ต้องแยกแยะให้ชัดเจนว่าข้อความใดเป็น “ข่าวประชาสัมพันธ์” ข้อความใดเป็น “ความคิดเห็น” “ความคิดส่วนบุคคล” “การแลกเปลี่ยนข่าวสารส่วนตัว” “การเผยแพร่ข่าวสารเรื่องงาน” หรืออื่นๆ และความคิดเห็นดังกล่าวควรคำนึงถึงประโยชน์สาธารณะด้วย
  - การใช้สื่อสังคมออนไลน์ที่แสดงสังกัดหน่วยงานภายในองค์กร ควรแจ้งให้ผู้บังคับบัญชาทราบก่อนทุกครั้ง
  - พึงระมัดระวังการใช้ถ้อยคำและภาษาที่อาจเป็นการดูหมิ่น หรือหมิ่นประมาทบุคคลอื่น และควรใช้ภาษาให้ถูกต้อง สุภาพ สร้างสรรค์
  - การแสดงความคิดเห็นต่างๆ ที่โพสต์โดยบุคลากรขององค์กร โดยที่ไม่ได้รับมอบหมายอย่างเป็นทางการถือเป็นการแสดงความเห็นส่วนบุคคลเท่านั้น ไม่ได้เป็นความคิดเห็นอย่างเป็นทางการขององค์กร
  - กรณีใช้ชื่อบัญชีผู้ใช้งาน (User Account) ที่ระบุถึงต้นสังกัด ผู้ใช้งานพึงใช้ความระมัดระวังในการปฏิบัติตามข้อบังคับจริยธรรม หลักเกณฑ์ และแนวปฏิบัติขององค์กรที่กำกับดูแลตามที่ระบุไว้ในขอบเขตของนโยบาย โดยเฉพาะความถูกต้องและการใช้ภาษาที่เหมาะสม
- หลักการส่งต่อข้อมูล
  - ควรส่งข้อมูลข่าวสารเฉพาะบุคคลที่รู้จัก แสดงตัวตน ตำแหน่ง หน้าที่การงาน สถานะที่ชัดเจน เท่านั้น
  - ละเว้นการส่งข้อมูลที่เป็นข่าวลือ ข่าวไม่ปรากฏที่มา หรือเป็นเพียงการคาดเดา
  - งดเว้นการส่งต่อข้อความเกี่ยวข้องกับองค์กรทุกกรณี ยกเว้น ข้อความนั้นๆ เป็นที่เผยแพร่ต่อสาธารณะแล้ว
  - พึงระลึกเสมอว่า การส่งต่อข้อความที่เป็นเท็จหรือข้อความที่เจ้าของประสงค์กระจายข่าวสร้างความสับสน วุ่นวายในบ้านเมือง เท่ากับตกเป็นเครื่องมือของบุคคลเหล่านั้น
  - ควรงดเว้นการส่งต่อข้อความเรื่องบุคคลเสียชีวิต เว้นเสียแต่ตรวจสอบข้อเท็จจริงแล้ว

  - การส่งต่อข้อความเชิญชวนไปร่วมชุมนุมหรือกระทำกิจกรรมทางสังคมใดๆ ต้องตรวจสอบข้อเท็จจริงให้แน่ชัดเสียก่อน

- การไม่เปิดเผยข้อมูลที่เป็นความลับ
    - การพูดคุยแลกเปลี่ยนกับชุมชนออนไลน์ รวมถึงการโพสต์ข้อความที่เกี่ยวข้องกับงานประจำ เป็นสิ่งที่บุคคลสามารถกระทำได้ ถ้าไม่ขัดต่อหลักจรรยาบรรณองค์กร เว้นแต่ข้อมูลนั้นเป็นข้อมูลที่มีความสำคัญหรือเป็นความลับขององค์กร ซึ่งห้ามเปิดเผยโดยเด็ดขาด เช่น รายละเอียดของโครงการ การลงทุน ข้อมูลสำคัญทางการเงิน งานวิจัย เป็นต้น
    - บุคลากรขององค์กรไม่ควรโพสต์ข้อมูลใดๆ ที่ขัดแย้งกับข้อกำหนดขององค์กร รวมถึงละเว้นการแสดงออกถึงความคิดเห็นที่ก้าวร้าว หมิ่นประมาท ดูถูกเป็นการส่วนตัว ลามกอนาจาร และอื่นๆ ที่ไม่เหมาะสม ตลอดจนหัวข้อที่เป็นความคิดเห็นส่วนตัวที่อาจเป็นการยั่วยุหรือขัดต่อจริยธรรม เช่น การเมือง ศาสนา เชื้อชาติ เป็นต้น
- ไม่ละเมิดกฎหมายลิขสิทธิ์และทรัพย์สินทางปัญญา
    - ไม่ละเมิดกฎหมายลิขสิทธิ์การใช้งานใดๆ ที่เป็นลิขสิทธิ์ของผู้อื่นรวมทั้งขององค์กรเอง
- การฝ่าฝืนและบทลงโทษ
    - องค์กรไม่รับผิดชอบต่อผลของการกระทำที่เกิดจากผู้ใช้งาน และ/หรือบัญชีผู้ใช้งานที่ฝ่าฝืนต่อ นโยบายนี้
    - หากองค์กรตรวจสอบแล้วพบว่าบัญชีผู้ใช้งานใดละเมิดต่อนโยบายนี้ องค์กรขอสงวนสิทธิ์ในการระงับ และ/หรือยกเลิกบัญชีผู้ใช้งาน และ/หรือหยุดให้บริการแก่ผู้ใช้งานนั้น
    - หากการกระทำอันฝ่าฝืนต่อนโยบายนี้เป็นความผิดตามกฎหมาย ให้องค์กรดำเนินคดีตามกฎหมาย โดยลำดับต่อไป

13.2 การปฏิบัติในสื่อสังคมออนไลน์องค์กร

- การจัดทำสื่อสังคมออนไลน์ในระดับองค์กร ควรที่จะคำนึงถึงหลักการพื้นฐานดังต่อไปนี้
    - วัตถุประสงค์ของการจัดทำ
    - แนวทางการใช้งานสื่อสังคมออนไลน์เพื่อช่วยพัฒนาและดำเนินงานขององค์กร
- การตั้งค่าบนสื่อสังคมออนไลน์ขององค์กร
    - การใช้ชื่อหรือตราสัญลักษณ์ขององค์กร เพื่อเปิดบัญชีผู้ใช้งานสื่อสังคมออนไลน์ โดยมีวัตถุประสงค์เพื่อการประชาสัมพันธ์ เผยแพร่ข้อมูลข่าวสาร หรือการสื่อสารภายในองค์กร จะต้องผ่านการรับทราบและเห็นชอบจากผู้บริหารสูงสุดและผู้บริหารฝ่ายไอที รวมทั้งจะต้องมีการตระหนักถึงหลักการพื้นฐาน ดังที่กล่าวมาข้างต้น
- การนำเสนอข่าวโดยการใช้สื่อสังคมออนไลน์ขององค์กร ควรมีหลักในการอ้างอิงถึงองค์กร ดังต่อไปนี้
    - ชื่อองค์กรที่เผยแพร่ข้อมูลข่าวสาร
    - รายละเอียดสัญลักษณ์ หรือชื่อย่อ ที่แสดงถึงองค์กร
    - มาตรการทางเทคนิคที่ยืนยันถึงสถานะและความมีตัวตนขององค์กร (ถ้ามี)
    - ชื่อตัวแทนองค์กรที่นำเสนอข่าวสาร (ถ้ามี)
- การปกป้องข้อมูลที่เป็นความลับขององค์กร
    - ในกรณีที่มีบัญชีผู้ใช้งานขององค์กร ควรมีการตั้งค่าความเป็นส่วนตัว (Privacy) เพื่อป้องกันไม่ให้ บุคคลอื่นโพสต์ข้อความหรือเข้าถึงข้อมูลที่มีความสำคัญหรือเป็นความลับขององค์กร ซึ่งห้ามเปิดเผยโดยเด็ดขาด เช่น รายละเอียดของโครงการการลงทุน ข้อมูลสำคัญทางการเงิน งานวิจัย เป็นต้น โดยมีการกำหนดให้อยู่ในวงจำกัดเท่านั้น และควรให้ความระมัดระวังในการโพสต์ข้อความเฉพาะกลุ่มหรือส่วน

บุคคลที่ไม่ต้องการเผยแพร่ให้สาธารณะชนรับรู้

- การนำเสนอข้อมูลข่าวสารขององค์กรผ่านสื่อสังคมออนไลน์ ควรเป็นไปตามข้อบังคับจริยธรรม หลักเกณฑ์ และแนวปฏิบัติขององค์กรที่กำกับดูแลตามที่ระบุไว้ในขอบเขตของนโยบาย และต้องไม่เป็นการสร้างความเกลียดชังระหว่างคนในชาติ จนอาจนำไปสู่ความขัดแย้งและเสียหายรุนแรงขึ้นในสังคม
- องค์กรต้องให้ความเคารพและยอมรับข้อมูลข่าวสารหรือภาพข่าวที่ผลิตโดยบุคคลอื่นผ่านสื่อสังคม ออนไลน์ การคัดลอก เลียน ข้อความใด ๆ จากสื่อสังคมออนไลน์ พึงได้รับการอนุญาตจากเจ้าของข้อความนั้น ๆ ตามแต่กรณีกรณีจำเป็นเพื่อประโยชน์ในการเผยแพร่ข้อมูลข่าวสาร ต้องอ้างอิงถึงแหล่งที่มาของข้อความและข่าวสารนั้นโดยรับรู้ถึงสิทธิ หรือลิขสิทธิ์ขององค์กรหรือบุคคลผู้เป็นเจ้าของ ข้อมูลดังกล่าว
- หลีกเลี่ยงการสื่อสารข้อความ ภาพนิ่ง ภาพเคลื่อนไหว เสียง และข้อมูลใด ๆ ขององค์กรหรือที่เกี่ยวข้องกับองค์กรที่ก่อให้เกิดความขัดแย้ง หรือโต้แย้งในสังคมขัดต่อหลักกฎหมายทั้งในประเทศและในระดับสากล หรือการเสนอเรื่องราวตลกไร้สาระ เพ้อฝัน ไร้ศีลธรรม เกินความจริง ไม่ให้เกียรติ ดูถูกเหยียดหยาม และลอกเลียนแบบผู้อื่น
- ไม่นำข้อมูลที่เป็นความลับทุกระดับชั้นขององค์กร มาเผยแพร่ผ่านสื่อสังคมออนไลน์ทุกประเภท
- กรณีที่พบข้อมูลความที่มีเสี่ยงต่อชื่อเสียงขององค์กร ต้องดำเนินการแจ้งให้ผู้บริหารสูงสุดทราบทันที

14. ความปลอดภัยในการใช้บริการ Cloud Computing

วัตถุประสงค์

เพื่อเป็นแนวทางในการกำกับดูแลด้านโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ และระบบงานสารสนเทศ เพื่อการจัดเก็บข้อมูล การประมวลผล หรือดำเนินการใดๆ ที่เกี่ยวข้องกับข้อมูลของบริษัท

- การจัดเก็บข้อมูลที่มีระดับชั้นความลับสูงสุดบน Cloud ของผู้ใช้งาน ต้องมีการรักษาความปลอดภัยที่รัดกุมเพียงพอจำกัดสิทธิการเข้าถึงและมีการเข้ารหัสข้อมูล
- การสำรองข้อมูล
- การยกเลิกการใช้งาน

15. การใช้ e-mail

วัตถุประสงค์

เพื่อใช้เป็นเครื่องมือสื่อสารทั้งภายในและนอกองค์กร พนักงานทุกท่านมีสิทธิขอบัญชี e-mail ได้ 1 บัญชี

- E-Mail-Address ของพนักงานคือ [login name]@thespi.com , (login name)@suosdeyfinance.com
- ระบบ E-Mail สามารถส่งและรับ E-Mail กับบุคคลได้ทั้งภายในและภายนอก
- กรุณาใช้ระบบ E-Mail เกี่ยวข้องกับการทำงานเท่านั้น
- เพื่อเป็นการป้องกันไวรัสคอมพิวเตอร์
    - กรุณาอย่าเปิด E-Mail ที่ส่งมาจาก E-Mail Address ที่ท่านไม่รู้จัก
    - กรุณาอย่าเปิดแฟ้มข้อมูลที่แนบมากับ E-Mail โดยเฉพาะ แฟ้มข้อมูลที่สามารถ Run ได้ เช่น .exe .com .bat และ .vbs
- ไม่ควรส่ง e-mail ที่แนบรูปภาพ ถ้าไม่จำเป็น
- พนักงานควรมีการเก็บสำรอง e-mail ของท่านเอง อย่างสม่ำเสมอ
- ถ้าพนักงานท่านใดสงสัยว่าเครื่องคอมพิวเตอร์ของท่านติดไวรัสคอมพิวเตอร์กรุณาแจ้งศูนย์รับแจ้งปัญหาโดยด่วน

16. การปฏิบัติตามข้อกำหนด (Compliance)

วัตถุประสงค์

เพื่อไม่ให้เกิดการละเมิดข้อกำหนดทางกฎหมายระเบียบปฏิบัติข้อกำหนดในสัญญาและข้อกำหนดทางด้านความปลอดภัยอื่นๆ

- พนักงานทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามนโยบายการรักษาความปลอดภัยของระบบสารสนเทศและระเบียบปฏิบัติต่าง ๆ โดยไม่ขัดต่อกฎหมายและข้อกำหนดของบริษัทอย่างเคร่งครัด ทั้งนี้รวมถึงแต่ไม่จำกัดเฉพาะ
    - นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
    - พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ 2550
    - พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ 2560
    - พ.ร.บ.ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ .ศ.2562
    - พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์
    - พ.ร.บ. ลิขสิทธิ์
    - ระเบียบคุ้มครองข้อมูลทั่วไปของสหภาพยุโรป (General Data Protection Regulation หรือ GDPR)
    - พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act หรือ PDPA)
    - NBC (National Bank of Cambodia)
- ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านบนระบบเทคโนโลยีสารสนเทศของบริษัท ถือเป็นทรัพย์สินของบริษัท (ยกเว้นข้อมูลที่เป็นทรัพย์สินของลูกค้า หรือบุคคลภายนอก รวมถึงซอฟต์แวร์ หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตร หรือลิขสิทธิ์ของบุคคลภายนอก) ทั้งนี้บริษัทสามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้ เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า
- บริษัทสามารถตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบเครือข่ายของผู้ใช้งาน ภายในกรอบการควบคุมตามนโยบายการรักษาความปลอดภัยของระบบสารสนเทศ เพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่นโยบายที่บริษัทกำหนดไว้
- บริษัทขอสงวนสิทธิ์ในการเข้าถึง ทบทวน และตรวจสอบอีเมล์ของผู้ใช้งาน โดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า อย่างไรก็ตาม บริษัทจะดำเนินการตรวจสอบดังกล่าวต่อเมื่อมีความจำเป็นและได้รับการอนุมัติจาก คณะกรรมการบริหารงานความปลอดภัยข้อมูลเท่านั้น
- ห้ามมิให้พนักงานใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศของบริษัทกระทำการใด ๆ ที่ขัดแย้งต่อกฎหมายไม่ว่าโดยกรณีใดก็ตาม
- ห้ามมิให้ผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใดๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของบริษัท
- การเจตนาเข้าถึงระบบโดยไม่ได้รับอนุญาต การจงใจใส่ข้อมูลที่ผิดพลาด และการเจตนาเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต ถือว่ามีความผิดทางวินัย
- เพื่อให้มั่นใจได้ว่ามีการปฏิบัติตามนโยบายนี้อย่างเคร่งครัด บริษัทจึงจำเป็นต้องจัดให้มีการสอบทาน ติดตามการปฏิบัติงานของพนักงาน ตลอดจนบุคคลอื่นที่เกี่ยวข้อง โดยทำการตรวจสอบติดตามการปฏิบัติงานภายใน (Internal audit) และการตรวจสอบ Security logs/ Audit trails ที่เกี่ยวข้อง

17. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)

วัตถุประสงค์

บริษัทมีมาตรการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management) เพื่อให้แน่ใจว่าความเสี่ยงที่เกี่ยวข้องกับระบบสารสนเทศและความปลอดภัยไซเบอร์จะถูกประเมิน ควบคุม และจัดการอย่างมีประสิทธิภาพ ซึ่งครอบคลุมแนวปฏิบัติดังต่อไปนี้:

- การประเมินความเสี่ยง (Risk Assessment)
  - ระบุและวิเคราะห์ความเสี่ยงด้าน IT ที่อาจส่งผลกระทบต่อการดำเนินธุรกิจ
  - กำหนดระดับของความเสี่ยง (High, Medium, Low) ตามโอกาสเกิดและผลกระทบที่อาจเกิดขึ้น
  - ทบทวนและอัปเดตรายการความเสี่ยงเป็นประจำ หรือเมื่อมีการเปลี่ยนแปลงทางเทคโนโลยี
- การลดความเสี่ยง (Risk Mitigation)
  - นำมาตรการควบคุม (Controls) มาใช้เพื่อลดความเสี่ยง เช่น Firewall, IDS/IPS, การเข้ารหัสข้อมูล
  - ใช้แนวปฏิบัติที่สอดคล้องกับมาตรฐานสากล เช่น NIST, ISO 27001
  - พัฒนาแนวทางการจัดการช่องโหว่ (Vulnerability Management) และดำเนินการ Patch ระบบอย่างสม่ำเสมอ
- การเฝ้าระวังและติดตามความเสี่ยง (Risk Monitoring & Reporting)
  - จัดให้มีระบบเฝ้าระวังภัยคุกคามทางไซเบอร์แบบเรียลไทม์
  - รายงานความเสี่ยงที่ตรวจพบไปยังผู้มีอำนาจที่เกี่ยวข้อง เช่น คณะกรรมการบริหารความเสี่ยง
  - ใช้ดัชนีชี้วัดความเสี่ยง (Key Risk Indicators - KRIs) เพื่อติดตามแนวโน้มของภัยคุกคาม
- การตอบสนองต่อเหตุการณ์ด้านความเสี่ยง (Risk Response)
  - มีแผนรับมือเหตุการณ์ด้าน IT (Incident Response Plan) และซ้อมแผนอย่างสม่ำเสมอ
  - กำหนดกระบวนการจัดการและรายงานเหตุการณ์ผิดปกติ เช่น การโจมตีไซเบอร์ การรั่วไหลของข้อมูล
  - พัฒนากลยุทธ์ Business Continuity (BCP) และ Disaster Recovery (DRP) เพื่อให้สามารถฟื้นฟูระบบหลังเกิดเหตุได้อย่างรวดเร็ว

18. การจ้างงานภายนอกบริการเทคโนโลยี (Technology Service Outsourcing)

วัตถุประสงค์

เพื่อเพิ่มประสิทธิภาพในการดำเนินงาน ลดต้นทุน และช่วยให้องค์กรสามารถเข้าถึงเทคโนโลยีและความเชี่ยวชาญเฉพาะทางได้ โดยยังคงควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูลและการดำเนินงานให้เป็นไปตามมาตรฐานที่กำหนด ทั้งนี้ การบริหารจัดการ IT Outsourcing ควรเป็นไปตามหลัก "Strategic Alignment, Risk Management, and Performance Optimization" เพื่อให้มั่นใจว่าผู้ให้บริการสามารถตอบสนองต่อเป้าหมายทางธุรกิจขององค์กรได้อย่างมีประสิทธิภาพ

แนวปฏิบัติ

- Vendor Assessment & Due Diligence: ผู้ให้บริการต้องผ่านการประเมินความสามารถและมาตรฐานความปลอดภัยของระบบก่อนการว่าจ้าง โดยพิจารณาทั้งผู้ให้บริการที่องค์กรมีความร่วมมือมาอย่างยาวนาน และผู้ให้บริการรายใหม่ที่มีศักยภาพในการดำเนินงานร่วมกันในระยะยาว
- Contractual Clarity & SLA: ต้องมีสัญญาที่กำหนดขอบเขตการให้บริการ ข้อกำหนดด้านความปลอดภัย และ Service Level Agreement (SLA) ที่ชัดเจน เพื่อให้แน่ใจว่าผู้ให้บริการทุกรายมีมาตรฐานและความรับผิดชอบที่สอดคล้องกับนโยบายขององค์กร

- Access Control & Data Protection: ต้องกำหนดมาตรการควบคุมสิทธิ์การเข้าถึงข้อมูลสำคัญขององค์กรตามหลัก "Least Privilege & Need-to-Know Basis"
- Ongoing Monitoring & Compliance: มีการตรวจสอบและติดตามผลการดำเนินงานของผู้ให้บริการเป็นระยะ รวมถึงให้มั่นใจว่ายังคงปฏิบัติตามกฎระเบียบ เช่น ISO 27001, NIST, PDPA, GDPR
- Incident Management & Response: กำหนดมาตรการป้องกันและรับมือกับเหตุการณ์ด้านความปลอดภัยของข้อมูล เพื่อให้สามารถตอบสนองได้อย่างรวดเร็วและลดผลกระทบที่อาจเกิดขึ้น
- Regulatory & Legal Compliance: ต้องมีการกำกับดูแลให้เป็นไปตามกฎหมายและมาตรฐานที่เกี่ยวข้อง เช่น Cybersecurity Act, Personal Data Protection Laws
- Termination & Exit Strategy: องค์กรสามารถยกเลิกหรือปรับเปลี่ยนข้อตกลงได้หากพบว่ามีความเสี่ยงที่ไม่สามารถยอมรับได้ และต้องมีแผนสำรอง (Contingency Plan) สำหรับการเปลี่ยนผู้ให้บริการอย่างราบรื่น

นโยบายฯ นี้มีผลบังคับตั้งแต่วันที่ 13 พฤษภาคม 2568

....

(ดร.ชุมพล พรประภา)

ประธานกรรมการ