SUPALAI

นโยบายเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัย

Information Technology and Security Policy

รหัสเอกสาร SPL-DT-PC-2601

Version: 00

ประวัติการปรับปรุงเอกสาร

(DOCUMENT VERSION HISTORY)

แก้ไขครั้งที่	วันที่บังคับใช้	รายละเอียดการแก้ไข
00	05 ก.พ. 2569	เอกสารเผยแพร่ฉบับแรก

การอนุมัติเอกสาร

ผู้จัดทำ	ผู้ทบทวน	ผู้อนุมัติ
เฉลิมพล ลีลาชุติพงศ์	*มงคล นิตะโคตร*	*ไตรเตชะ ตั้งมติธรรม*
คุณเฉลิมพล ลีลาชุติพงศ์	คุณมงคล นิตะโคตร	คุณไตรเตชะ ตั้งมติธรรม
ผู้จัดการแผนก Digital Infrastructure & Cybersecurity Office (ประธาน ISMR)	ผู้อำนวยการ ฝ่ายดิจิทัลเทคโนโลยี (รองประธาน ISMS Management)	กรรมการผู้จัดการ (ประธาน ISMS Management)
5 / ก.พ. / 2569	5 / ก.พ. / 2569	5 / ก.พ. / 2569

สารบัญ

หลักการและเหตุผล 6

วัตถุประสงค์ 6

ขอบเขต/การใช้บังคับ 6

คำจำกัดความ 6

หมวดที่ 1 นโยบายเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยในระดับองค์กร (Organization of Information Technology and Security Policy) 12

ส่วนที่ 1.1 การจัดโครงสร้างความมั่นคงปลอดภัยด้านสารสนเทศ (Organization of Information Security) 13

ส่วนที่ 1.2 การบริหารจัดการทรัพย์สิน (Asset Management) 14

ส่วนที่ 1.3 การควบคุมการเข้าถึง (Access Control) 16

ส่วนที่ 1.4 การบริหารจัดการความสัมพันธ์กับหน่วยงานภายนอก (Supplier Relationships) 18

ส่วนที่ 1.5 ความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์ (Information security for use of cloud services) 20

ส่วนที่ 1.6 การจัดการด้านงบประมาณและการควบคุมการใช้จ่ายของการให้บริการ (Budgeting and Accounting for Services Policy) 22

ส่วนที่ 1.7 การจัดการระดับการให้บริการ (Service Level Management Policy) 23

ส่วนที่ 1.8 การให้บริการด้านงานเทคโนโลยีสารสนเทศแก่บุคคลอื่น (IT Insourcing) และการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing) 24

ส่วนที่ 1.9 การบริหารจัดการเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management) 25

ส่วนที่ 1.10 การบริหารจัดการเหตุขัดข้อง และการบริหารจัดการคำร้องขอ (Incident and Service Request Management Policy) 27

ส่วนที่ 1.11 ความมั่นคงปลอดภัยสำหรับการบริหารจัดการความต่อเนื่องในการดำเนินธุรกิจ (Information Security Aspects of Business Continuity Management) 28

ส่วนที่ 1.12 การบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management) 29

ส่วนที่ 1.13 การปฏิบัติตามกฎระเบียบและข้อบังคับ (Compliance) 30

ส่วนที่ 1.14 เอกสารขั้นตอนการปฏิบัติงาน (Documented operating procedures) 33

หมวดที่ 2 นโยบายความปลอดภัยด้านทรัพยากรบุคคล (Human Resource Security) 34

ส่วนที่ 2.1 การรักษาความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resources Security) 34

ส่วนที่ 2.2 การปฏิบัติงานจากระยะไกล (Remote working) 36

ส่วนที่ 2.3 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย (Reporting Information Security Events) 36

หมวดที่ 3 นโยบายความมั่นคงปลอดภัยทางกายภาพ (Physical Controls) 37

ส่วนที่ 3.1 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environment Security) 37

หมวดที่ 4 นโยบายความมั่นคงปลอดภัยทางด้านเทคโนโลยี (Technological Controls) 41

ส่วนที่ 4.1 การรักษาความมั่นคงปลอดภัยสำหรับอุปกรณ์ที่ใช้ปฏิบัติงานหรืออุปกรณ์ของผู้ใช้งาน (User Endpoint Device Security Policy) 41

ส่วนที่ 4.2 การบริหารจัดการสิทธิ์การเข้าถึง (Access Right Management Policy) 43

ส่วนที่ 4.3 การดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ (Operations Security) 46

ส่วนที่ 4.5 การบริหารข้อมูลสารสนเทศเพื่อรายงานผลการให้บริการ (Service Reporting Policy) 49

ส่วนที่ 4.4 ความมั่นคงปลอดภัยข้อมูล (Data Security Policy) 50

ส่วนที่ 4.5 การสื่อสารด้านความมั่นคงปลอดภัยสารสนเทศ (Communications Security) 52

ส่วนที่ 4.6 การเข้ารหัสข้อมูล (Use of Cryptography) 54

ส่วนที่ 4.7 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance) 55

ส่วนที่ 4.8 การจัดการบริหารเปลี่ยนแปลงระบบสารสนเทศ (Change Management Policy) 59

ส่วนที่ 4.9 การป้องกันระบบสารสนเทศระหว่างที่ทดสอบการตรวจประเมิน (Protection of information systems during audit testing 60

หมวดที่ 5 นโยบายการกำกับดูแลการใช้งานปัญญาประดิษฐ์ (Artificial Intelligence) 61

บทลงโทษทางวินัย 61

เอกสารแนบท้าย 1 จรรยาบรรณการทำงานของคู่ค้าศุภาลัย 62

เอกสารแนบท้าย 2 แบบประเมินความเสี่ยง IT และ Cyber Security สำหรับผู้รับจ้างภายนอก 67

หลักการและเหตุผล

ด้วยบริษัท ศุภาลัย จำกัด (มหาชน) และบริษัทย่อย ("บริษัท") ได้จัดให้มีการใช้งานระบบเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวก เพิ่มประสิทธิภาพ และให้ประสิทธิผลต่อการทำงานทั้งระบบ ทั้งนี้เพื่อให้การใช้บริการ และการให้บริการสามารถดำเนินการใช้งานร่วมกันได้อย่างเหมาะสมสอดคล้องกับนโยบายทางธุรกิจ และป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานเครือข่ายระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องทั้งจากผู้ใช้งาน และภัยคุกคามต่างๆ ซึ่งอาจส่งผลกระทบต่อระบบธุรกิจของบริษัทให้ได้รับความเสียหายได้

ดังนั้นเพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัทคงไว้ซึ่งการรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ จึงเห็นสมควรกำหนดนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศเพื่อให้ถือเป็นแนวทางในการปฏิบัติเดียวกันดังต่อไปนี้

วัตถุประสงค์

1. เพื่อกำหนดทิศทาง หลักการ และกรอบของข้อกำหนดในการบริหารจัดการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
2. เพื่อสร้างความรู้ความเข้าใจให้พนักงานปฏิบัติตามนโยบาย มาตรฐาน กรอบการดำเนินงานขั้นตอนการปฏิบัติงาน คำแนะนำ รวมถึงกฎหมายที่เกี่ยวกับระบบคอมพิวเตอร์ได้อย่างถูกต้องและเหมาะสม
3. เพื่อให้พนักงาน และผู้ที่ต้องใช้ หรือเชื่อมต่อระบบคอมพิวเตอร์ของบริษัท ให้สามารถใช้งานระบบคอมพิวเตอร์ของบริษัทได้อย่างถูกต้องและเหมาะสม
4. เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท โดนบุกรุก ขโมย ทำลายแทรกแซงการทำงาน หรือโจรกรรมในรูปแบบต่างๆ ที่อาจจะสร้างความเสียหายต่อการดำเนินธุรกิจของบริษัท
5. เพื่อปกป้องทรัพย์สิน ฐานข้อมูล ข้อมูลของบริษัทฯ จากภัยคุกคามต่าง ๆ ทั้งที่เป็นภัยคุกคามจากภายในและภายนอก เจตนาหรือไม่ตั้งใจ ให้คงไว้ซึ่งการเก็บรักษาความสมบูรณ์ (Integrity) ความลับ (Confidential) และการพร้อมใช้ของข้อมูลสารสนเทศ (Availability) ฐานข้อมูลและการสื่อสารข้อมูลอิเล็กทรอนิกส์ อย่างถูกต้อง ตามข้อกำหนด กฎระเบียบและ กฎหมายที่เกี่ยวข้อง

ขอบเขต/การใช้บังคับ

นโยบายฉบับนี้ครอบคลุมถึงพนักงานทุกระดับของบริษัทฯ รวมถึงบุคคลภายนอกที่ได้รับอนุญาตจากบริษัทฯ ให้เข้าถึง หรือใช้ระบบคอมพิวเตอร์ เครือข่ายสารสนเทศ และข้อมูลของบริษัทฯ ทั้งนี้ การปฏิบัติตามนโยบายดังกล่าวถือเป็นข้อบังคับที่ทุกฝ่ายต้องยึดถืออย่างเคร่งครัด

คำจำกัดความ

No.	คำศัพท์	คำจำกัดความ
1.	บริษัท	บริษัท ศุภาลัย จำกัด (มหาชน) และบริษัทย่อย
2.	บริษัทย่อย	บริษัท ศุภาลัย จำกัด (มหาชน) มีอำนาจควบคุมได้
3.	คณะทำงานฯ /คณะทำงาน ISMS / ISMS Working Committee	คณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ
4.	ฝ่ายดิจิทัลเทคโนโลยี (Digital Technology : DT)	หน่วยงานที่รับผิดชอบในการดำเนินงานด้านบริหารจัดการเทคโนโลยีสารสนเทศขององค์กร

No.	คำศัพท์	คำจำกัดความ
5.	ผู้บริหารระดับฝ่าย	ผู้บริหารสูงสุดของแต่ละฝ่ายงาน
6.	ผู้มีอำนาจ	ผู้บังคับบัญชาระดับผู้อำนวยการฝ่ายขึ้นไป หรือผู้ที่ได้รับมอบหมายให้มีหน้าที่ตัดสินใจ
7.	ผู้ดูแลระบบ (Administrator)	เจ้าหน้าที่ฝ่ายดิจิทัลเทคโนโลยีที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบ หรือเครือข่ายคอมพิวเตอร์ รวมไปถึงการแก้ไขปัญหาการใช้งานระบบสารสนเทศในด้านต่างๆ ซึ่งสามารถเข้าถึงโปรแกรม หรือเครือข่ายคอมพิวเตอร์เพื่อการจัดการต่างๆ ได้
8.	บุคลากร หรือ ผู้ใช้งาน	บุคลากรของบริษัท ศุภาลัย จำกัด (มหาชน) และบริษัทย่อย
9.	บุคคลภายนอก	บุคคล หรือพนักงานของหน่วยงานภายนอกที่มาติดต่อสื่อสาร และมีการเข้าถึงทรัพย์สินสารสนเทศขององค์กร
10.	ผู้ให้บริการภายนอก/หน่วยงานภายนอก (Third party)	ผู้ค้า หุ้นส่วนการค้า ผู้ให้บริการ/จำหน่ายระบบ (Vendor) พนักงานสัญญาจ้าง (Outsource) และบุคคล หรือนิติบุคคลอื่นใดทั้งในประเทศและต่างประเทศที่ให้บริการด้านเทคโนโลยีสารสนเทศ ซึ่งเข้าทำสัญญาหรือทำข้อตกลงในการให้บริการให้กับองค์กร รวมถึงหน่วยงานผู้รับจ้างช่วงที่ผู้ให้บริการภายนอกเป็น
11.	ผู้จัดจ้าง โดยได้รับอนุญาตให้มีสิทธิ์เข้าถึงสถานที่หรือทรัพย์สินสารสนเทศขององค์กร และใช้งานระบบสารสนเทศขององค์กรตามอำนาจหน้าที่ที่รับผิดชอบ	ผู้ค้า หุ้นส่วนการค้า ผู้ให้บริการ/จำหน่ายระบบ (Vendor) พนักงานสัญญาจ้าง (Outsource) และบุคคล หรือนิติบุคคลอื่นใดทั้งในประเทศและต่างประเทศที่ให้บริการด้านเทคโนโลยีสารสนเทศ ซึ่งเข้าทำสัญญาหรือทำข้อตกลงในการให้บริการให้กับองค์กร รวมถึงหน่วยงานผู้รับจ้างช่วงที่ผู้ให้บริการภายนอกเป็นผู้จัดจ้าง โดยได้รับอนุญาตให้มีสิทธิ์เข้าถึงสถานที่หรือทรัพย์สินสารสนเทศขององค์กร และใช้งานระบบสารสนเทศขององค์กรตามอำนาจหน้าที่ที่รับผิดชอบ
12.	ผู้ใช้งาน (User)	บุคลากร บุคคลภายนอก และหน่วยงานภายนอก ที่ใช้งานระบบงานคอมพิวเตอร์ขององค์กร
13.	เจ้าของโครงการ	หน่วยงานภายในบริษัท ศุภาลัย จำกัด (มหาชน) และบริษัทย่อย ที่เป็นผู้รับผิดชอบในการดำเนินงานโครงการที่มีการจัดจ้างผู้ให้บริการภายนอก/หน่วยงานภายนอกเข้ามาปฏิบัติงานให้กับองค์กร
14.	เจ้าของทรัพย์สิน (Asset Owner)/ เจ้าของข้อมูล (Data Owner)	บุคคล ส่วนงาน หรือฝ่ายงานผู้เป็นเจ้าของข้อมูล หรือเป็นผู้ที่ได้รับความเสียหายสูงสุดเมื่อข้อมูลนั้นเสียหายหรือถูกเปิดเผย
15.	ข้อมูล (Information)	ข้อความ ข่าวสาร เอกสาร เสียง หรือสิ่งอื่นใดที่สามารถสื่อความหมายได้ที่อยู่ใน รูปของตัวเลข ภาษา ภาพ สัญลักษณ์ต่างๆ ที่ยังไม่ผ่านการประมวลผล ทั้งที่อยู่ในรูปอิเล็กทรอนิกส์หรือที่อยู่ ในรูปสื่อสิ่งพิมพ์ และให้ความหมายรวมถึงข้อมูลคอมพิวเตอร์ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย
16.	อิเล็กทรอนิกส์ข้อมูล	ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

No.	คำศัพท์	คำจำกัดความ
17.	ข้อมูลคอมพิวเตอร์	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย
18.	บัญชีผู้ใช้ (User Name หรือ Account)	กลุ่มของข้อมูลที่ใช้ในการอ้างถึงเพื่อระบุตัวตน สิทธิ์การเข้าถึง และข้อจำกัดต่างๆในการเข้าถึงระบบสารสนเทศ
19.	รหัสผ่าน (Password)	กลุ่มอักขระที่ใช้ในการพิสูจน์ตัวตน ใช้เพื่อควบคุมการเข้าถึงระบบสารสนเทศหรือข้อมูลสารสนเทศ
20.	สิทธิ์พิเศษ (Privilege)	สิทธิระดับสูง สิทธิที่สามารถใช้งาน โดยได้รับสิทธิ์ที่มากกว่าสิทธิ์ของผู้ดูแลระบบหรือผู้ใช้งานทั่วไปในระบบ เช่น Root หรือ Administrator
21.	ระบบสารสนเทศ (Information system)	ระบบคอมพิวเตอร์ ระบบเก็บข้อมูล ระบบจดหมายอิเล็กทรอนิกส์ (E-mail) ระบบสื่อสารข้อมูลทุกประเภท อุปกรณ์สื่อสาร เครื่องพิมพ์ เครื่องสแกนหรืออุปกรณ์ใดๆ ที่ เกี่ยวข้องที่เป็นกรรมสิทธิ์ขององค์กร และ/หรือ ที่องค์กรได้รับอนุญาตให้ใช้ได้ตามกฎหมาย
22.	ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)	การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)
23.	เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)	กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
24.	เหตุขัดข้อง (Incident)	เหตุขัดข้องที่ส่งผลทำให้ระบบสารสนเทศไม่สามารถให้บริการได้ตามที่กำหนดไว้หรือคุณภาพในการให้บริการลดลง เช่น ระบบอีเมลไม่สามารถใช้งานได้ เครื่องแม่ข่ายขัดข้อง หรือ ระบบงานประมวลข้าผิดปกติ เป็นต้น
25.	การสำรองข้อมูล (Data Backup)	การทำสำเนาข้อมูลทั้งหมดในระบบที่ต้องการ เพื่อเป็นการสำรองข้อมูลที่อาจมีการแก้ไข เปลี่ยนแปลง หรือสูญหายให้สามารถนำกลับมาใช้งานได้
26.	แหล่งข้อมูล (Source of Data and Information)	ที่เก็บข้อมูล หรือสารสนเทศทั้งที่อยู่ในรูปแบบต่างๆ กัน เช่น ข้อมูลแหล่งข้อมูลเฉพาะและแหล่งข้อมูลส่วนกลาง เป็นต้น
27.	สถานการด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)	สถานการด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
28.	การเข้ารหัส (Encryption)	การเปลี่ยนแปลงรูปแบบของข้อมูลให้อยู่ในรูปแบบที่มีความมั่นคงปลอดภัย โดยใช้กุญแจในการเข้ารหัสลับ เพื่อที่ผู้เข้าถึงข้อมูลจะไม่สามารถทราบเนื้อหาที่แท้จริงของข้อมูลได้ ถ้าไม่มีการถอดรหัสลับจากกุญแจที่ใช้ในการถอดรหัสที่ถูกต้อง ทั้งนี้ขึ้นอยู่กับเทคนิคการเข้ารหัสลับข้อมูลที่ใช้ โดยลักษณะของการเข้ารหัสลับมีด้วยกัน 2 ประเภท คือ

No.	คำศัพท์	คำจำกัดความ
		• การเข้ารหัสแบบสมมาตร (Symmetric Key Encryption) เป็นการเข้ารหัสที่ใช้กุญแจรหัสเดียวในการเข้ารหัสและถอดรหัส เรียกว่า กุญแจลับ (Secret Key) • การเข้ารหัสแบบอสมมาตร(Asymmetric Key Encryption or Public Key Cryptography) เป็นการเข้ารหัสในลักษณะที่มีกุญแจคู่ เรียกว่ากุญแจ ส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) โดยในนโยบายฉบับนี้เรียกว่ากุญแจคู่
29.	กุญแจ (Key)	กุญแจที่ใช้ในกระบวนการเข้ารหัสลับ หรือถอดรหัสลับ ขึ้นอยู่กับการใช้งานเทคนิคการเข้ารหัสลับข้อมูล โดยแยกเป็น 2 ประเภท คือ • กุญแจลับ (Secret Key) ซึ่งใช้ในการเข้ารหัสลับแบบสมมาตร (Symmetric Key Encryption) ตัวอย่างของอัลกอริทึมสำหรับการเข้ารหัสแบบสมมาตร เช่น 3DES, RC5, RC6, AES เป็นต้น • กุญแจคู่ ซึ่งใช้ในการเข้ารหัสแบบอสมมาตร (Asymmetric Key Encryption or Public Key Cryptography) ประกอบไปด้วย กุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) ตัวอย่างของอัลกอริทึมสำหรับการเข้ารหัสแบบอสมมาตร เช่น RSA (Rivest-Shamir-Adleman), Diffie-Hellman Key Exchange Protocol, Elliptic Curve Cryptography (ECC) เป็นต้น
30.	ช่องโหว่ (Vulnerability)	สภาพหรือสภาวะที่เป็นข้อบกพร่องหรือไม่สมบูรณ์ของทรัพย์สินสารสนเทศ ซึ่งอาจเกิดจากความบกพร่องในการผลิต หรือการออกแบบ หรือการบริหารจัดการทำให้เกิดจุดอ่อน โดยมีความเสี่ยงที่จะเกิดภัยคุกคามจากช่องโหว่ที่เกิดขึ้น เช่น ช่องโหว่ของโปรแกรมที่ทำให้บุคคลภายนอกสามารถเข้าใช้โปรแกรมได้โดยไม่ต้องผ่านการพิสูจน์ตัวตน
31.	การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัย (Security Awareness)	การให้ความรู้ความเข้าใจทางด้านความมั่นคงปลอดภัยของสารสนเทศ เพื่อสร้างความตระหนักถึงภัยคุกคามและปัญหาทางด้านความมั่นคงปลอดภัยสารสนเทศแก่บุคลากร
32.	ทรัพย์สินสารสนเทศ (Information Asset)	ข้อมูล ข่าวสาร หรือองค์ประกอบด้านเทคโนโลยีที่มีมูลค่าและมีความสำคัญต่อการดำเนินงานขององค์กร ทั้งในรูปแบบอิเล็กทรอนิกส์และเอกสาร รวมถึงระบบคอมพิวเตอร์และเครือข่าย ซึ่งจำเป็นต้องได้รับการบริหารจัดการและรักษาความมั่นคงปลอดภัยเพื่อป้องกันความเสียหายจากการถูกทำลายหรือรั่วไหล เช่น • อุปกรณ์เทคโนโลยีสารสนเทศ และอุปกรณ์อื่นใดที่ใช้งานร่วมกับอุปกรณ์เทคโนโลยีสารสนเทศที่เกี่ยวข้องทุกประเภท • ชุดคำสั่ง โปรแกรมระบบงานสารสนเทศ และโปรแกรมอื่นใดที่ใช้งานร่วมกับโปรแกรมระบบงานสารสนเทศ • ข้อมูล ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ และ/หรือ ทรัพย์สินทางปัญญาใดๆ
33.	พื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Secure Area)	คือ บริเวณที่ใช้เก็บรักษาอุปกรณ์สารสนเทศที่ใช้ในงานระบบสารสนเทศ แบ่งได้เป็น 3 ประเภท คือ

No.	คำศัพท์	คำจำกัดความ
		• พื้นที่ห้องจัดเก็บอุปกรณ์สารสนเทศ • พื้นที่ห้องปฏิบัติการคอมพิวเตอร์ • พื้นที่ห้องศูนย์ข้อมูล (Data Center)
34.	บันทึกเหตุการณ์ (Logs)	Logs บันทึกเหตุการณ์การใช้งานของระบบสารสนเทศ การเข้าใช้งานระบบงานหรือระบบสารสนเทศ การประมวลผลกิจกรรมของระบบสารสนเทศ และเหตุการณ์ทางด้านความมั่นคงปลอดภัยเพื่อตรวจสอบถึงประสิทธิภาพความปลอดภัย และความผิดปกติที่เกิดจากการประมวลผลกิจกรรมต่างๆ ของระบบสารสนเทศ
35.	การเฝ้าระวัง (Monitoring)	การเฝ้าระวังทางด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อตรวจสอบความผิดปกติจากการประมวลผลกิจกรรมต่างๆ ของระบบสารสนเทศ จากบันทึกเหตุการณ์ (Logs) เช่น การเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต การใช้งานสารสนเทศผิดวัตถุประสงค์ และปัญหาที่เกิดจากระบบงาน
36.	ความเสี่ยง (Risk)	โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ หรือการกระทำใดๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน ซึ่งอาจเกิดขึ้นในอนาคตและมีผลกระทบหรือทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายของการให้บริการ
37.	โปรแกรมที่ไม่พึงประสงค์ (Malicious Code or Malware)	โปรแกรมหรือ Code ที่เป็นอันตรายต่อประสิทธิภาพ และความปลอดภัยของระบบสารสนเทศไม่ทางใดก็ทางหนึ่ง เช่น ไวรัส (Virus) เวิร์ม (Worm) หรือโทรจัน (Trojan) เป็นต้น
38.	แผนการบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Plan)	การสร้างความต่อเนื่องทางธุรกิจ เพื่อป้องกันการติดขัดหรือการหยุดชะงักของระบบงานธุรกรรมที่สำคัญซึ่งอาจมีสาเหตุมาจากภัยทางด้านสิ่งแวดล้อม เหตุการณ์ทางด้านความมั่นคงปลอดภัยหรือภัยคุกคามอื่นๆ
39.	แผนรองรับกรณีเกิดเหตุฉุกเฉิน (Disaster Recovery Plan: DRP)	การเตรียมความพร้อมรองรับเหตุฉุกเฉินและแผนการปฏิบัติงานเมื่อเกิดเหตุฉุกเฉิน เช่น การย้ายสถานที่ปฏิบัติงาน ไปจนถึงการใช้งานระบบสารสนเทศสำรอง
40.	แผนสำหรับย้อนกลับสู่สภาวะเดิม (Fallback Plan)	แผนการดำเนินงานเพื่อใช้ในการกลับสู่สถานการณ์ดำเนินงานครั้งล่าสุด เพื่อใช้ในกรณีที่การแก้ไขเหตุฉุกเฉินไม่เป็นผลสำเร็จ
41.	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective: RPO)	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลสูญหายจากระบบได้ และเพื่อเป็นข้อมูลในการออกแบบวิธีการสำรองข้อมูลเพื่อให้ข้อมูลไม่สูญหายเกินกว่าที่กำหนดไว
42.	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objective: RTO)	ระยะเวลาเป้าหมายที่ใช้ในการดำเนินการเพื่อส่งมอบผลิตภัณฑ์ บริการ และกิจกรรมหรือกระบวนการกลับสู่สภาวะปกติหลังจากเกิดสถานการณ์ไม่พึงประสงค์ที่มีความเสียหายระดับรุนแรง
43.	ช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด (Maximum Tolerable Period of Disruption: MTPD)	ช่วงเวลาสูงสุดที่การดำเนินงานหยุดชะงัก หากเกินกำหนดช่วงเวลานี้แล้ว จะไม่สามารถทำให้การดำเนินงานฟื้นคืนสู่สภาพปกติได้
44.	ข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA)	ข้อตกลงร่วมกันระหว่างผู้ให้บริการและผู้รับบริการที่อธิบายถึงรายละเอียดการบริการ ระดับการให้บริการที่จะถูกวัดและประเมินผล เป้าหมายของระดับการ

No.	คำศัพท์	คำจำกัดความ
		ให้บริการ รวมไปถึงระบุหน้าที่ความรับผิดชอบที่ชัดเจนของทั้งผู้ให้บริการและผู้รับบริการ
45.	ข้อตกลงการให้บริการระดับปฏิบัติงาน (Operational Level Agreement: OLA)	ข้อตกลงในการให้บริการการสำหรับปฏิบัติงานร่วมกันระหว่างหน่วยงานภายในเพื่อสนับสนุนให้การบริการของผู้รับบริการเป็นไปตามข้อตกลงระดับการให้บริการ (SLA)
46.	สัญญาการให้บริการ (Underpinning Contracts: UC)	ข้อตกลงร่วมกันระหว่างผู้ให้บริการและผู้ให้บริการ/ผู้จำหน่ายระบบ (Vendor) เพื่อให้บริการผู้รับบริการได้ตามข้อตกลงการให้บริการ (SLA)
47.	พื้นที่ในการพัฒนาระบบงาน (Development Area)	ระบบสารสนเทศที่ใช้ในการพัฒนาระบบงาน โดยเป็นการจำลองทรัพยากร และสภาพแวดล้อมของระบบให้บริการจริง เพื่อใช้ปรับปรุงและพัฒนาระบบงาน
48.	ระบบงานทดสอบ (User Acceptance Test)	เป็นกระบวนการสุดท้ายของการทดสอบระบบและเกิดขึ้นก่อนนำขึ้นสู่ระบบงานจริง โดยทดสอบจากกลุ่มผู้ใช้งาน เพื่อตรวจสอบให้แน่ใจว่า ระบบใช้งานได้จริง เป็นไปตามความต้องการ และได้รับประสบการณ์การใช้งานที่ดี
49.	ระบบสารสนเทศสำรอง (Disaster Recovery Center: DR)	ระบบงาน ข้อมูล และระบบเครือข่ายสำรองนอกเหนือจากระบบสารสนเทศหลักเพื่อให้สามารถทำธุรกรรมหลักได้อย่างต่อเนื่อง และลดผลกระทบเมื่อเกิดเหตุการณ์ฉุกเฉิน
50.	ระบบให้บริการจริง(Production Area)	ระบบสารสนเทศที่ให้บริการจริงแก่ผู้ใช้งานซึ่งต้องมีการรักษาความมั่นคงปลอดภัยและการควบคุมการเข้าถึงจากการพัฒนาระบบและการทดสอบระบบอย่างเคร่งครัด
51.	อุปกรณ์สื่อสารประเภทพกพา (Mobile Device)	เครื่องคอมพิวเตอร์พกพา (Laptop Computer) สมาร์ทโฟน (Smartphone) แท็บเลตคอมพิวเตอร์ (Tablet Computer) ที่องค์กรอนุญาตให้เชื่อมต่อและใช้งานระบบสารสนเทศขององค์กรได้
52.	สื่อบันทึกข้อมูล (Media)	อุปกรณ์อิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น Hard Drive หรือFlash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard Drive เป็นต้น
53.	ปัญญาประดิษฐ์ (Artificial Intelligence :AI)	เทคโนโลยีที่ถูกพัฒนาขึ้นเพื่อให้คอมพิวเตอร์มีคุณสมบัติหรือพฤติกรรมใกล้เคียงมนุษย์ เช่น การเรียนรู้ การรับรู้และตอบสนองต่อสภาพแวดล้อม การให้เหตุผล และการแก้ไขปัญหา เป็นต้น ตามวัตถุประสงค์ที่มนุษย์กำหนด
54	ศูนย์ข้อมูล (Data Center : DC)	สถานที่ทางกายภาพที่จัดตั้งขึ้นเพื่อเป็นศูนย์กลางการจัดเก็บ ประมวลผล และบริหารจัดการข้อมูลดิจิทัลขนาดมหาศาลขององค์กร ภายในประกอบด้วย เซิร์ฟเวอร์ (Server), ระบบจัดเก็บข้อมูล (Storage), และอุปกรณ์เครือข่าย โดยมีระบบสนับสนุนความปลอดภัยสูง เช่น ระบบระบายความร้อน, ไฟฟ้าสำรอง (UPS), และการป้องกันการบุกรุก ทำงานต่อเนื่องตลอด 24 ชั่วโมง

หมวดที่ 1 นโยบายเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยในระดับองค์กร (Organization of Information Technology and Security Policy)

บริษัทฯ จัดทำนโยบายเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยฉบับนี้ เพื่อกำหนดทิศทาง หลักการ และกรอบของข้อกำหนดในการป้องกันทรัพย์สินที่เกี่ยวข้องกับสารสนเทศให้ปลอดภัยจากภัยคุกคามที่อาจก่อให้เกิดความเสียหายต่อการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ (Availability) ของข้อมูลและระบบงานสารสนเทศ เพื่อผลักดันให้มีการควบคุมภายในด้านสารสนเทศที่รัดกุมตามแนวความเสี่ยง (Risk Based Approach) ที่สอดคล้องกับมาตรฐานสากล และเพื่อสนับสนุนผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และได้รับทราบถึงหน้าที่ความรับผิดชอบและแนวทางปฏิบัติในการควบคุมความเสี่ยงต่างๆ โดยองค์กรต้องจัดให้มีนโยบายและมาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีแนวทางปฏิบัติดังนี้

1. เป้าหมายด้านความมั่นคงปลอดภัยสารสนเทศ

   บริษัทฯ ได้มีการกำหนดเป้าหมายสอดคล้องตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้ เพื่อเป็นกรอบในการกำหนดตัวชี้วัด ดังนี้

   1) เพื่อสร้างความมั่นใจว่า องค์กรได้มีมาตรการจัดการความมั่นคงปลอดภัยสารสนเทศของระบบ สอดคล้องตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลและเป็นมาตรฐานสากล
   2) เพื่อสร้างความตระหนักรู้ในเรื่องความมั่นคงปลอดภัยสารสนเทศ และเสริมสร้างความสามารถของบุคลากรภายใต้ขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
   3) เพื่อดำเนินการเชิงแก้ไขสำหรับการไม่ปฏิบัติตามนโยบายความมั่นคงปลอดภัยที่ตรวจพบ
   4) เพื่อให้ระบบภายใต้ขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและระบบบริหารจัดการข้อมูลส่วนบุคคล มีการรักษาความลับ ความถูกต้อง ความพร้อมใช้งาน และสามารถให้บริการได้อย่างต่อเนื่อง
   5) เพื่อวัดจำนวนเหตุการณ์ที่มีผลกระทบต่อระบบบริหารจัดการความมั่นคงปลอดภัยการให้บริการเทคโนโลยีสารสนเทศ

2. ทิศทางการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ (Management Directions for Information Security)

   1) นโยบายสำหรับความมั่นคงปลอดภัยด้านสารสนเทศ (Policy for Information Security)
      - องค์กรต้องจัดให้มีนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร โดยได้รับการอนุมัติจากประธานกรรมการบริษัท หรือผู้บริหารระดับสูงที่ประธานกรรมการบริษัทมอบหมายให้เป็นผู้อนุมัติ
      - องค์กรต้องเผยแพร่นโยบายดังกล่าวให้ผู้ใช้งานและหน่วยงานภายนอกที่เกี่ยวข้องได้รับทราบและถือปฏิบัติเป็นไปตามที่นโยบายกำหนด โดยการเผยแพร่ต้องดำเนินการในลักษณะที่ผู้ใช้งานเข้าถึงได้ง่าย
   2) การเผยแพร่นโยบาย
      - ฝ่ายดิจิทัลเทคโนโลยีหน้าที่รับผิดชอบในการประกาศและเผยแพร่นโยบายไปยังผู้ใช้งานระบบสารสนเทศขององค์กร เพื่อช่วยให้เกิดความเข้าใจในบทบาทของตนเองในการใช้งานเทคโนโลยีสารสนเทศและปกป้องทรัพย์สินขององค์กร

3) การทบทวนนโยบายเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยของระบบสารสนเทศ (Review of the Policies for Information Technology and Security)
   - นโยบายเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยฉบับนี้ต้องได้รับการทบทวนปรับปรุงให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญของสภาพแวดล้อมต่างๆ เช่น สภาพธุรกิจ กฎเกณฑ์ กฎหมายและเทคโนโลยี เป็นต้น โดยถือเป็นหน้าที่ของฝ่ายดิจิทัลเทคโนโลยีในการทบทวนและปรับปรุง โดยมีผู้บริหารฝ่ายดิจิทัลเทคโนโลยีเป็นผู้ควบคุมดูแลให้เกิดการทบทวนและปรับปรุงตามที่ได้กำหนดไว้
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องดำเนินการตรวจสอบ และทบทวนนโยบายเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยตามเงื่อนไขที่กำหนดไว้

ส่วนที่ 1.1 การจัดโครงสร้างความมั่นคงปลอดภัยด้านสารสนเทศ (Organization of Information Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม กำกับ และติดตามการปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับส่วนงานต่างๆ ภายในองค์กร และเพื่อเป็นแนวทางควบคุมการใช้งานอุปกรณ์สื่อสารประเภทพกพา ให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

1.1.1. การจัดโครงสร้างภายในองค์กร (Internal Organization)

1) การกำหนดบทบาทและหน้าที่ความรับผิดชอบความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Roles and Responsibilities) ผู้บริหารระดับฝ่ายต้องกำหนดรายละเอียดหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคง ปลอดภัยระบบสารสนเทศสำหรับบุคลากรในหน่วยงานอย่างเป็นลายลักษณ์อักษร และให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่กำหนดไว้การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of Duties) ผู้บริหารระดับฝ่ายต้องกำหนดให้มีการแบ่งแยกหน้าที่ความรับผิดชอบ ในการปฏิบัติงานด้านต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศออกจากกันอย่างชัดเจนเพื่อให้มีการสอบทานระหว่างนได้
2) การประสานงานกับหน่วยงานภายนอกที่เกี่ยวข้องด้านความมั่นคงปลอดภัย (Contact with authorities) ฝ่ายดิจิทัลเทคโนโลยี ต้องรวบรวมข้อมูลติดต่อของผู้เกี่ยวข้องกับการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศทั้งหมด รวมถึงข้อมูลการติดต่อของผู้เชี่ยวชาญที่เกี่ยวข้อง และดำเนินการทบทวนอย่างสม่ำเสมอ และต้องจัดให้มีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่นๆ เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) และหน่วยงานกำกับดูแล เป็นต้น เพื่อใช้สำหรับติดต่อประสานงานทางด้านความมั่นคงปลอดภัยสารสนเทศ ในกรณีที่มีความจำเป็นหรือเกิดเหตุการณ์ละเมิดด้านความมั่นคงปลอดภัยสารสนเทศ

3) การประสานงานกับกลุ่มผู้เชี่ยวชาญที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Contact with special interest groups) ให้ฝ่ายดิจิทัลเทคโนโลยี มีการเข้าร่วมกลุ่มและรวบรวมรายชื่อกลุ่มพิเศษที่มีความสนใจในเรื่องเดียวกัน กลุ่มที่มีผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ และสมาคมที่มีความเป็นมืออาชีพ เช่น สมาคมธนาคารไทย (TB-Cert) ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (Thai CERT) เป็นต้น เพื่อเข้าถึง คำแนะนำ ความรู้ การแบ่งปัน และแลกเปลี่ยนสารสนเทศเกี่ยวกับเทคโนโลยี ผลิตภัณฑ์ บริการ ภัยคุกคามหรือช่องโหว่ใหม่ๆ หรือข่าวกรองด้านภัยคุกคามที่เกี่ยวข้องกับระบบสารสนเทศที่สำคัญ (Threat Intelligence) เพื่อนำมาปรับปรุงแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ และต้องมีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับการติดต่อกลุ่มต่างๆ และดำเนินการทบทวนอย่างสม่ำเสมอ
4) การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศในการบริหารจัดการโครงการ (Information Security in Project Management) ผู้บริหารระดับฝ่ายจะต้องกำหนดให้มีการควบคุมความเสี่ยง การติดตามการดำเนินงานโครงการ รวมถึงการประเมินภาพรวมในการดำเนินงานโครงการ ทั้งโครงการที่เป็นโครงการภายในและโครงการที่จัดซื้อจัดจ้างจากหน่วยงานภายนอก และต้องปฏิบัติตามข้อกำหนดด้านความปลอดภัย รวมถึงควรมีการระบุความรับผิดชอบและอำนาจหน้าที่ในการรักษาความปลอดภัยข้อมูลที่เกี่ยวข้องกับโครงการ โดยครอบคลุมประเด็นสำคัญ ดังนี้
    - การรวมความมั่นคงปลอดภัยเข้ากับโครงการ ตั้งแต่เริ่มต้นโครงการ ต้องพิจารณาความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลและวางแผนมาตรการป้องกัน
    - การฝึกอบรมและความตระหนักรู้ ผู้ที่เกี่ยวข้องกับโครงการต้องได้รับการฝึกอบรมและตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของข้อมูล
    - การควบคุมการเข้าถึงข้อมูล ต้องมีการควบคุมการเข้าถึงข้อมูลที่ใช้ในโครงการอย่างเหมาะสม เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต
    - การตรวจสอบและการประเมินความเสี่ยง การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูลต้องถูกดำเนินการอย่างต่อเนื่องในระหว่างโครงการ
    - การจัดการกับเหตุการณ์ด้านความมั่นคงปลอดภัย ควรมีแผนรับมือและดำเนินการทันทีเมื่อพบเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้นในระหว่างโครงการ

ส่วนที่ 1.2 การบริหารจัดการทรัพย์สิน (Asset Management)

วัตถุประสงค์

เพื่อให้สินทรัพย์และระบบสารสนเทศขององค์กรได้รับการปกป้องในระดับที่เหมาะสม เพื่อลดความเสี่ยงต่อการถูกเปิดเผยข้อมูลขององค์กรโดยไม่ได้รับอนุญาต รวมถึงป้องกันการนำทรัพย์สินสารสนเทศไปใช้โดยผิดวัตถุประสงค์ และเกิดความเสียหายกับทรัพย์สินสารสนเทศขององค์กร

1.2.1. หน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for assets)

1) การจัดทำบัญชีทรัพย์สิน (Inventory of Assets) ฝ่ายดิจิทัลเทคโนโลยี ต้องควบคุมให้หน่วยงานภายในฝ่ายจัดทำบัญชีทรัพย์สินสารสนเทศเพื่อบริหารจัดการและควบคุมทรัพย์สินสารสนเทศอย่างเหมาะสมและให้มีการปรับปรุงบัญชีทรัพย์สินให้เป็นปัจจุบันอยู่เสมอ
2) การระบุผู้ถือครองทรัพย์สิน (Ownership of Assets) ผู้บังคับบัญชาฝ่ายดิจิทัลเทคโนโลยี(ระดับ 6.2 ขึ้นไป) ต้องกำหนดให้มีการระบุผู้ถือครองทรัพย์สิน ผู้มีหน้าที่ดูแลควบคุมการใช้งานทรัพย์สินสารสนเทศ และผู้มีหน้าที่รับผิดชอบทรัพย์สินสารสนเทศอย่างเหมาะสม
3) การใช้ทรัพย์สินสารสนเทศ (Acceptable Use of Assets) ผู้จัดการฝ่ายดิจิทัลเทคโนโลยีขึ้นไป ต้องจัดทำข้อกำหนดในการใช้ทรัพย์สิน เพื่อการบริหารจัดการอุปกรณ์คอมพิวเตอร์ให้เหมาะสมก่อให้เกิดประสิทธิภาพสูงสุด รวมทั้งมีความปลอดภัยจากความเสียหายที่อาจเกิดขึ้นได้ โดยต้องสื่อสารให้บุคลากรขององค์กรรับทราบและปฏิบัติตาม
4) การคืนทรัพย์สิน (Return of Assets) ฝ่ายบริหารทรัพยากรบุคคล หัวหน้างาน หรือผู้บังคับบัญชา ต้องกำกับและติดตามให้บุคลากรในหน่วยงานหรือหน่วยงานภายนอกที่เข้ามาให้บริการดำเนินการคืนทรัพย์สิน อาทิ เครื่องคอมพิวเตอร์พกพา เอกสาร กุญแจ บัตรพนักงาน ที่เป็นทรัพย์สินขององค์กรให้กับหน่วยงานที่เกี่ยวข้อง

1.2.2. การจัดลำดับชั้นความลับของสารสนเทศ (Information Classification)

1) การจัดลำดับชั้นความลับของสารสนเทศ (Classification of Information)
    - องค์กรต้องกำหนดให้มีการจัดหมวดหมู่ของทรัพย์สินสารสนเทศ และจัดลำดับชั้นความลับของสารสนเทศ โดยต้องกำหนดชั้นความลับโดยให้นำกฎหมายและข้อกำหนดทีเกี่ยวข้องกับองค์กรมาร่วมพิจารณาการกำหนดชั้นความลับที่เหมาะสม
    - หน่วยงานภายในองค์กร ต้องจัดหมวดหมู่ของข้อมูลและทรัพย์สินสารสนเทศที่ใช้ในการดำเนินงานขององค์กร และกำหนดลำดับชั้นความลับของข้อมูลและทรัพย์สินสารสนเทศ
    - หน่วยงานภายในองค์กร ต้องดำเนินการบริหารจัดการลำดับชั้นความลับข้อมูลตามแนวทางการเนินงานที่กำหนดไว้ในระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
2) การบ่งชี้สารสนเทศ (Labeling of Information)
    - องค์กร ต้องควบคุมให้ข้อมูลที่อยู่ในรูปแบบของเอกสารที่ถูกจัดทำขึ้นมีการควบคุมและรักษาความมั่นคงปลอดภัยอย่างเหมาะสม ตั้งแต่การเริ่มพิมพ์ การจัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้บุคลากรและ
    - ผู้ที่เกี่ยวข้องต้องปฏิบัติตาม เพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความมั่นคงปลอดภัยอย่างเหมาะสม

- ฝ่ายดิจิทัลเทคโนโลยีและหน่วยงานที่เกี่ยวข้อง ต้องทำป้ายชื่อตามทะเบียนบัญชีทรัพย์สินและขั้นตอนการใช้งานติดที่อุปกรณ์คอมพิวเตอร์ทุกชิ้น

3) การบริหารจัดการทรัพย์สิน (Handling of Assets) ฝ่ายดิจิทัลเทคโนโลยี ต้องควบคุมกำกับให้มีขั้นตอนการปฏิบัติงานในการบริหารจัดการทรัพย์สินสารสนเทศ เพื่อมิให้ข้อมูลสำคัญขององค์กรรั่วไหล หรือทรัพย์สินสารสนเทศถูกนำไปใช้ผิดประเภท

1.2.3. การถ่ายโอนข้อมูลสารสนเทศ (Information transfer)

1) จัดทำแนวทางหรือขั้นตอนการถ่ายโอนข้อมูลสารสนเทศ ผ่านเครื่องมือหรืออุปกรณ์ในการถ่ายโอนข้อมูลสารสนเทศ ทุกประเภท ทั้งการถ่ายโอนข้อมูลสารสนเทศภายในองค์กร รวมไปถึงการถ่ายโอนข้อมูลสารสนเทศระหว่างองค์กร กับ หน่วยงานภายนอก โดยต้องมีการรักษาความมั่นคงปลอดภัยสารสนเทศตามลำดับชั้นความลับของข้อมูลสารสนเทศที่องค์กรได้กำหนดไว้ โดยครอบคลุม

- ข้อมูลสารสนเทศที่อยู่อุปกรณ์ที่ใช้ปฏิบัติงาน (in Use/ at Endpoint)
- ข้อมูลสารสนเทศที่อยู่ระหว่างการส่งผ่านเครือข่าย (in Transit)
- ข้อมูลสารสนเทศที่อยู่ในระบบและสื่อบันทึกข้อมูล (at Rest) ได้แก่ ข้อมูลสารสนเทศบนระบบอุปกรณ์ และสื่อบันทึกข้อมูลฯ เป็นต้น

ส่วนที่ 1.3 การควบคุมการเข้าถึง (Access Control)

วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย สำหรับการควบคุมเข้าถึงและการใช้งานระบบสารสนเทศขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก รวมถึงจากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้แก่ข้อมูลขององค์กร

1.3.1. ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business Requirement for Access Control)

1) นโยบายควบคุมการเข้าถึง (Access Control Policy) องค์กรต้องกำหนดให้มีขั้นตอนควบคุมการเข้าถึง (Access Control Procedure) อย่างเป็นลายลักษณ์อักษร และปรับปรุงขั้นตอนให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม

2) การควบคุมการเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Networks and Network Service)

- ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดให้มีการขอเข้าถึงข้อมูลและระบบสารสนเทศของผู้ใช้งานโดยต้องได้รับการอนุมัติจากผู้บังคับบัญชาเท่านั้น
- ฝ่ายดิจิทัลเทคโนโลยี ต้องจำกัดให้ผู้ใช้งานสามารถเข้าถึงระบบเครือข่ายได้เฉพาะบริการที่ผู้ใช้งานได้รับอนุญาตให้เข้าถึงเท่านั้น โดยสิทธิ์ที่ได้รับต้องเป็นไปตามหน้าที่ความรับผิดชอบและความจำเป็นในการใช้งาน

1.3.2. การบริหารจัดการการเข้าถึงของผู้ใช้ (User Access Management)

1) การลงทะเบียนและถอดถอนสิทธิ์ผู้ใช้งาน (User Registration and De-Registration) ฝ่ายดิจิทัลเทคโนโลยีและเจ้าของข้อมูล ต้องร่วมกันกำหนดวิธีการบริหารจัดการการลงทะเบียนและถอดถอนสิทธิ์ผู้ใช้งานอย่างเป็นลายลักษณ์อักษรและปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม
2) การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Provisioning)
    - ฝ่ายดิจิทัลเทคโนโลยีและเจ้าของข้อมูล ต้องกำหนดให้มีการมอบหมายหรือกำหนดสิทธิ์การใช้งานให้แก่ผู้ใช้งานในการเข้าถึงข้อมูลหรือระบบสารสนเทศตามหน้าที่ความรับผิดชอบ
    - ฝ่ายดิจิทัลเทคโนโลยีและเจ้าของข้อมูล ต้องจัดทำเอกสารการมอบหมายสิทธิ์การเข้าถึงข้อมูลหรือระบบสารสนเทศ และจัดเก็บไว้เป็นหลักฐานในการดำเนินงาน
    - ฝ่ายดิจิทัลเทคโนโลยีและเจ้าของข้อมูล ต้องกำหนดกระบวนการในการบริหารจัดการสิทธิ์การเข้าถึง ในกรณีที่ผู้ใช้งานมีความจำเป็นต้องใช้งานข้อมูลหรือระบบสารสนเทศเกินสิทธิ์ที่ได้รับมอบหมาย
3) การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights)
    - ฝ่ายดิจิทัลเทคโนโลยีและเจ้าของข้อมูล ต้องจัดทำขั้นตอนปฏิบัติการทบทวนสิทธิ์การเข้าถึงข้อมูล ระบบสารสนเทศ และโปรแกรมประยุกต์ (Application) อย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม
    - ฝ่ายดิจิทัลเทคโนโลยีและเจ้าของข้อมูล ต้องกำหนดรอบในการทบทวนสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศอย่างชัดเจนและแจ้งให้ผู้ที่เกี่ยวข้องรับทราบ
    - การทบทวนสิทธิ์การเข้าถึง ต้องพิจารณาประเด็นดังต่อไปนี้
        1) รอบการทบทวนสิทธิ์ที่กำหนดไว้
        2) การพ้นสภาพการเป็นบุคลากรขององค์กร
        3) การเปลี่ยนแปลงโยกย้ายหน้าที่การปฏิบัติงาน
        4) การขอใช้สิทธิ์นอกเหนือจากหน้าที่ความรับผิดขอบที่กำหนดไว้
    - เมื่อดำเนินการทบทวนสิทธิ์เรียบร้อยแล้ว ให้เจ้าของข้อมูล หรือผู้ดูแลระบบจัดเก็บหลักฐานการทบทวนสิทธิ์ โดยให้แยกหลักฐานตามช่วงเวลาการทบทวนสิทธิ์
4) การถอดถอนสิทธิ์ในการเข้าถึง (Removal of Access Rights) เจ้าของข้อมูลและผู้ดูแลระบบ ต้องกำหนดเกณฑ์การพิจารณาการถอดถอนสิทธิ์การเข้าถึงและวิธีการถอดถอนสิทธิ์ในการเข้าถึงอย่างเป็นลายลักษณ์อักษร รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม

1.3.3. การบริหารจัดการอัตลักษณ์ (ที่ใช้ในการพิสูจน์ตัวตนเข้าระบบ) (Identity management)

1) ให้มีการบริหารจัดการลักษณะข้อมูลเฉพาะเพื่อยืนยันตัวตนที่เชื่อมโยงตัวบุคคลเพียงคนเดียว และกำหนดกระบวนการรักษาความมั่นคงปลอดภัยข้อมูลที่เกี่ยวข้องกับการพิสูจน์ตัวตน และต้องมีสื่อสารสร้างความตระหนักถึงการรักษาความมั่นคงปลอดภัยข้อมูลที่เกี่ยวข้องกับการพิสูจน์ตัวตน เพื่อให้บุคลากรมีการปฏิบัติอย่างเหมาะสม เช่น ต้องไม่เขียนชื่อผู้ใช้และรหัสผ่านไว้บนโต๊ะทำงาน ซึ่งอาจส่งผลให้ผู้ไม่มีสิทธิ์สามารถนำมาเข้าถึงระบบขององค์กรได้

1.3.4. การใช้งานข้อมูลการพิสูจน์ตัวตน (Use of Secret Authentication Information)

1) กำหนดกระบวนการและเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการอ้างถึงว่าเป็นผู้ใช้งานจริง โดยครอบคลุมตั้งแต่ขั้นตอนการกำหนดตัวตน การเปลี่ยนแปลงแก้ไขตัวตน การระงับตัวตน และการเพิกถอนตัวตน เพื่อให้การเข้าถึงข้อมูลสารสนเทศขององค์กร และบุคลากรเป็นไปตามบทบาท หน้าที่ และความรับผิดชอบที่ได้รับมอบหมาย ตามความจำเป็นอย่างเหมาะสม
2) ระบบสำหรับบริหารจัดการรหัสผ่าน (Password Management System)
    - ฝ่ายดิจิทัลเทคโนโลยี ต้องจัดให้มีระบบสำหรับบริหารจัดการบัญชีผู้ใช้และรหัสผ่านสำหรับการเข้าถึงระบบสารสนเทศของผู้ใช้งานภายในองค์กร เพื่อให้เกิดการบริหารจัดการที่เป็นมาตรฐานเดียวกัน
3) หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)
    - ผู้ใช้งานจะต้องไม่ใช้โครงสร้างรหัสผ่านหรือคุณลักษณะที่ง่ายต่อการเดา อาทิ คำศัพท์ในพจนานุกรม หรือคัดลอกหรือผสมจากชื่อผู้ใช้ หรืออักขระเรียงลำดับ หรือข้อมูลส่วนบุคคล หรือประโยควลีใดๆ ที่สามารถคาดเดาได้ง่าย
    - ผู้ใช้งานจะต้องไม่เขียนหรือบันทึกรหัสผ่านที่ใช้ และเก็บหรือแสดงให้เห็นไว้ใกล้กับระบบหรืออุปกรณ์ที่ใช้กับรหัสผ่านนั้น
    - ผู้ใช้งานจะต้องรับผิดชอบต่อการกระทำทุกอย่างที่เกิดขึ้นหากการกระทำนั้นสามารถ
    - บ่งชี้ให้เห็นว่าเกิดจากบัญชีผู้ใช้งานนั้น และจะต้องไม่อนุญาตให้ผู้อื่นกระทำการใดๆ โดยใช้บัญชีผู้ใช้งานของตน หรือกระทำการใดๆ โดยใช้บัญชีผู้ใช้งานอื่นที่ไม่มีสิทธิ์
    - ผู้ใช้งานจะต้องปฏิบัติตามข้อกำหนดการบริหารจัดการรหัสผ่านอื่นๆ ที่องค์กรกำหนดไว้

ส่วนที่ 1.4 การบริหารจัดการความสัมพันธ์กับหน่วยงานภายนอก (Supplier Relationships)

วัตถุประสงค์

เพื่อกำหนดมาตรการพิจารณาใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก รวมถึงมาตรการสำหรับการกำกับดูแล ติดตามการดำเนินงาน และรายงานผลการดำเนินงานของผู้ให้บริการรายอื่น และเพื่อให้การใช้บริการดังกล่าวเกิดประสิทธิภาพ มีความมั่นคงปลอดภัย และเกิดประโยชน์สูงสุดแก่องค์กร

1.4.1. ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับหน่วยงานภายนอก (Information Security in Supplier Relationships)

1) นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับหน่วยงานภายนอก (Information Security Policy for Supplier Relationships)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับหน่วยงานภายนอก โดยผู้ที่เกี่ยวข้องต้องพิจารณาหรือประเมินความเสี่ยงที่อาจเกิดขึ้นและกำหนดแนวทางป้องกันเพื่อลดความเสี่ยงนั้นก่อนที่จะอนุญาตให้หน่วยงานภายนอกหรือบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศขององค์กรผู้ดูแลระบบ และหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องควบคุมกำกับให้มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้าง ปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงาน ด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ

2) การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (Addressing Security within Supplier Agreements)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องควบคุมให้มีการกำหนดข้อตกลงเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้องกับการอนุญาตให้หน่วยงานภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศ เพื่อการอ่าน การประมวลผล การบริหารจัดการระบบสารสนเทศ หรือการพัฒนาระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร
   - ผู้ดูแลระบบ และหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องควบคุมให้หน่วยงานภายนอกสามารถเข้าถึงสารสนเทศขององค์กรเฉพาะส่วนที่มีความจำเป็นต้องรู้ และต้องได้รับการยินยอมจากเจ้าของข้อมูลสารสนเทศ อย่างเป็นลายลักษณ์อักษรเท่านั้น
   - ผู้ดูแลระบบ และหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องควบคุมดูแลให้หน่วยงานภายนอกปฏิบัติตามข้อกำหนดหรือข้อตกลงที่จัดทำขึ้นระหว่างองค์กรและหน่วยงานภายนอก

3) การบริหารจัดการและการสื่อสารต่อผู้รับจ้างช่วงของหน่วยงานภายนอก (Information and Communication Technology Supply Chain) ฝ่ายดิจิทัลเทคโนโลยี ต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับหน่วยงานภายนอกที่ให้บริการด้านสารสนเทศและบริการด้านการสื่อสาร โดยให้ครอบคลุมถึงผู้รับจ้างช่วงที่หน่วยงานภายนอกเป็นผู้จัดหา

1.4.2. การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier Service Delivery Management)

1) การติดตามและทบทวนการให้บริการของหน่วยงานภายนอก (Monitoring and Review of Supplier Services) ผู้ดูแลระบบ และหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องติดตามและตรวจทานการดำเนินงานของหน่วยงานภายนอกซึ่งมีหน้าที่ในการบริหารจัดการระบบประมวลผลข้อมูลสารสนเทศให้กับองค์กร ทั้งในด้านฐานะทางการเงิน กระบวนการปฏิบัติงานและประสิทธิภาพการให้บริการอย่างสม่ำเสมอ

2) การบริหารจัดการการเปลี่ยนแปลงบริการของหน่วยงานภายนอก (Managing Changes to Supplier Services) กรณีที่ผู้ให้บริการภายนอกมีการเปลี่ยนแปลงกระบวนการ ขั้นตอน วิธีการปฏิบัติงาน การรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน ผู้ดูแลระบบ และหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องจัดให้มีการประเมินความเสี่ยงจากการเปลี่ยนแปลงดังกล่าว โดยต้องรายงานให้ผู้บริหารและผู้ที่เกี่ยวข้องรับทราบ รวมถึงให้กำหนดกระบวนการบริหารจัดการความเสี่ยงดังกล่าวให้สอดคล้องเหมาะสม

ส่วนที่ 1.5 ความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์ (Information security for use of cloud services)

วัตถุประสงค์

เพื่อกำหนดหลักการ มาตรการ และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์ (Cloud) ขององค์กร เพื่อให้มั่นใจว่าการใช้งาน การจัดเก็บข้อมูล การประมวลผล และการบริหารจัดการบริการคลาวด์ (Cloud) มีความปลอดภัย สอดคล้องกับกฎหมาย มาตรฐาน และนโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

1.5.1. การคัดเลือกและประเมินผู้ให้บริการคลาวด์ (Cloud Provider Selection & Assessment)

1) องค์กรต้องดำเนินการประเมินความมั่นคงปลอดภัย ความน่าเชื่อถือ และการปฏิบัติตามมาตรฐานสากลของผู้ให้บริการคลาวด์ (เช่น ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018) รวมถึงประเมินความเสี่ยงก่อนเริ่มการใช้งานและเมื่อมีการเปลี่ยนแปลงบริการที่สำคัญ
2) องค์กรต้องตรวจสอบความเหมาะสมของเงื่อนไข SLA ความพร้อมใช้งาน การสำรองข้อมูล ความสามารถในการกู้คืนระบบ และความรับผิดชอบด้านความปลอดภัย ก่อนทำสัญญาหรือเริ่มใช้บริการ
3) การใช้บริการคลาวด์ทุกประเภทต้องได้รับอนุมัติจากผู้บริหารระดับฝ่ายของหน่วยงานและผู้บริหารฝ่ายดิจิทัลเทคโนโลยี โดยพิจารณาตามความจำเป็นและความเสี่ยงที่เกี่ยวข้องอย่างรอบคอบ รวมถึงการขออนุญาตจัดเก็บหรือประมวลผลข้อมูลสำคัญบนบริการคลาวด์สาธารณะ
4) องค์กรต้องจัดทำและบันทึกรายการทรัพย์สินทั้งหมดที่อยู่บนบริการคลาวด์ (Cloud Asset Inventory) เช่น Virtual Machines, Databases, Storage และบริการอื่น ๆ เพื่อให้สามารถควบคุม ตรวจสอบ และประเมินความเสี่ยงที่เกี่ยวข้องได้อย่างเหมาะสม รายการทรัพย์สินต้องได้รับการทบทวนและปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ

1.5.2. ความมั่นคงปลอดภัยของข้อมูล (Data Security & Protection)

1) ข้อมูลสำคัญและข้อมูลส่วนบุคคลที่ถูกจัดเก็บหรือประมวลผลบนบริการคลาวด์ ต้องได้รับการเข้ารหัสทั้งในขณะจัดเก็บ (at rest) และขณะส่งผ่านข้อมูล (in transit) เพื่อป้องกันการเข้าถึงหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

2) ก่อนนำข้อมูลขึ้นสู่ระบบคลาวด์ องค์กรต้องดำเนินการ จัดระดับชั้นความลับของข้อมูล (Information Classification) อย่างชัดเจน เพื่อให้สามารถกำหนดมาตรการควบคุมที่เหมาะสมกับระดับความเสี่ยงของข้อมูลแต่ละประเภท
3) ข้อมูลที่พ้นความจำเป็นในการใช้งานต้องได้รับการจัดการตามนโยบายการเก็บรักษาข้อมูล (Data Retention Policy) หรือนโยบายการลบข้อมูล (Data deletion policy) และต้องถูกลบหรือทำลายอย่างปลอดภัยตามมาตรฐานที่องค์กรกำหนด เพื่อป้องกันการนำข้อมูลไปใช้ในทางที่ไม่เหมาะสมหรือเกิดการรั่วไหล

1.5.3. การตั้งค่าและความปลอดภัยของระบบคลาวด์ (Secure Configuration & Hardening)

1) บริการคลาวด์ขององค์กรต้องได้รับการตั้งค่าให้มีความมั่นคงปลอดภัยตามแนวปฏิบัติที่ได้รับการยอมรับอย่างกว้างขวาง เช่น CIS Benchmark หรือแนวทางที่แนะนำโดยผู้ให้บริการ (Vendor Best Practice) เพื่อป้องกันความเสี่ยงจากการตั้งค่าที่ไม่เหมาะสม
2) ระบบและบริการที่ทำงานบนคลาวด์ต้องมีการตั้งค่าเวลา (Clock Synchronization) ให้สอดคล้องกับมาตรฐานเวลาที่องค์กรกำหนด เช่น NTP Server กลางขององค์กร เพื่อให้มั่นใจว่าการบันทึกเหตุการณ์ การวิเคราะห์ Log และการตรวจสอบเหตุการณ์ด้านความมั่นคงปลอดภัยสามารถดำเนินการได้อย่างถูกต้องและเชื่อถือได้
3) ระบบคลาวด์ต้องได้รับการควบคุมด้านความปลอดภัยของเครือข่ายอย่างรัดกุม เช่น การกำหนด Firewall Rules เพื่อจำกัดการเข้าถึงและลดโอกาสการถูกโจมตีจากภายนอกและภายใน รวมถึงต้องเปิดใช้งานเครื่องมือและบริการด้านความปลอดภัยที่จำเป็น เช่น Anti-malware และการตรวจสอบช่องโหว่ (Vulnerability Scanning) เพื่อช่วยป้องกัน ตรวจจับ และลดความเสี่ยงด้านความปลอดภัยในสภาพแวดล้อมคลาวด์ขององค์กร
4) องค์กรต้องมีการติดตาม ตรวจสอบ และประเมินประสิทธิภาพการทำงานของระบบบนคลาวด์อย่างต่อเนื่อง (Performance Efficiency Monitoring) รวมถึงการใช้ทรัพยากร (Resource Utilization) ความพร้อมใช้งาน (Availability) และขีดความสามารถของระบบ (Capacity) เช่น CPU, Memory, Network, Storage และบริการอื่น ๆ ที่เกี่ยวข้อง

1.5.4. ความต่อเนื่องทางธุรกิจและการกู้คืนระบบ (Backup & Business Continuity)

1) ระบบที่ทำงานบนคลาวด์ต้องมีการสำรองข้อมูลตามระดับความสำคัญ (Criticality Level) ที่องค์กรกำหนด โดยต้องดำเนินการสำรองข้อมูลอย่างสม่ำเสมอและเก็บรักษาให้ปลอดภัย
2) องค์กรต้องทดสอบการกู้คืนข้อมูล (Backup Restoration Test) เป็นประจำ เพื่อให้มั่นใจว่าสามารถกู้คืนข้อมูลได้อย่างถูกต้องและทันเวลาเมื่อต้องใช้งานจริง
3) บริการคลาวด์ต้องอยู่ภายใต้แผนความต่อเนื่องทางธุรกิจและการกู้คืนระบบ (BCP/DRP) ขององค์กร หรือมีความสอดคล้องกับความสามารถและแผนของผู้ให้บริการคลาวด์ เพื่อป้องกันผลกระทบต่อการดำเนินงานในกรณีเกิดเหตุหยุดชะงัก

1.5.5. การตรวจสอบและการติดตาม (Monitoring & Logging)

1) ต้องมีการบันทึก รักษาความสมบูรณ์ และจัดเก็บ Log ของเหตุการณ์ด้านความมั่นคงปลอดภัยที่สำคัญตามข้อกำหนดขององค์กร โดยข้อมูล Log ต้องสามารถนำไปตรวจสอบและวิเคราะห์ย้อนหลังได้

2) องค์กรต้องดำเนินการตรวจสอบ Log อย่างสม่ำเสมอ เพื่อระบุพฤติกรรมผิดปกติหรือสัญญาณของเหตุการณ์ด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้น

1.5.6. ความเป็นส่วนตัวและกฎหมาย (Privacy & Legal Compliance)

1) การประมวลผลข้อมูลส่วนบุคคลบนบริการคลาวด์ต้องเป็นไปตามกฎหมายและข้อบังคับที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) หรือข้อกฎหมายที่เกี่ยวข้องในพื้นที่ที่จัดเก็บหรือประมวลผลข้อมูล

1.5.7. การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (Incident Management)

1) บริการคลาวด์ต้องถูกบูรณาการเข้ากับแผนตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยขององค์กร (Incident Response Plan) เพื่อให้สามารถจัดการเหตุการณ์ได้อย่างเป็นระบบ

2) ผู้ให้บริการคลาวด์ต้องแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยต่อองค์กรตามกรอบเวลาและเงื่อนไขที่ระบุไว้ใน SLA เพื่อให้สามารถดำเนินการแก้ไขและบรรเทาความเสียหายได้ทันท่วงที

3) องค์กรต้องมีช่องทางการติดต่อเหตุฉุกเฉินและขั้นตอนการ Escalation ที่ชัดเจน เพื่อรองรับกรณีที่ต้องประสานงานกับผู้ให้บริการหรือหน่วยงานภายในที่เกี่ยวข้อง

1.5.8. การยุติสัญญาและถอนการใช้งาน (Termination & Exit Process)

1) เมื่อยุติการใช้บริการคลาวด์ องค์กรต้องดำเนินการถอนการใช้งานอย่างปลอดภัย รวมถึงการลบบัญชีผู้ใช้ การปิดสิทธิ์การเข้าถึง และการจัดการทรัพยากรบนคลาวด์ให้สมบูรณ์

2) ผู้รับผิดชอบต้องดำเนินการประสานงานกับผู้ให้บริการคลาวด์เพื่อให้ลบข้อมูลทั้งหมดที่เกี่ยวข้องกับองค์กรอย่างปลอดภัย พร้อมทั้งขอรับเอกสารรับรองการลบข้อมูล (Data Deletion Certificate) เพื่อยืนยันว่าการลบข้อมูลได้ดำเนินการครบถ้วนและถูกต้องตามข้อกำหนดขององค์กร

3) องค์กรต้องจัดทำแผนการย้ายข้อมูล (Data Migration / Exit Plan) เพื่อป้องกันภาวะการผูกติดกับผู้ให้บริการ (Vendor Lock-in) และเพื่อให้มั่นใจว่าสามารถย้ายข้อมูลกลับหรือย้ายไปยังผู้ให้บริการรายใหม่ได้อย่างปลอดภัยและต่อเนื่อง

ส่วนที่ 1.6 การจัดการด้านงบประมาณและการควบคุมการใช้จ่ายของการให้บริการ (Budgeting and Accounting for Services Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางในการบริหารจัดการงบประมาณและควบคุมค่าใช้จ่ายที่เกี่ยวข้องกับการสนับสนุนการให้บริการด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม

1.6.1. ฝ่ายดิจิทัลเทคโนโลยี ต้องดำเนินการจัดสรรงบประมาณให้ครบถ้วนและเพียงพอต่อการให้บริการและควบคุมการใช้จ่ายงบประมาณให้เกิดประสิทธิภาพสูงสุด

1.6.2. ฝ่ายดิจิทัลเทคโนโลยี ต้องจัดให้มีการจัดสรรงบประมาณจะต้องพิจารณาต้นทุนทางตรง (Direct Cost) ต้นทุนทางอ้อม (Indirect Cost) ค่าใช้จ่ายของการจัดซื้อทรัพย์สินสารสนเทศ (IT Asset) ค่าใช้จ่ายจากการใช้ทรัพยากรร่วมกัน (Shared Resource Cost) ค่าใช้จ่ายประจำสำนักงาน (General and Administrative Expense) ค่าใช้จ่ายในการจัดจ้างหน่วยงานภายนอก (Externally Supplied Service Cost) ค่าใช้จ่ายของการจัดจ้างบุคลากร (People) และค่าใช้จ่ายด้านลิขสิทธิ์ต่างๆ (License Expense) รวมถึงค่าใช้จ่ายอื่นๆ ที่เกี่ยวข้องในการให้บริการ

1.6.3. ฝ่ายดิจิทัลเทคโนโลยี ต้องติดตามการใช้งบประมาณ และตรวจสอบงบประมาณคงเหลือเพื่อให้บริหารการใช้งบประมาณได้อย่างมีประสิทธิภาพ

ส่วนที่ 1.7 การจัดการระดับการให้บริการ (Service Level Management Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางในการจัดทำข้อตกลงสำหรับระดับการให้บริการด้านเทคโนโลยีสารสนเทศ ระหว่างฝ่ายดิจิทัลเทคโนโลยีและผู้ใช้งานระบบสารสนเทศขององค์กร ให้อยู่ในเกณฑ์ที่สามารถยอมรับได้

1.7.1. องค์กรต้องกำหนดให้มีการจัดทำสัญญาที่ระบุถึงข้อตกลงระดับการให้บริการดังต่อไปนี้

1) ข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) ระหว่างหน่วยงานผู้ให้บริการและผู้ใช้งาน
2) ข้อตกลงการให้บริการระดับปฏิบัติงาน (Operational Level Agreement: OLA) ระหว่างหน่วยงานผู้ให้บริการภายในองค์กร
3) สัญญาการให้บริการ (Underpinning Contracts: UC) ระหว่างหน่วยงานผู้ให้บริการและหน่วยงานภายนอก

1.7.2. ฝ่ายดิจิทัลเทคโนโลยี ต้องจัดทำข้อตกลงการให้บริการระหว่างฝ่ายดิจิทัลเทคโนโลยีและผู้ใช้งาน ทั้งนี้ข้อตกลงการให้บริการต้องได้รับการอนุมัติอย่างเป็นทางการจากผู้บริหารระดับฝ่ายดิจิทัลเทคโนโลยีและตัวแทนผู้บริหารจากหน่วยงานต่างๆ ภายในองค์กร

1.7.3. ฝ่ายดิจิทัลเทคโนโลยี ต้องดำเนินการบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับสัญญาข้อตกลงการให้บริการ

1.7.4. ฝ่ายดิจิทัลเทคโนโลยี ต้องดำเนินการตรวจสอบวิเคราะห์ประสิทธิภาพการทำงาน แนวโน้มของการให้บริการเป็นระยะตามความเหมาะสม และนำมาแก้ไขปรับปรุงเพื่อเพิ่มประสิทธิภาพในการดำเนินงานต่อไป

1.7.5. การแก้ไขเอกสารใดๆ ที่เกี่ยวข้องกับ ความต้องการด้านการให้บริการ (Service Requirement) ระดับการให้บริการ (Service Level Agreement) หรือรายละเอียดการให้บริการ (Service Catalogue) ต้องถูกดำเนินการผ่านการบริหารจัดการการเปลี่ยนแปลง (Change Management) ที่องค์กรกำหนดไว

ส่วนที่ 1.8 การให้บริการด้านงานเทคโนโลยีสารสนเทศแก่บุคคลอื่น (IT Insourcing) และการใช้บริการด้านงาน เทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing)

วัตถุประสงค์

เพื่อจัดทำข้อกำหนดต่างๆ และกรอบการปฏิบัติงานในการให้บริการหรือการใช้บริการด้านงานเทคโนโลยีสารสนเทศขององค์กรให้มีประสิทธิภาพ มีความมั่นคงปลอดภัยและเกิดผลประโยชน์สูงสุดแก่องค์กร

1.8.1. การให้บริการด้านงานเทคโนโลยีสารสนเทศแก่บุคคลอื่น (IT Insourcing)

1) ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดให้มีการควบคุมและกำกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ ให้เป็นไปตามข้อกำหนดต่างๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจขององค์กร โดยฝ่ายเทคโนโลยีสารสเทศจะให้บริการทางเทคโนโลยีสารสนเทศภายในองค์กรและบริษัทย่อยเท่านั้น
2) ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดให้มีการควบคุมภายในและจัดทำขั้นตอนการปฏิบัติงาน (Operation Procedure Manual) โดยให้มีการแบ่งแยกอำนาจหน้าที่ของผู้ปฏิบัติงาน (Segregation of Duty) ตามโครงสร้างผู้ปฏิบัติงานที่ชัดเจนและให้บันทึกการปฏิบัติงานนั้นอย่างสม่ำเสมอ
3) ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดให้มีมาตรการรองรับเหตุฉุกเฉิน โดยจัดให้มีแผนการรองรับเหตุฉุกเฉินและการสำรองข้อมูล รวมถึงกำหนดรอบการสำรองข้อมูลตามที่ตกลงกันไว้กับผู้รับบริการ
4) ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดให้มีการสำรองข้อมูลโดยใช้สื่อบันทึกข้อมูล และเก็บสื่อบันทึกข้อมูลในสถานที่ที่ผู้รับบริการจัดหาและเตรียมไว้ให้เป็นการเฉพาะ หรือสถานที่ที่ได้ตกลงไว้ร่วมกันรวมถึงไม่นำข้อมูลการให้บริการของผู้รับบริการไปเผยแพร่หรือนำไปใช้กับบุคคลภายนอก
5) องค์กรต้องกำหนดให้ผู้ให้บริการมีการบริหารการจัดการระดับการให้บริการตามนโยบายที่การจัดการระดับการให้บริการ (Service Level Management Policy) กำหนดไว้ใน

1.8.2. การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing)

การจัดหาผู้ให้บริการภายนอกเพื่อให้บริการงานด้านเทคโนโลยีสารสนเทศต้องพิจารณาให้มีความสอดคล้องกับกลยุทธ์ทางธุรกิจขององค์กร และคำนึงถึงการให้บริการแก่ลูกค้าอย่างต่อเนื่องและมีความถูกต้องน่าเชื่อถือ โดยมีหลักเกณฑ์เบื้องต้นในการใช้บริการจากผู้ให้บริการภายนอก ดังนี้

1) หลักเกณฑ์ในการพิจารณาการใช้บริการจากผู้ให้บริการภายนอก ต้องไม่ขัดแย้งกับกฎระเบียบ หรือข้อกำหนดที่หน่วยงานราชการประกาศใช้
2) การจัดให้มีการบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management) เพื่อให้มั่นใจว่าระบบสารสนเทศขององค์กรและบริษัทสามารถดำเนินธุรกิจหรือให้บริการลูกค้าได้อย่างต่อเนื่อง

3) แนวทางในการพิจารณาคัดเลือกผู้ให้บริการเพื่อประเมินถึงความน่าเชื่อถือของการให้บริการและเพื่อให้แน่ใจว่าผู้ให้บริการมีความสามารถในการให้บริการบริษัทฯ ได้ตามข้อตกลงการให้บริการพร้อมกับให้ผู้ให้บริการภายนอกประเมินตนเองใน "แบบประเมินความเสี่ยงด้าน IT และ Cyber security (F-DT-01-04)"
4) แนวทางในการรักษาความมั่นคงปลอดภัยและรักษาความลับของข้อมูล เพื่อให้แน่ใจว่าได้ดูแลและรับผิดชอบต่อลูกค้า และมีการคุ้มครองผู้บริโภค (Customer Protection) อย่างเหมาะสม
5) การติดตาม การประเมินผล และการตรวจสอบการให้บริการจากบุคคลภายนอกอย่างสม่ำเสมอ เพื่อให้เป็นไปตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้
6) กำหนดให้มีแนวทางการบริหารความเสี่ยงจากการใช้บริการจากบุคคลภายนอก สำหรับความเสี่ยงด้านปฏิบัติการ (Operational risk) ความเสี่ยงด้านกลยุทธ์ (Strategic risk) ความเสี่ยงด้านชื่อเสียง(Reputational risk) และความเสี่ยงด้านกฎหมาย (Legal risk) โดยกำหนดแนวทางการบริหารความเสี่ยงจากการใช้บริการบุคคลภายนอกเพื่อใช้บริการด้านเทคโนโลยีสารสนเทศไว้อย่างชัดเจนและเป็นลายลักษณ์อักษร ให้เหมาะสมกับความสำคัญของระบบงานที่ใช้บริการจากบุคคลภายนอก และสอดคล้องกับนโยบายการบริหารความเสี่ยงโดยรวม รวมทั้งสื่อสารให้บุคคลที่เกี่ยวข้องเข้าใจและถือปฏิบัติตามแนวทางที่กำหนดไว้
7) มีการสื่อสารแก่ผู้ให้บริการภายนอกทราบ และลงนามเกี่ยวกับจรรยาบรรณการทำงานของบริษัทฯ

ส่วนที่ 1.9 การบริหารจัดการเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

วัตถุประสงค์

เพื่อกำหนดแนวทางในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ การเรียนรู้ข้อผิดพลาดจากปัญหาที่เกิดขึ้นและการปรับปรุงแก้ไข ซึ่งเป็นการป้องกันไม่ให้เกิดเหตุการณ์ทางด้านความมั่นคงปลอดภัยสารสนเทศซ้ำขึ้นอีก

1.9.1. การบริหารจัดการเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Management of Information Security Incidents and Improvements)

1) หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)
   - ฝ่ายดิจิทัลเทคโนโลยีต้องกำหนดหน้าที่ในการบริหารจัดการสถานการด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดคิด และมอบหมายสิทธิ์การดำเนินงานอย่างชัดเจนให้บุคลากรภายในฝ่าย
   - ฝ่ายดิจิทัลเทคโนโลยีต้องกำหนดให้มีการจำแนกสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดคิดออกจากเหตุขัดข้องด้านการปฏิบัติงานทั่วไป เพื่อกำหนดแนวทางการแก้ไขที่ถูกต้องเหมาะสม

- ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดช่องทางและเกณฑ์ในการรายงานเหตุการณ์หรือจุดอ่อนหรือเหตุขัดข้องที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศและสื่อสารให้บุคลากรในองค์กรและหน่วยงานภายนอกรับทราบ

2) การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and Decision on Information Security Events) ผู้ดูแลระบบ ต้องประเมินเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ทำการจัดแยกกลุ่มเหตุการณ์หรือจุดอ่อนด้านความมั่นคงปลอดภัยและจัดลำดับความสำคัญตามเกณฑ์ที่กำหนดไว้ และแจ้งผู้ที่เกี่ยวข้องรับทราบเพื่อแก้ไขในกรณีที่พบว่าเหตุการณ์หรือจุดอ่อนนั้นอาจเป็นเหตุการณ์ที่ส่งผลกระทบด้านความมั่นคงปลอดภัยสารสนเทศ
3) การตอบสนองต่อเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Response to Information Security Incidents)
   - บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ และหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ ต้องดำเนินการตามขั้นตอนการปฏิบัติงานสำหรับการแก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศที่ได้กำหนดไว้
   - บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ และหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ ต้องดำเนินการตอบสนองและแก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศตามระยะเวลาที่กำหนดไว้ หากไม่สามารถแก้ไขได้ตามเวลาที่กำหนดต้องแจ้งให้ผู้บังคับบัญชารับทราบโดยเร็วที่สุด
4) การเรียนรู้จากเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Learning from Information Security Incidents) บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ และหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ จะต้องจัดเตรียมรายงานผลการวิเคราะห์และการแก้ไขเหตุขัดข้อง จุดอ่อน หรือช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และจัดเก็บไว้เป็นองค์ความรู้ เพื่อใช้ในการเรียนรู้ในการดำเนินงานและลดโอกาสเกิดในอนาคต
5) การเก็บรวบรวมหลักฐาน (Collection of Evidence) บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศและหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ จะต้องดำเนินการเก็บรวบรวมหลักฐานที่เกี่ยวข้องกับเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น เพื่อรวบรวมหลักฐานให้เพียงพอต่อการนำเสนอผู้บริหารหน่วยงานที่เกี่ยวข้อง และใช้ในการดำเนินการด้านกฎหมายต่อไป

ส่วนที่ 1.10 การบริหารจัดการเหตุขัดข้อง และการบริหารจัดการคำร้องขอ (Incident and Service Request Management Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางการแก้ไขเหตุขัดข้อง การจัดหา และการจัดการระบบงานคอมพิวเตอร์ขององค์กร ให้สามารถสนับสนุนการให้บริการธุรกิจขององค์กรได้อย่างรวดเร็ว มีความต่อเนื่อง มีความถูกต้องน่าเชื่อถือ และมีประสิทธิภาพ

1.10.1. การบริหารจัดการเหตุขัดข้อง

1) ฝ่ายดิจิทัลเทคโนโลยี ต้องดำเนินการกำหนดเกณฑ์ในการวัดระดับผลกระทบ(Impact) ความเร่งด่วน (Urgency) และลำดับความสำคัญ (Priority) ของเหตุขัดข้อง
2) ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดหน้าที่ความรับผิดชอบในการแก้ไขเหตุขัดข้อง พร้อมทั้งจัดทำขั้นตอนการปฏิบัติงานสำหรับการบริหารจัดการเหตุขัดข้องและบริหารจัดการคำร้องขอ เพื่อใช้เป็นแนวทางในการดำเนินงาน
3) ฝ่ายดิจิทัลเทคโนโลยี ต้องดำเนินการบันทึกรายละเอียดของเหตุขัดข้องและคำร้องขอให้ครบถ้วนตามขั้นตอนปฏิบัติงานที่ระบุไว้ เพื่อใช้เป็นหลักฐานและใช้ประกอบการวิเคราะห์หาวิธีการแก้ไข และรายงานผลการดำเนินงานต่อไป
4) บุคลากรฝ่ายดิจิทัลเทคโนโลยี ต้องดำเนินการแก้ไขเหตุขัดข้องและคำร้องขอ ที่ได้รับแจ้งมาอย่างรวดเร็วเต็มความสามารถ ให้สอดคล้องกับข้อตกลงการให้บริการที่ได้กำหนดไว้

1.10.2. กรณีที่ผู้รับเรื่องไม่สามารถแก้ไขเหตุขัดข้องและคำร้องขอได้ด้วยตนเองจะต้องยกระดับการให้บริการ(Escalation) ไปยังผู้เกี่ยวข้องตามลำดับ เพื่อเพิ่มประสิทธิภาพและความรวดเร็วในการดำเนินงาน

1.10.3. การบริหารจัดการคำร้องขอ

1) หน่วยงานที่ต้องการให้มีการจัดหาระบบงานคอมพิวเตอร์ ต้องระบุความต้องการระบบงานคอมพิวเตอร์ของแต่ละหน่วยงาน รวมทั้งจัดทำเป็นโครงการและขออนุมัติงบประมาณในการจัดทำโครงการ โดยให้มีการบันทึกเป็นลายลักษณ์อักษรและได้รับการอนุมัติจากผู้บริหารระดับฝ่าย และคณะกรรมการเทคโนโลยีสารสนเทศ
2) ฝ่ายดิจิทัลเทคโนโลยี ต้องให้การสนับสนุนด้านข้อมูลที่เกี่ยวข้องกับการจัดหาระบบงานคอมพิวเตอร์ เช่น หน่วยงานภายนอก คุณสมบัติของเครื่องคอมพิวเตอร์ ข้อมูลความมั่นคงปลอดภัยด้านสารสนเทศ หรือข้อมูลอื่นใดที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศตามที่ได้รับการร้องขอ

ส่วนที่ 1.11 ความมั่นคงปลอดภัยสำหรับการบริหารจัดการความต่อเนื่องในการดำเนินธุรกิจ (Information Security Aspects of Business Continuity Management)

วัตถุประสงค์

เพื่อป้องกันการติดขัด หรือหยุดชะงักของการดำเนินธุรกิจขององค์กรและป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวของระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบสารสนเทศกลับคืนมาได้ในระยะเวลาอันเหมาะสม

1.11.1. ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Continuity)

1) การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning Information Security Continuity) เจ้าของข้อมูลและฝ่ายดิจิทัลเทคโนโลยี ต้องร่วมกันระบุเหตุการณ์ที่อาจส่งผลกระทบกับกระบวนการทางธุรกิจ ประเมินความเสี่ยงเหตุการณ์และระบบงานสำคัญ เพื่อให้ได้มาซึ่งข้อมูลที่มีความถูกต้อง และครบถ้วน เพื่อใช้ในการจัดทำแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ
2) การสร้างกระบวนการความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing Information Security Continuity) ฝ่ายดิจิทัลเทคโนโลยี ต้องจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉิน โดยให้กำหนดมาตรการด้านความมั่นคงปลอดภัยสารสนเทศไว้เป็นส่วนหนึ่งของแผน และให้มีความสอดคล้องกับแผนบริหารความต่อเนื่องทางธุรกิจขององค์กร
3) การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, Review and Evaluate Information Security Continuity)
    - ฝ่ายดิจิทัลเทคโนโลยี ต้องทดสอบแผนรองรับกรณีเกิดเหตุฉุกเฉินอย่างน้อยปีละ 1 ครั้งและจัดให้มีการบันทึกผลการทดสอบ เพื่อให้มั่นใจว่าแผนงานที่จัดทำมีความถูกต้องและสามารถตอบสนองต่อการดำเนินงานได้เป็นอย่างดี
    - บุคลากรผู้ซึ่งมีส่วนเกี่ยวข้องในการปฏิบัติงานกู้คืนระบบสารสนเทศ ต้องมีความรู้ด้านเทคนิคที่จำเป็นต่อการกู้คืนระบบและเข้าร่วมการซักซ้อมแผน
    - เจ้าของข้อมูลและผู้ใช้งานระบบที่เกี่ยวข้องกับแผนรองรับการดำเนินการทางธุรกิจอย่างต่อเนื่องต้องเข้าร่วมการทดสอบแผน และดำเนินงานตามแผนที่กำหนดไว้

1.11.2. การจัดให้มีอุปกรณ์หรือระบบสารสนเทศสำรอง (Redundancies)

1) สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of Information Processing Facilities)
    - องค์กรต้องควบคุมให้มีการประเมินความต้องการด้านการรักษาสภาพความพร้อมใช้งาน (Availability) ของระบบสารสนเทศที่มีความสำคัญสูง
    - องค์กรต้องกำกับให้มีการติดตั้งระบบสารสนเทศสำรอง หรืออุปกรณ์สำรอง หรือระบบสำหรับสนับสนุนการให้บริการที่เพียงพอ เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจที่เหมาะสม

ส่วนที่ 1.12 การบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management)

วัตถุประสงค์

เพื่อกำหนดแนวทางการบริหารจัดการความต่อเนื่องในการให้บริการระบบสารสนเทศ ในกรณีที่เกิดเหตุฉุกเฉินหรือเหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศใดๆ ซึ่งอาจส่งผลกระทบให้การดำเนินธุรกิจขององค์กรหยุดชะงัก

1.12.1. องค์กรต้องจัดให้มีการสำรองข้อมูลและการกู้คืนระบบสารสนเทศ เพื่อให้มั่นใจว่ากระบวนการทางธุรกิจสามารถดำเนินการได้อย่างต่อเนื่อง และลดผลกระทบเมื่อเกิดเหตุการณ์ที่ส่งผลให้การดำเนินธุรกิจหยุดชะงัก โดยมีผู้บริหารระดับสูงสุดขององค์กรเป็นผู้มีอำนาจตัดสินใจในการสั่งการ

1.12.2. หน่วยงานผู้ใช้บริการ และฝ่ายดิจิทัลเทคโนโลยี ต้องร่วมกันกำหนดกรอบมาตรฐาน (Framework) เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจและครอบคลุมข้อกำหนดความมั่นคงปลอดภัยด้านสารสนเทศที่ได้กำหนดไว้ รวมถึงมีความสะดวกในการจัดลำดับความสำคัญของแผนและกิจกรรมที่ต้องดำเนินการ

1.12.3. หน่วยงานผู้ใช้บริการ และฝ่ายดิจิทัลเทคโนโลยี ต้องจัดให้มีการประเมินความเสี่ยงและบันทึกความเสี่ยงที่อาจส่งผลให้การให้บริการระบบสารสนเทศขาดความต่อเนื่อง และทำข้อตกลงเงื่อนไขความต้องการ ได้แก่ ช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด (Maximum Tolerable Period of Disruption: MTPD) หรือระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objective: RTO) และ ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery point objective: RPO) อย่างเป็นลายลักษณ์อักษร

1.12.4. หน่วยงานผู้ใช้บริการ และฝ่ายดิจิทัลเทคโนโลยี ต้องควบคุม กำกับให้มีการจัดทำแผนการบริหารจัดการความต่อเนื่องทางธุรกิจภายใต้กรอบมาตรฐานที่กำหนดไว้ และเผยแพร่ให้ผู้ที่เกี่ยวข้องรับทราบทั้งนี้แผนการบริหารจัดการความต่อเนื่องทางธุรกิจควรได้รับการทดสอบอย่างน้อยปีละ 1 ครั้ง

1.12.5. ฝ่ายดิจิทัลเทคโนโลยี ต้องจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉิน (Disaster Recovery Plan: DRP) โดยให้มีความสอดคล้องกับแผนการบริหารจัดการความต่อเนื่องทางธุรกิจขององค์กร

1.12.6. ฝ่ายดิจิทัลเทคโนโลยี ต้องดำเนินการสำรองข้อมูล เอกสาร ซอฟต์แวร์ และระบบงาน รวมถึงอุปกรณ์ต่างๆ และบุคลากรที่จำเป็น เพื่อสนับสนุนให้การกู้คืนระบบสารสนเทศให้เป็นไปอย่างรวดเร็วที่สุด หลังจากเกิดการหยุดชะงักในการให้บริการหรือเหตุภัยพิบัติ

1.12.7. ฝ่ายดิจิทัลเทคโนโลยี ต้องจัดให้มีการทดสอบแผนรองรับกรณีเกิดเหตุฉุกเฉิน (Disaster Recovery Plan: DRP) อย่างน้อยปีละ 1 ครั้ง และให้มีการบันทึกผลการทดสอบเพื่อให้มั่นใจได้ว่าธุรกิจสามารถดำเนินต่อไปได้เมื่อเกิดเหตุการณ์ที่กระทบกับกระบวนการทางธุรกิจขององค์กร

ส่วนที่ 1.13 การปฏิบัติตามกฎระเบียบและข้อบังคับ (Compliance)

วัตถุประสงค์

เพื่อให้การดำเนินงานต่างๆ ขององค์กรเป็นไปตามกฎหมาย ข้อตกลง สัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยต่างๆ ที่องค์กรและบุคลากรขององค์กรต้องปฏิบัติตาม รวมถึงให้มีการตรวจสอบการปฏิบัติตามนโยบายทางด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้

1.13.1. การปฏิบัติตามกฎหมาย กฎระเบียบ และข้อบังคับที่เกี่ยวข้อง (Compliance with Legal and Contractual Requirements)

1) การระบุกฎหมายและข้อกำหนดในสัญญาจ้าง (Identification of Applicable Legislation and Contractual Requirements)
   - ฝ่ายดิจิทัลเทคโนโลยีต้องร่วมกับฝ่ายกฎหมาย และฝ่ายบริหารทรัพยากรบุคคลในการรวบรวมกฎหมาย กฎระเบียบ หลักเกณฑ์ และข้อกำหนดต่างๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และจัดทำเป็นเอกสารเพื่อใช้เป็นข้อกำหนดในการปฏิบัติงานอย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ
   - บุคลากรทั้งหมดต้องรับผิดชอบในการปฏิบัติตามข้อกำหนดที่ได้มีการระบุไว้อย่างเคร่งครัด
   - ห้ามเจ้าหน้าที่ในองค์กรใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศขององค์กรกระทำการใดๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทยและกฎหมายระหว่างประเทศไม่ว่าโดยกรณีใดก็ตาม

2) การป้องกันสิทธิ และทรัพย์สินทางปัญญา (Intellectual Property Rights)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องจัดทำกระบวนการสำหรับการบริหารจัดการการใช้ซอฟต์แวร์ลิขสิทธิ์และทรัพย์สินทางปัญญา เพื่อให้มั่นใจว่าการใช้งานข้อมูลสารสนเทศที่อาจถือเป็นทรัพย์สินทางปัญญา หรือการใช้งานซอฟต์แวร์ที่พัฒนาโดยผู้ประกอบธุรกิจมีความสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่างๆ
   - ผู้ใช้งานต้องไม่ทำสำเนาหรือเผยแพร่ซอฟต์แวร์ที่องค์กรได้จัดซื้อลิขสิทธิ์เพื่อการใช้งาน ยกเว้นการทำสำเนานั้นเพียงแต่เพื่อไว้ใช้สำหรับเหตุฉุกเฉินหรือเพื่อเป็นสำเนาไว้ ใช้แทนซอฟต์แวร์ต้นฉบับเท่านั้น
   - ห้ามผู้ใช้งานทำการใช้งานทำซ้ำ หรือ เผยแพร่รูปภาพ บทความ หนังสือ หรือเอกสารใดๆ
   - ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบสารสนเทศขององค์กรโดยเด็ดขาด
   - ซอฟต์แวร์ที่พัฒนาเพื่อองค์กร ทั้งโดยหน่วยงานภายนอกหรือบุคลากรในหน่วยงานขององค์กรถือว่าเป็นทรัพย์สินขององค์กร องค์กรไม่อนุญาตให้หน่วยงานภายนอกหรือบุคลากรในหน่วยงานขององค์กรทำสำเนา หรือเผยแพร่ซอฟต์แวร์ที่เป็นทรัพย์สินขององค์กรโดยไม่ได้รับอนุญาต

- ผู้ใช้งานที่ใช้งานซอฟต์แวร์บนระบบสารสนเทศขององค์กรต้องยึดถือและปฏิบัติตามกฎหมายลิขสิทธิ์ นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ และข้อกำหนดของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด
- ห้ามมิให้พนักงานเปิดเพลงที่ไม่มีใบอนุญาต และเพลงที่ทางบริษัทไม่ได้เป็นผู้จัดส่งให้เข้าในระบบกระจายเสียงของบริษัท ทั้งนี้รวมถึงการเปิดเพลงจากแผ่นเสียงที่มีลิขสิทธิ์ถูกต้อง หรือจากเครือข่ายสาธารณะ เช่น วิทยุ YouTube เป็นต้น เนื่องจากการกระทำดังกล่าวถือเป็นการละเมิดลิขสิทธิ์ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 ในเรื่องของการเผยแพร่ผลงานต่อสาธารณชนโดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์

3) การป้องกันข้อมูลขององค์กร (Protection of Records)
   - เจ้าของข้อมูล ต้องปฏิบัติตามข้อบังคับทางกฎหมายที่เกี่ยวกับข้อมูลสารสนเทศบางประเภทเช่น ด้านบัญชี ด้านลูกค้า และต้องจัดทำข้อกำหนดในการจัดการข้อมูลสารสนเทศ ระยะเวลาในการจัดเก็บ ให้สอดคล้องกับข้อบังคับดังกล่าว
   - เจ้าของข้อมูลต้องควบคุม ป้องกันมิให้ข้อมูลบันทึกหลักฐาน (Logs) ต่างๆ เกิดความเสียหายสูญหาย ถูกเปลี่ยนแปลงแก้ไข ถูกเข้าถึงหรือเผยแพร่โดยไม่ได้รับอนุญาต โดยการควบคุมต้องให้สอดคล้องกับกฎหมาย ข้อกำหนด และความต้องการทางธุรกิจ
4) ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and Protection of Personal Identifiable Information)
   - องค์กร ต้องจัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมายประกาศหลักเกณฑ์ที่รัฐบาลได้ประกาศไว้ รวมถึงข้อบังคับต่างๆ ที่มีผลบังคับใช้กับองค์กร
   - ข้อมูลสารสนเทศรายละเอียดที่เกี่ยวกับลูกค้าถือว่ามีความสำคัญ หน่วยงานผู้รับผิดชอบในการดูแลข้อมูลต้องกำหนดให้บุคลากรและลูกจ้างที่ได้รับมอบหมายตามหน้าที่งานหรือได้รับอนุญาตจากผู้บังคับบัญชาเท่านั้นที่สามารถเปลี่ยนแปลงแก้ไขข้อมูลสารสนเทศดังกล่าวได้
   - ข้อมูลสารสนเทศส่วนบุคคลของบุคลากร ลูกจ้าง และลูกค้า ถือว่าเป็นความลับ และ สามารถเปิดเผยได้เฉพาะผู้ที่มีสิทธิ์ ตามที่องค์กรกำหนดเท่านั้น
5) ระเบียบข้อบังคับสำหรับมาตรการเข้ารหัสลับข้อมูล (Regulation of Cryptographic Controls) ฝ่ายดิจิทัลเทคโนโลยี ต้องควบคุมการเข้ารหัสลับข้อมูลให้มีความสอดคล้องกับกฎหมายประกาศ หลักเกณฑ์ที่รัฐบาลได้ประกาศไว้ รวมถึงข้อบังคับต่างๆ ที่มีผลบังคับใช้กับองค์กร

1.13.2. การทบทวนความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Reviews)

1) การตรวจประเมินระบบสารสนเทศจากผู้ตรวจสอบอิสระ (Independent Review of Information Security)
   - องค์กรต้องจัดให้มีการตรวจประเมินความมั่นคงปลอดภัยสารสนเทศโดยส่วนตรวจสอบระบบงานหรือผู้ตรวจสอบอิสระภายนอก เพื่อตรวจสอบการปฏิบัติตามนโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ ตลอดจนทบทวนถึงความพอเพียงของการควบคุมระบบสารสนเทศ และการปฏิบัติตามการควบคุมต่างๆ
2) การปฏิบัติตามนโยบายและมาตรฐานความปลอดภัยสารสนเทศ (Compliance with Security Policies and Standards)
   - ผู้บังคับบัญชาของแต่ละแผนกต้องรับผิดชอบในการสอบทานการปฏิบัติตามนโยบาย มาตรฐานและขั้นตอนปฏิบัติงานที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ ของบุคลากรใต้บังคับบัญชาอย่างสม่ำเสมอ
   - กรณีที่ผู้บังคับบัญชาของแต่ละแผนกตรวจพบการปฏิบัติงานที่ไม่สอดคล้องกับนโยบายมาตรฐาน และขั้นตอนปฏิบัติซึ่งยังไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร ผู้บังคับบัญชาต้องชี้แจงให้บุคลากรใต้บังคับบัญชารับทราบและทำความเข้าใจ แต่หากความไม่สอดคล้องที่พบส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศขององค์กรผู้บังคับบัญชาต้องดำเนินการลงโทษทางวินัยตามกฎระเบียบที่องค์กรกำหนดไว้
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องให้การสนับสนุนด้านการให้คำแนะนำในการใช้งาน หรือการปฏิบัติตามนโยบาย มาตรฐาน ขั้นตอนปฏิบัติ และข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศต่อหน่วยงานอื่นเมื่อได้รับคำร้องขอ
3) การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review)
   - ต้องจัดให้มีการทบทวนระบบสารสนเทศในด้านเทคนิค เช่น การทดสอบการบุกรุกระบบสารสนเทศ (Penetration Test) อย่างสม่ำเสมอ เพื่อให้สอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ
   - ส่วนตรวจสอบระบบงาน ต้องตรวจสอบการควบคุมทางเทคนิคของระบบสารสนเทศ
   - เพื่อตรวจสอบว่ามีความเพียงพอเหมาะสม และมีการปฏิบัติตามการควบคุมเหล่านั้น
   - ผู้ดูแลระบบ ต้องจัดให้มีการทดสอบระดับมาตรฐานความมั่นคงปลอดภัยของระบบสารสนเทศอย่างสม่ำเสมอ เช่น การตรวจหาช่องโหว่ของระบบสารเทศ (Vulnerability Assessment) หรือการทดสอบการบุกรุกระบบ (Penetration Test) อย่างสม่ำเสมอ เพื่อให้สอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

ส่วนที่ 1.14 เอกสารขั้นตอนการปฏิบัติงาน (Documented operating procedures)

วัตถุประสงค์

เพื่อกำหนดหลักการและมาตรฐานในการจัดทำ จัดเก็บ และเผยแพร่ขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับการประมวลผลข้อมูล เพื่อให้การดำเนินงานมีความถูกต้องมั่นคงปลอดภัยและสอดคล้องตามมาตรฐานกำหนด

1.14.1. ฝ่ายดิจิทัลเทคโนโลยี ต้องจัดให้มีขั้นตอนปฏิบัติงานสำหรับด้านระบบสารสนเทศที่สำคัญเป็นลายลักษณ์อักษร โดยต้องแบ่งแยกอำนาจหน้าที่ของบุคลากรตามโครงสร้างการปฏิบัติหน้าที่ที่ชัดเจนเพื่อให้บุคลากรสามารถปฏิบัติงานได้อย่างถูกต้องและเป็นไปตามนโยบายเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร ดังนี้

- เมื่อกิจกรรมจำเป็นต้องดำเนินการในลักษณะเดียวกันโดยหลายบุคคล
- เมื่อกิจกรรมนั้นมีความถี่ในปฏิบัติงานน้อย
- เมื่อกิจกรรมนั้นเป็นกิจกรรมใหม่และก่อความเสี่ยงหากดำเนินการไม่ถูกต้อง
- เมื่อต้องส่งมอบกิจกรรมนั้นให้กับพนักงานใหม่ บุคคลอื่น หรือหน่วยงานอื่น

1.14.2. การจัดทำเอกสารขั้นตอนการปฏิบัติงานสำหรับกิจกรรมการดำเนินงานขององค์กรที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ ควรมีการระบุถึงผู้รับชอบ วิธีการติดตั้ง หรือการกำหนดการตั้งค่าระบบที่ปลอดภัย การประมวลผลและการจัดการสารสนเทศทั้งแบบอัตโนมัติและ Manual มาตรการการรักษาความปลอกภัย ข้อแนะนำ เงื่อนไขต่างๆ ช่องทางการติดต่อฝ่ายสนับสนุนทั้งภายในและภายนอกบริษัทฯ เป็นต้น

1.14.3. หน่วยงานในฝ่ายดิจิทัลเทคโนโลยี ต้องจัดทำคู่มือ เอกสารประกอบระบบงาน และฐานข้อมูลความรู้ เพื่อให้ผู้ที่เกี่ยวข้องมีความเข้าใจระบบงาน ลักษณะงาน และกระบวนการทำงาน

1.14.4. หน่วยงานในฝ่ายดิจิทัลเทคโนโลยี ต้องทบทวนวิธีปฏิบัติ คู่มือ เอกสารประกอบระบบงานและฐานข้อมูลความรู้ให้เป็นปัจจุบันอยู่เสมอ รวมทั้งจัดให้ขั้นตอนปฏิบัติงานดังกล่าวอยู่ในสภาพที่พร้อมใช้งานและเข้าถึงได้ และต้องสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบและปฏิบัติตาม

1.14.5. ฝ่ายดิจิทัลเทคโนโลยีต้องควบคุม กำกับให้มีการจัดการควบคุมการเปลี่ยนแปลงของการเปลี่ยนแปลงโครงสร้างองค์กร ขั้นตอนการปฏิบัติงาน ระบบสารสนเทศ เพื่อควบคุมก่อนการเปลี่ยนแปลง แก้ไข หรือกระทำการใดๆ ซึ่งส่งผลต่อการดำเนินงานของระบบงานต่างๆ ทั้งนี้ให้ปฏิบัติตามที่กำหนดไว้ใน การบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ (Change Management Policy)

หมวดที่ 2 นโยบายความปลอดภัยด้านทรัพยากรบุคคล (Human Resource Security)

ส่วนที่ 2.1 การรักษาความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resources Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม การกำกับ และติดตามการสรรหาบุคลากรเข้ามาปฏิบัติงานภายในองค์กร การบริหารจัดการบุคลากรระหว่างการจ้างงาน และการบริหารจัดการบุคลากรเมื่อพ้นสภาพการเป็นลูกจ้างหรือเมื่อมีการเปลี่ยนแปลงหน้าที่การปฏิบัติงาน

2.1.1. การบริหารจัดการบุคลากรก่อนการจ้างงาน (Prior to Employment)

1) การตรวจสอบประวัติ (Screening) องค์กรต้องกำหนดให้มีการตรวจสอบประวัติของผู้สมัครงานและหน่วยงานภายนอกที่ต้องเข้ามาให้บริการภายในหน่วยงาน
2) ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and Conditions of Employment) ฝ่ายบริหารทรัพยากรบุคคล ต้องกำกับให้มีการลงนามในสัญญาจ้างหรือข้อตกลงการปฏิบัติงานของบุคลากร หรือสัญญาว่าจ้างหน่วยงานหรือบุคคลภายนอก ซึ่งได้มีการระบุหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศไว้ในสัญญาหรือข้อตกลงการปฏิบัติงาน ซึ่งผู้ใช้งานต้องรับทราบและยอมรับระเบียบปฏิบัติขององค์กร โดยจะต้องอ่านทำความเข้าใจและปฏิบัติตามนโยบาย กฎระเบียบที่องค์กรได้กำหนดไว้
3) ในสัญญาจ้าง หรือข้อตกลงการปฏิบัติงานของพนักงาน สัญญาว่าจ้างหน่วยงาน หรือบุคคลภายนอก ให้ระบุหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศ และสัญญาไม่เปิดเผยความลับของหน่วยงาน (Non-Discloser Agreement : NDA) โดยให้สอดคล้องกับนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ และระเบียบปฏิบัติที่กำหนดไว้

2.1.2. ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or Non-Disclosure Agreements)

1) ผู้บริหารระดับฝ่าย ต้องจัดให้บุคลากรและหน่วยงานภายนอกที่ปฏิบัติงานให้องค์กร มีการทำสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลขององค์กรอย่างเป็นลายลักษณ์อักษร รวมถึงการลงนามจรรยาบรรณการทำงานของคู่ค้าศุภาลัย
2) ข้อตกลงการรักษาความลับต้องครอบคลุมไปจนถึงการรักษาความลับหลังจากสิ้นสุดสัญญา และจัดทำเป็นลายลักษณ์อักษร

2.1.3. การบริหารจัดการบุคลากรระหว่างการจ้างงาน (During employment)

1) หน้าที่ในการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (Management Responsibilities) ผู้บริหารระดับฝ่ายต้องกำหนดให้มีการควบคุม และกำกับให้บุคลากร หรือหน่วยงานภายนอกที่ได้รับการว่าจ้างเพื่อปฏิบัติงานหรือให้บริการกับองค์กร ปฏิบัติงานตามนโยบายเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่องค์กรได้ประกาศใช้

2) การอบรมการสร้างความตระหนัก การให้ความรู้ในเรื่องที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness, Education and Training)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดช่องทางให้บุคลากรสามารถทำการศึกษาและทำความเข้าใจในนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ บทบาท และหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยของตนเองก่อนที่จะอนุญาตให้เริ่มต้นปฏิบัติงานกับองค์กร
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องจัดให้มีการอบรมที่เกี่ยวข้องกับการปฏิบัติงานทั่วไปโดยหน่วยงานผู้รับผิดชอบ เพื่อให้ผู้รับการว่าจ้างได้เรียนรู้และทำความเข้าใจในหัวข้อเหล่านั้นอย่างสม่ำเสมอ เช่น วิธีการใช้ระบบงาน วิธีการใช้งานซอฟต์แวร์สำเร็จรูป การแก้ปัญหาการใช้คอมพิวเตอร์เบื้องต้น การปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับที่เกี่ยวข้อง เป็นต้น
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องจัดการอบรมและสร้างความตระหนักด้านความมั่นคงปลอดภัยเพื่อให้ผู้รับการว่าจ้างได้เรียนรู้และทำความเข้าใจในหัวข้อเหล่านั้นอย่างสม่ำเสมอ เพื่อช่วยให้ผู้รับการว่าจ้างสามารถปฏิบัติงานที่ตนเองรับผิดชอบได้เป็นอย่างดีและอย่างมั่นคงปลอดภัย

3) ทุกหน่วยงานของบริษัทฯ ต้องควบคุมดูแลให้บุคลากร และผู้ให้บริการภายนอก ปฏิบัติตามกฎระเบียบที่กำหนดไว้อย่างเคร่งครัด

4) กระบวนการลงโทษทางวินัย (Disciplinary Process) องค์กรต้องจัดให้มีกระบวนการลงโทษทางวินัย เพื่อลงโทษผู้ใช้งานที่ฝ่าฝืนหรือละเมิดนโยบายเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หรือขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

2.1.4. การสิ้นสุดการจ้างงานหรือโยกย้ายตำแหน่งงาน (Termination or Change of Employment)

1) การบริหารจัดการบุคลากรพ้นสภาพหรือเปลี่ยนหน้าที่ความรับผิดชอบในการปฏิบัติงาน (Termination or Change of Employment Responsibilities)
   - ฝ่ายบริหารทรัพยากรบุคคล ต้องกำหนดกฎระเบียบและความรับผิดชอบที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคลากร และหน่วยงานภายนอกภายหลังจากที่พ้นสภาพการจ้างงาน หรือมีการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน อย่างเป็นลายลักษณ์อักษร

ส่วนที่ 2.2 การปฏิบัติงานจากระยะไกล (Remote working)

วัตถุประสงค์

เพื่อให้มั่นใจว่าการปฏิบัติการจากภายนอกองค์กรหรือการใช้งานอุปกรณ์พกพามีความปลอดภัยเพียงพอ

2.2.1. การปฏิบัติงานภายนอกสำนักงาน (Teleworking)

1) ผู้ใช้งานที่มีการทำงานจากภายนอกสำนักงานทั้งหมด จะต้องปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กรเช่นเดียวกันกับการทำงานภายในสำนักงาน
2) ผู้ใช้งานที่มีการใช้ข้อมูลสารสนเทศขององค์กรในการทำงานนอกสำนักงาน หรือการเข้าสู่ระบบผ่านทางไกล (Remote Access) ต้องได้รับอนุญาตจากเจ้าของข้อมูลสารสนเทศ และหน่วยงานต้นสังกัดโดยต้องมีเหตุผลอันควร
3) ผู้ใช้งานที่ต้องการเข้าสู่ระบบผ่านทางไกล (Remote Access) ต้องได้รับอนุญาตจากผู้ดูแลระบบก่อนเข้าใช้งาน

ส่วนที่ 2.3 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย (Reporting Information Security Events)

วัตถุประสงค์

เพื่อสนับสนุนการรายงานเหตุการณ์ด้านการรักษาความปลอดภัยของสารสนเทศอย่างทันท่วงที สม่ำเสมอ และมีประสิทธิภาพ

2.3.1. การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย (Reporting Information Security Events)

1) ผู้ใช้งานและหน่วยงานภายนอกต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศขององค์กรต่อผู้บังคับบัญชาและฝ่ายดิจิทัลเทคโนโลยี โดยผ่านช่องทางการรายงานที่กำหนดไว้และจะต้องดำเนินการรายงานอย่างรวดเร็วที่สุด

2.3.2. การรายงานจุดอ่อนด้านความมั่นคงปลอดภัย (Reporting Information Security Weaknesses)

1) ผู้ใช้งานและหน่วยงานภายนอกต้องรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศขององค์กรต่อผู้บังคับบัญชาและฝ่ายดิจิทัลเทคโนโลยี โดยผ่านช่องทางการรายงานที่กำหนดไว้และจะต้องดำเนินการรายงานอย่างรวดเร็วที่สุด
2) ผู้ใช้งานและหน่วยงานภายนอกที่พบเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศหรือจุดอ่อนใดๆของระบบสารสนเทศในองค์กร ต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้นผู้บังคับบัญชาและฝ่ายดิจิทัลเทคโนโลยี และห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศนั้นด้วยตนเอง

หมวดที่ 3 นโยบายความมั่นคงปลอดภัยทางกายภาพ (Physical Controls)

ส่วนที่ 3.1 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environment Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการป้องกัน ควบคุมการใช้งานและการบำรุงรักษาด้านกายภาพของทรัพย์สินสารสนเทศและอุปกรณ์สารสนเทศซึ่งเป็นโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบสารสนเทศขององค์กร ให้อยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้ รวมถึงป้องกันการเข้าถึงทรัพย์สินสารสนเทศหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

3.1.1. พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure Area)

1) ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical Security Perimeter) องค์กรจะต้องพิจารณาและจัดทำพื้นที่ที่ต้องการรักษาความปลอดภัยโดยจะประกอบด้วยพื้นที่กั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทางเข้า-ออกหลัก และระบบรักษาความปลอดภัยอย่างเหมาะสม
2) การควบคุมการเข้าออกทางกายภาพ (Physical Entry Controls)
    - องค์กรต้องควบคุมการเข้าถึงพื้นที่ปฏิบัติงานและพื้นที่ซึ่งมีข้อมูลสำคัญให้เข้าถึงได้เฉพาะบุคลากรผู้ได้รับอนุญาตเท่านั้น
    - รายชื่อผู้ได้รับอนุญาตให้เข้าถึงพื้นที่ปฏิบัติงานและพื้นที่ซึ่งมีข้อมูลสำคัญต้องได้รับการตรวจสอบ ปรับปรุง และดูแลให้เหมาะสมอย่างสม่ำเสมอ
    - ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดให้มีการควบคุมการเข้าออกพื้นที่ที่ต้องการรักษาความปลอดภัย (Secure Area) ได้แก่ ห้องคอมพิวเตอร์ รวมถึงพื้นที่ปฏิบัติงานของผู้ดูแลระบบ โดยต้องกำหนดให้เฉพาะผู้มีสิทธิ์ที่สามารถเข้าออกได้ และมีการเก็บบันทึกการเข้าออกห้องคอมพิวเตอร์ และบันทึกการเข้าออกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล เวลาผ่านเข้าออก วัตถุประสงค์การผ่านเข้าออก รวมถึงต้องมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ
3) การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ (Securing Offices, Rooms, and Facilities)
    - ฝ่ายดิจิทัลเทคโนโลยี ต้องออกแบบและติดตั้งระบบการรักษาความมั่นคงปลอดภัยทางกายภาพ เพื่อป้องกันพื้นที่ปฏิบัติงานและพื้นที่ซึ่งมีข้อมูลสำคัญ ห้องคอมพิวเตอร์ และพื้นที่ปฏิบัติงานของผู้ดูแลระบบหรืออุปกรณ์สารสนเทศต่างๆ ที่ใช้ในการปฏิบัติงานอันเนื่องจากการได้รับความเสียหายและถูกเข้าถึงโดยไม่ได้รับอนุญาต
4) การตรวจสอบการรักษาความปลอดภัยทางกายภาพ (Physical security monitoring)
    - ต้องมีการตรวจสอบเฝ้าระวังพื้นที่ การเข้าถึงอาคาร หรือพื้นที่ที่มีระบบงานสำคัญ โดยให้มีสัญญาณเตือนแจ้งเหตุ ระบบเฝ้าระวัง หรือจัดให้มีเจ้าหน้าที่รักษาความปลอดภัย

- ติดตั้งระบบเฝ้าระวัง เช่น กล้องวงจรปิด (CCTV) เพื่อบันทึกข้อมูลการเข้าออกพื้นที่บริเวณภายในและภายนอกสถานที่ปฏิบัติงาน
- ดำเนินการทดสอบเครื่องมือเฝ้าระวังการตรวจจับต่าง ๆ ให้พร้อมใช้งาน เพื่อให้สามารถส่งสัญญาณเตือนเมื่อมีผู้บุกรุก

5) การป้องกันภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting Against External end Environmental Threats)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องควบคุม กำกับให้มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันภัยคุกคามจากภายนอก ทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติ เช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น
6) การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in Secure Areas)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องกำกับให้มีการกำหนดแนวปฏิบัติของการป้องกันทางกายภาพสำหรับการปฏิบัติงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure Area) ได้แก่ ห้องคอมพิวเตอร์ และพื้นที่ปฏิบัติงานของผู้ดูแลระบบ และกำหนดให้มีการนำแนวปฏิบัติไปใช้งานอย่างเคร่งครัด
7) พื้นที่สำหรับรับส่งสิ่งของ (Delivery and Loading Areas)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดให้มีการควบคุมบริเวณที่ผู้ไม่มีสิทธิ์เข้าถึงอาจสามารถเข้าถึงได้ โดยต้องกำหนดพื้นที่การส่งมอบสินค้าและพื้นที่การเตรียมหรือประกอบอุปกรณ์สารสนเทศก่อนนำเข้าห้องคอมพิวเตอร์ ทั้งนี้ให้แยกเป็นสัดส่วนที่ชัดเจนเพื่อหลีกเลี่ยงการเข้าถึงระบบสารสนเทศและข้อมูลสารสนเทศโดยผู้ที่ไม่ได้รับอนุญาต

3.1.2. อุปกรณ์ (Equipment)

1) การจัดวางและการป้องกันอุปกรณ์ (Equipment Setting and Protection)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องจัดวางอุปกรณ์สารสนเทศไว้ในห้อง หรือบริเวณที่ปลอดภัยอุปกรณ์ที่มีตู้ ประตูของตู้วางคอมพิวเตอร์แม่ข่ายและอุปกรณ์สื่อสารเครือข่ายต้องถูกล็อคอยู่เสมอ โดยกำหนดให้มีเพียงเจ้าหน้าที่ผู้ที่ได้รับอนุญาตเท่านั้นที่มีสิทธิ์ในการเปิดเพื่อซ่อมบำรุงหรือการปรับปรุงการตั้งค่าของระบบ (Reconfiguration) เพื่อลดความเสี่ยงจากการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต
2) ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)
   - ฝ่ายดิจิทัลเทคโนโลยี จะต้องควบคุมดูแลให้มีการติดตั้งอุปกรณ์ป้องกันการล้มเหลวของระบบและอุปกรณ์สนับสนุนการทำงานต่างๆ ภายในห้องคอมพิวเตอร์ ได้แก่ อุปกรณ์ดับเพลิง อุปกรณ์ดักจับควันไฟ อุปกรณ์สำรองไฟฟ้า ระบบควบคุมอุณหภูมิและความชื้น ระบบเตือนภัยน้ำรั่วหรือระบบแจ้งเตือนเมื่ออุปกรณ์สารสนเทศทำงานผิดปกติ เป็นต้น และต้องบำรุงดูแลรักษาอุปกรณ์ให้พร้อมใช้งานอยู่เสมอ

3) ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling Security)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องควบคุมดูแลให้การติดตั้งและการบำรุงรักษาสายไฟฟ้าและสายสื่อสารในพื้นที่ปฏิบัติงานและห้องคอมพิวเตอร์เป็นไปตามมาตรฐานความปลอดภัยอุตสาหกรรมเพื่อป้องกันไม่ให้มีการเข้าถึงหรือดักจับข้อมูล หรือเกิดความเสียหายทางด้านกายภาพ
4) การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องควบคุมดูแลให้อุปกรณ์ระบบสารสนเทศหลักทั้งหมดซึ่งใช้ในการประมวลผลในระดับปฏิบัติการ รวมถึงอุปกรณ์สนับสนุนการทำงานได้รับการบำรุงดูแลรักษาตามช่วงเวลาและตามข้อกำหนดที่ผู้ผลิตแนะนำ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้งาน
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องควบคุมให้มีการบันทึกบันทึกกิจกรรมการบำรุงอุปกรณ์ รวมถึงบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ให้อยู่ในสภาพพร้อมใช้งานเสมอ
5) การนำทรัพย์สินสารสนเทศออกนอกสำนักงาน (Removal of Assets)
   - ผู้ทำหน้าที่กำกับดูแลพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยและอาคารสถานที่ต้องไม่อนุญาตให้นำอุปกรณ์สารสนเทศออกจากองค์กร ยกเว้นจะมีการอนุญาตให้นำออกโดยผู้ที่ได้รับมอบหมายในการอนุญาตให้นำทรัพย์สินออก
   - ผู้ใช้งานต้องไม่นำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกนอกองค์กร ยกเว้นจะได้รับอนุญาตจากผู้ที่ได้รับมอบหมายในการอนุญาตให้นำทรัพย์สินออก
   - ฝ่ายดิจิทัลเทคโนโลยีต้องกำหนดขั้นตอนปฏิบัติสำหรับการนำทรัพย์สินออกนอกสำนักงานอย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม
6) ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน (Security of Equipment and Asset Off - Permission)
   - กำหนดให้ผู้บริหารระดับฝ่ายขึ้นไป เป็นผู้มีอำนาจในการอนุญาตให้นำอุปกรณ์สารสนเทศขององค์กรไปใช้งานภายนอกสำนักงาน และต้องกำหนดให้มีการป้องกันอุปกรณ์สารสนเทศต่างๆ ที่ใช้งานอยู่ภายนอกสำนักงานเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์ โดยพิจารณาจากความเสี่ยงที่อาจเกิดขึ้นกับอุปกรณ์เหล่านั้น
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดมาตรการความมั่นคงปลอดภัยในการควบคุมทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน เพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินขององค์กรออกไปใช้งาน
7) การป้องกันอุปกรณ์ที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended User Equipment)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดมาตรการควบคุมการป้องกันเครื่องคอมพิวเตอร์และอุปกรณ์สารสนเทศที่ทิ้งไว้โดยไม่มีผู้ดูแล เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลที่ไม่ได้รับอนุญาต

- ผู้ดูแลระบบ ต้องกำหนดให้ผู้ใช้งานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์
- ผู้ใช้งานต้องออกจากระบบสารสนเทศ ระบบงานคอมพิวเตอร์ที่ใช้งาน หรือเครื่องคอมพิวเตอร์โดยทันทีเมื่อไม่มีความจำเป็นต้องใช้งาน หรือเมื่อเสร็จสิ้นการปฏิบัติงาน
- ผู้ใช้งานต้องล็อคหน้าจอเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือเมื่อออกห่างจากเครื่องคอมพิวเตอร์

8) นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)
   - ผู้ดูแลระบบต้องกำกับและควบคุมให้มีการล็อกหน้าจอคอมพิวเตอร์โดยอัตโนมัติเมื่อไม่มีการใช้งาน ภายในระยะเวลาไม่เกิน 15 นาที รวมถึงให้มีการตั้งค่าการตัดออกจากระบบ (Session Timeout) เพื่อป้องกันการเข้าถึงข้อมูลหรือระบบโดยมิได้รับอนุญาต
   - ผู้ใช้งานต้องไม่ละเลยข้อมูลสารสนเทศที่สำคัญ เช่น เอกสารกระดาษ หรือสื่อบันทึกข้อมูล ให้อยู่ในสถานที่ไม่ปลอดภัย พื้นที่สาธารณะ หรือสถานที่ที่พบเห็นได้โดยง่าย ผู้ใช้งานต้องจัดเก็บข้อมูลสารสนเทศในสถานที่ที่เหมาะสม รวมถึงมีการป้องกันเพื่อให้ยากต่อการเข้าถึงของผู้ไม่มีสิทธิ์
   - ผู้ใช้งานต้องไม่จัดเก็บข้อมูลสำคัญไว้บนหน้าเดสท็อป (Desktop) ของเครื่องคอมพิวเตอร์ โดยผู้ใช้งานต้องจัดสรรพื้นที่ในการจัดเก็บข้อมูลในเครื่องคอมพิวเตอร์และควบคุมการเข้าถึงอย่างเหมาะสม เพื่อป้องกันผู้อื่นเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

3.1.3. การจัดการสื่อบันทึกข้อมูล (Media Handling)

1) การบริหารจัดการสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ (Management of Removable Media)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องจัดทำขั้นตอนการปฏิบัติงานสำหรับการบริหารจัดการสื่อที่ใช้ในการบันทึกข้อมูลสารสนเทศที่เคลื่อนย้ายได้อย่างเป็นลายลักษณ์อักษรและปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม
   - การบริหารจัดการสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ ต้องมีความสอดคล้องกับการกำหนดลำดับชั้นความลับข้อมูล
2) การทำลายสื่อบันทึกข้อมูล (Disposal of Media)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องจัดทำขั้นตอนปฏิบัติการทำลายสื่อบันทึกข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูล ที่เป็นความลับหรือมีความสำคัญ
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดมาตรการควบคุมการทำลายสื่อบันทึกข้อมูลโดยอ้างอิงมาตรฐานซึ่งเป็นที่ยอมรับในสากล

3) การเคลื่อนย้ายสื่อบันทึกข้อมูล (Physical Media Transfer)
   - ฝ่ายดิจิทัลเทคโนโลยีต้องกำหนดขั้นตอนปฏิบัติงาน หรือข้อกำหนดในการดูแลรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ในกรณีที่มีการเคลื่อนย้ายสื่อบันทึกข้อมูลออกจากพื้นที่ติดตั้งหรือพื้นที่ปฏิบัติงาน

3.1.4. ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์กลับมาใช้งานซ้ำ (Secure Disposal or Re-Use of Equipment)

ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อให้มั่นใจว่าข้อมูลสารสนเทศที่สำคัญหรือซอฟต์แวร์ลิขสิทธิ์ที่อยู่ภายในสื่อบันทึกข้อมูลได้มีการลบ ย้าย หรือทำลายอย่างเหมาะสมตามลำดับชั้นความลับข้อมูล ก่อนที่จะทำลายหรือจำหน่ายอุปกรณ์หรือนำอุปกรณ์กลับมาใช้ใหม่

หมวดที่ 4 นโยบายความมั่นคงปลอดภัยทางด้านเทคโนโลยี (Technological Controls)

ส่วนที่ 4.1 การรักษาความมั่นคงปลอดภัยสำหรับอุปกรณ์ที่ใช้ปฏิบัติงานหรืออุปกรณ์ของผู้ใช้งาน (User Endpoint Device Security Policy)

วัตถุประสงค์

เพื่อป้องกันสารสนเทศไม่ให้เกิดความเสี่ยงจากการใช้อุปกรณ์ปลายทางของผู้ใช้ (Endpoint Devices) ทุกประเภทที่ใช้ในการเข้าถึง เช่น คอมพิวเตอร์ตั้งโต๊ะ (Desktop) คอมพิวเตอร์พกพา (Laptop/Notebook) อุปกรณ์พกพา (Mobile Device, Tablet) โทรศัพท์มือถือที่ใช้ปฏิบัติงาน อุปกรณ์เสริมที่จัดเก็บข้อมูล เช่น External Drive, USB, Portable Storage อุปกรณ์ส่วนบุคคลที่อนุญาตให้ใช้ปฏิบัติงาน (BYOD) เป็นต้น รวมถึงอุปกรณ์ของบุคลากร ผู้รับจ้าง และบุคคลภายนอกที่ได้รับอนุญาตให้เชื่อมต่อกับเครือข่ายหรือระบบขององค์กร

4.1.1. การรักษาความมั่นคงปลอดภัยสำหรับอุปกรณ์ที่ใช้ปฏิบัติงานหรืออุปกรณ์ของผู้ใช้งาน (User Endpoint Device Security

1) การอนุญาตและการขึ้นทะเบียนอุปกรณ์
   - อุปกรณ์ทุกเครื่องที่ใช้เข้าถึงข้อมูลหรือระบบขององค์กรต้องผ่านการอนุมัติจากฝ่ายดิจิทัลเทคโนโลยีก่อนนำไปใช้งาน
   - ต้องมีการขึ้นทะเบียนอุปกรณ์ (Asset Inventory) และบันทึกข้อมูลสำคัญ เช่น ผู้ครอบครอง หมายเลขประจำเครื่อง ระบบปฏิบัติการ และสถานะการรักษาความปลอดภัย
2) การกำหนดค่าความมั่นคงปลอดภัย (Secure Configuration)
   - อุปกรณ์ทุกเครื่องต้องถูกกำหนดค่าความปลอดภัยตามมาตรฐานขององค์กร เช่น การปิดบริการที่ไม่จำเป็น การตั้งค่ารหัสผ่านให้มีความแข็งแรง การเปิดใช้งาน Firewall และการปรับตั้งค่าความปลอดภัยของระบบปฏิบัติการให้เหมาะสม
   - ผู้ใช้งานห้ามดัดแปลง ปิดการป้องกัน หรือติดตั้งซอฟต์แวร์ใด ๆ ที่ไม่ได้รับอนุมัติจากองค์กรเด็ดขาด

3) การควบคุมการเข้าถึง (Access Control)
   - อุปกรณ์ต้องตั้งค่ารหัสผ่านหรือกลไกการยืนยันตัวตนที่แข็งแรง และต้องตั้งค่าให้ล็อกอัตโนมัติเมื่อไม่มีการใช้งานในระยะเวลาที่กำหนด
   - การเข้าถึงระบบที่มีความสำคัญต้องใช้การพิสูจน์ตัวตนหลายปัจจัย (MFA) เพื่อเพิ่มความปลอดภัยผู้ใช้งาน ห้ามแชร์บัญชีหรือรหัสผ่าน กับบุคคลอื่นไม่ว่ากรณีใด
4) การปกป้องข้อมูล (Data Protection)
   - อุปกรณ์ทุกเครื่องที่มีการจัดเก็บข้อมูลขององค์กรควรเปิดใช้ระบบเข้ารหัสเต็มดิสก์ (Full-disk Encryption) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
   - ข้อมูลสำคัญต้องจัดเก็บในระบบที่ได้รับอนุมัติ เช่น Cloud หรือ File Server ขององค์กร ห้ามจัดเก็บข้อมูลสำคัญบนอุปกรณ์ส่วนบุคคลหรือพื้นที่ที่ไม่ได้รับอนุญาต
5) ซอฟต์แวร์และอัปเดตความปลอดภัย
   - อุปกรณ์ต้องติดตั้งเฉพาะซอฟต์แวร์และแอปพลิเคชันที่ได้รับการอนุมัติจากฝ่ายดิจิทัลเทคโนโลยีเท่านั้น
   - ระบบปฏิบัติการ (OS) โปรแกรมป้องกันไวรัส และแพตช์ความปลอดภัยต้องได้รับการอัปเดตอย่างสม่ำเสมอตามรอบที่กำหนดอุปกรณ์ต้องเปิดใช้งานระบบตรวจจับและป้องกันมัลแวร์ตลอดเวลาเพื่อป้องกันภัยคุกคามที่อาจเกิดขึ้น
6) การเชื่อมต่อเครือข่าย (Network Security)
   - อุปกรณ์ต้องเชื่อมต่อกับเครือข่ายขององค์กรผ่านช่องทางที่ปลอดภัย เช่น VPN ที่องค์กรกำหนดห้ามเชื่อมต่อกับเครือข่าย Wi-Fi สาธารณะที่ไม่มีการเข้ารหัสหรือมีความเสี่ยงต่อการถูกดักจับข้อมูล
   - อุปกรณ์ต้องผ่านการตรวจสอบและยืนยันความปลอดภัยก่อนอนุญาตให้เข้าถึงระบบขององค์กร (Network Access Control)
7) การป้องกันอุปกรณ์สูญหายหรือถูกขโมย
   - ผู้ใช้งานต้องรักษาอุปกรณ์ให้อยู่ในความดูแลอย่างเหมาะสม และห้ามปล่อยให้อุปกรณ์อยู่โดยลำพังในสถานที่ที่ไม่ปลอดภัย หากอุปกรณ์สูญหายหรือถูกขโมย ผู้ใช้งานต้องแจ้งผู้บังคับบัญชาฝ่ายงานและฝ่ายดิจิทัลเทคโนโลยีทันที เพื่อให้สามารถดำเนินมาตรการควบคุมความเสี่ยงได้ เช่น ระงับบัญชีผู้ใช้งานหรือสั่งลบข้อมูลจากระยะไกล

4.1.2. การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานภายนอกองค์กร (Mobile Computing and Teleworking)

1) การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile Computing and Communication)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดให้มีมาตรการที่เหมาะสมเพื่อรับรองความปลอดภัยของอุปกรณ์สื่อสารประเภทพกพา โดยพิจารณาจากความเสี่ยงที่มีการนำอุปกรณ์เข้ามาเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ขององค์กร และเมื่อนำอุปกรณ์ออกไปใช้งานนอกสถานที่

- ผู้ใช้งานที่มีการใช้งานอุปกรณ์สื่อสารประเภทพกพาเพื่อเชื่อมต่อกับระบบสารสนเทศขององค์กรทั้งหมดต้องปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และตระหนักถึงการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด
- ผู้ใช้งานต้องระมัดระวังไม่ให้บุคคลอื่นมองเห็นข้อมูลบนหน้าจอในที่สาธารณะ (Screen Privacy)

4.1.3. การใช้งานอุปกรณ์ส่วนบุคคล (Bring Your Own Device : BYOD)

1) ไม่อนุญาตให้บุคลากรนำอุปกรณ์เคลื่อนที่หรือคอมพิวเตอร์แบบพกพาส่วนบุคคลมาใช้ในการปฏิบัติงานขององค์กรโดยไม่ได้รับอนุญาต
2) อุปกรณ์ส่วนบุคคลที่นำมาใช้ปฏิบัติงานต้องปฏิบัติตามมาตรการความมั่นคงปลอดภัยเช่นเดียวกับอุปกรณ์ขององค์กร
3) องค์กรมีสิทธิ์ติดตั้งระบบควบคุมด้านความมั่นคงปลอดภัย เช่น ระบบ MDM และลบข้อมูลขององค์กรในอุปกรณ์ส่วนบุคคล หากมีความจำเป็นด้านความปลอดภัย ผู้ใช้งานต้องลงนามยินยอมในการปฏิบัติตามเงื่อนไข BYOD ก่อนการใช้งานจริง

ส่วนที่ 4.2 การบริหารจัดการสิทธิ์การเข้าถึง (Access Right Management Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางในการจัดการสิทธิ์การเข้าถึงข้อมูล ระบบงานสารสนเทศ และทรัพยากรต่างๆ ขององค์กร ให้มั่นใจว่าผู้ใช้งานได้รับสิทธิ์ที่เหมาะสมตามหน้าที่ความรับผิดชอบ และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต โดยครอบคลุมผู้ใช้งานภายในและผู้ใช้งานภายนอก ที่ได้รับสิทธิ์เข้าถึงข้อมูล ทรัพยากร หรือระบบงานสารสนเทศขององค์กร

4.2.1. การจัดการสิทธิ์การเข้าถึงในระดับสิทธิ์พิเศษ (Privileged access rights)

1) การจัดการบัญชีผู้ใช้ระดับสิทธิ์พิเศษ (Privileged Account Management)
   - ฝ่ายดิจิทัลเทคโนโลยี มีหน้าที่ในการกำหนดกระบวนการจัดการและควบคุมสิทธิ์การเข้าถึงที่มีสิทธิ์สูง (Privileged Access Rights) เพื่อป้องกันการละเมิดข้อมูล การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และกำหนดการบริหารจัดการสิทธิ์การเข้าถึง เปลี่ยนแปลงหรือยกเลิกการใช้งาน ระบบหรืออุปกรณ์สารสนเทศเฉพาะผู้มีสิทธิ์สูง (Privileged Access Rights) ตามความจำเป็นต่อการใช้งานเท่านั้น
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดขั้นตอนปฏิบัติงานสำหรับการบริหารจัดการรหัสผู้ใช้งานที่มีสิทธิ์ระดับสูงอย่างเป็นลายลักษณ์อักษร รวมถึงสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบและปฏิบัติตาม
   - ต้องกำหนดสิทธิ์ตามหลัก Least Privilege และ Need-to-Use เท่านั้น และห้ามให้สิทธิ์ระดับสูงเป็นการถาวรหากไม่จำเป็น โดยควรใช้วิธี Just-in-Time Access (JIT) หรือการมอบสิทธิ์ชั่วคราวสำหรับงานเฉพาะกิจ

- กำหนดให้ต้องมีการพิสูจน์ตัวตนในการเข้าใช้งานระบบเพื่อให้เกิดความมั่นคงปลอดภัย และมีการตรวจติดตามการใช้งานตามกำหนดระยะเวลาการใช้งานตามที่กำหนด
- บัญชีที่มีสิทธิ์ระดับสูงต้องถูกสร้าง แยกประเภท และควบคุมอย่างชัดเจน เช่น บัญชีทั่วไป (Normal User) และบัญชี Admin ต้องแยกออกจากกัน
- ห้ามใช้บัญชีระดับสูงสำหรับงานทั่วไป เช่น การใช้งานอินเทอร์เน็ต การอ่านอีเมล หรือการทำงานพื้นฐาน
- บัญชี Service Account, API Account, Automation Account ต้องถูกควบคุม ตรวจสอบ และเก็บรหัสผ่านอย่างปลอดภัย

2) การยืนยันตัวตนและความปลอดภัยของบัญชี (Authentication & Protection)
   - บัญชีระดับสิทธิ์สูงต้องใช้การพิสูจน์ตัวตนหลายปัจจัย (MFA) โดยรหัสผ่านต้องมีความซับซ้อนและเป็นไปตามนโยบาย Password Policy ขององค์กร
   - ต้องมีการหมุนเวียนรหัสผ่าน หรือเปลี่ยนรหัสทันทีเมื่อพบความเสี่ยงด้านความปลอดภัย
   - สำหรับงานที่มีความเสี่ยงสูง ควรใช้ระบบ PAM (Privileged Access Management) เพื่อควบคุมและบันทึกการใช้งาน
3) การใช้งานบัญชีระดับสูง (Usage Control)
   - การใช้งานสิทธิ์ระดับสูงต้องกระทำเฉพาะกรณีจำเป็น และต้องมีเหตุผลประกอบอย่างชัดเจน โดยเฉพาะงานสำคัญ เช่น การเปลี่ยนค่าตั้งระบบ การลบข้อมูล การเพิ่มผู้ใช้ หรือการปรับสิทธิ์ ต้องมีการบันทึกคำสั่งและจัดเก็บเป็นหลักฐาน
   - การเข้าถึงเพื่อแก้ไขปัญหาเฉพาะหน้า ต้องมีการบันทึกเหตุผลและระยะเวลาการใช้งาน
   - เมื่อผู้ใช้ไม่มีความจำเป็นต้องใช้งานสิทธิ์ระดับสูง สิทธิ์ทั้งหมดต้องถูกยกเลิกในทันที
4) การบริหารจัดการรหัสผู้ใช้งานที่มีสิทธิ์ระดับสูง (Management of Privileged Access Right)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องจัดเก็บรหัสผู้ใช้งานที่มีสิทธิ์ระดับสูง เช่น Administrator/ root บนเครื่องแม่ข่าย หรือ Administrator ของระบบ Application และให้มีการเบิกใช้งานตามความจำเป็นเท่านั้น
   - รหัสผ่านสำหรับบัญชีสิทธิ์สูง (Privileged Accounts) ต้องมีการเปลี่ยนอย่างน้อยทุก 90 วัน และต้องเปิดใช้งานการพิสูจน์ตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) หากมีความสามารถรองรับ ทั้งนี้ อาจพิจารณาปรับรอบระยะเวลาในการเปลี่ยนรหัสผ่านให้สอดคล้องกับระดับความเสี่ยงและความเหมาะสมของแต่ละระบบ
   - องค์กรสามารถสั่งเปลี่ยนรหัสผ่านได้ทันทีเมื่อพบความเสี่ยงด้านความมั่นคงปลอดภัย ไม่ว่าจะเป็นความเสี่ยงเชิงเทคนิค การปฏิบัติงาน หรือเหตุการณ์ใด ๆ ที่อาจก่อให้เกิดการเข้าถึงระบบหรือข้อมูลโดยไม่ได้รับอนุญาต ทั้งนี้ เพื่อป้องกันและลดผลกระทบที่อาจเกิดขึ้นต่อระบบและข้อมูลขององค์กร

4.2.2. การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้ (Management of Secret Authentication Information of Users)

1) ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดวิธีการบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้อย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอรวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม

4.2.3. การจำกัดการเข้าถึงข้อมูลสารสนเทศ (Information access restriction)

1) การควบคุมการเข้าถึงแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)
   - เจ้าของข้อมูลและผู้ดูแลระบบ ต้องกำหนดวิธีการเข้าถึงข้อมูล ระบบสารสนเทศและฟังก์ชั่นในระบบงาน โดยต้องมีการจำกัดให้สอดคล้องกับนโยบายควบคุมการเข้าถึง
   - เจ้าของข้อมูลและผู้ดูแลระบบ ต้องกำหนดวิธีการใช้งานระบบสารสนเทศที่สำคัญ ไม่ว่าจะเป็นข้อมูล ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของฝ่ายงานนั้นๆ เป็นลายลักษณ์อักษร
2) การเข้าสู่ระบบสารสนเทศที่มีความมั่นคงปลอดภัย (Secure Log-on Procedures)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดวิธีการเข้าสู่ระบบสารสนเทศที่มีความมั่นคงปลอดภัยอย่างเป็นลายลักษณ์อักษร โดยอ้างอิงวิธีการที่เป็นมาตรฐานสากลและปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม
3) การควบคุมการใช้โปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs)
   - ฝ่ายดิจิทัลฝ่ายเทคโนโลยี ต้องกำหนดให้มีการควบคุมการใช้โปรแกรมอรรถประโยชน์ และจำกัดการใช้งานโปรแกรมอรรถประโยชน์สำหรับระบบสารสนเทศ หรือโปรแกรมคอมพิวเตอร์ที่สำคัญ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้
4) การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Restrictions on Changes to Software Packages)
   - ซอฟต์แวร์สำเร็จรูปที่นำมาใช้งานในองค์กรควรใช้งานโดยปราศจากการแก้ไข หากในกรณีที่มีความจำเป็นต้องดำเนินการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำเร็จรูป หน่วยงานที่ได้รับมอบหมายให้ดำเนินการต้องพิจารณาการควบคุมการแก้ไขอย่างเข้มงวด
   - การเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำเร็จรูป ต้องดำเนินการเปลี่ยนแปลงตามขั้นตอนปฏิบัติการควบคุมการเปลี่ยนแปลงที่ฝ่ายดิจิทัลเทคโนโลยีกำหนดไว้

5) การจำกัดการเข้าถึงซอร์สโค้ด (Access to source code)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดมาตรการควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม และการนำซอร์สโค้ดของโปรแกรมไปใช้ในการพัฒนา เพื่อป้องกันการเกิดข้อผิดพลาดในการพัฒนาระบบสารสนเทศ และระบบงานขององค์กร

ส่วนที่ 4.3 การดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ (Operations Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมให้การดำเนินงาน การจัดการด้านการสื่อสารความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร มีแนวทางปฏิบัติที่มีขั้นตอนชัดเจนและมีความมั่นคงปลอดภัย

4.3.1. การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

1) การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)
   - ผู้ดูแลระบบต้องประเมินสมรรถภาพและความเพียงพอ(Capacity) ของทรัพยากรสารสนเทศ เช่น การใช้งานของเครื่องแม่ข่ายและอุปกรณ์เครือข่าย เช่น หน่วยประมวลผล(CPU) หน่วยความจำ(Memory) หน่วยจัดเก็บข้อมูล (Disk) หรือปริมาณการใช้งานระบบเครือข่าย(Bandwidth) เป็นต้น และต้องวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศให้ระบบสารสนเทศมีประสิทธิภาพที่เหมาะสม และเพียงพอต่อการใช้งานในอนาคต
   - ผู้ดูแลระบบ ต้องติดตามประสิทธิภาพการทำงานของระบบงานและอุปกรณ์สารสนเทศที่สำคัญให้ทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ และบันทึกการใช้ทรัพยากรอย่างต่อเนื่อง เช่น CPU, RAM, Storage, Network, Database Performance รวมถึงทรัพยากรบน Cloud
   - ต้องกำหนดค่าการแจ้งเตือน (Threshold Alerts) เมื่อการใช้ทรัพยากรเข้าใกล้ระดับวิกฤต เพื่อให้สามารถดำเนินการแก้ไขหรือเพิ่มขยายได้ทันเวลา
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องจัดทำรายงานด้านขีดความสามารถและประสิทธิภาพของระบบอย่างสม่ำเสมอ รวมถึงข้อมูลการใช้งานทรัพยากรต้องถูกนำมาวิเคราะห์ เพื่อใช้ประกอบการตัดสินใจด้านการลงทุนและการวางแผนระบบ

4.3.2. การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

1) มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls Against Malware)
   - ฝ่ายดิจิทัลเทคโนโลยีจะต้องกำหนดมาตรการสำหรับการตรวจจับ การป้องกันและการกู้คืนระบบเพื่อป้องกันทรัพย์สินจากซอฟต์แวร์ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานอย่างเหมาะสม
   - เครื่องคอมพิวเตอร์ของผู้ปฏิบัติงานต้องติดตั้งโปรแกรมป้องกันไวรัสหรือมัลแวร์ (Anti Malware Virus)
   - ข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใดที่ได้รับจากผู้ปฏิบัติงานอื่น ต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์ และโปรแกรมไม่พึงประสงค์ก่อนนำมาใช้งาน หรือเก็บบันทึกทุกครั้ง
   - เมื่อผู้ปฏิบัติงานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ปฏิบัติงานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่ระบบเครือข่าย และต้องแจ้งให้ผู้ดูแลระบบทราบ เพื่อทำการตรวจสอบแก้ไขทันที

4.3.3. การบริหารจัดการช่องโหว่ทางเทคนิคในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)

1) การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)
   - ผู้ที่ได้รับมอบหมายหรือผู้ดูแลระบบมีหน้าที่ในการติดตามช่องโหว่ทางเทคนิคและหาแนวทางป้องกันเพื่อนำเสนอดำเนินการ
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องควบคุมให้ระบบสารสนเทศขององค์กร ได้รับการพิสูจน์ถึงช่องโหว่ทางเทคนิคซึ่งอาจเกิดขึ้นได้ โดยให้ดำเนินการอย่างน้อยปีละ 1 ครั้ง
   - ผู้ดูแลระบบต้องดูแลและบำรุงรักษาระบบ เพื่อรักษาระดับความมั่นคงปลอดภัยด้านสารสนเทศของระบบอย่างสม่ำเสมอ ได้แก่ การตรวจสอบหาช่องโหว่ การประเมินความเสี่ยงของช่องโหว่ที่ตรวจสอบพบ และการปรับปรุงแก้ไขช่องโหว่ของระบบสารสนเทศ

4.3.4. การบริหารจัดการการกำหนดค่า (Configuration management)

1) การจัดทำและทบทวนมาตรฐานการกำหนดค่า Configurations
   - องค์กรต้องกำหนดค่าเริ่มต้น (Baseline Configuration) สำหรับฮาร์ดแวร์ ซอฟต์แวร์ เครือข่าย และบริการทั้งหมดที่สำคัญให้เป็นลายลักษณ์อักษร โดยการจัดทำและทบทวนมาตรฐานการกำหนดค่า Configurations ควรจะคำนึงถึงดังนี้
     - จำกัดจำนวนผู้ที่ได้สิทธิ์เป็นผู้ดูแลระบบ (Administrator) ให้น้อยที่สุด
     - ปิดสิทธิ์ของผู้ใช้งานที่ไม่มีความจำเป็น ไม่ได้ใช้งาน รวมถึงสิทธิ์ที่ไม่มีการดูแลรักษาความปลอดภัย
     - ปิดการใช้งานฟังก์ชั่นและบริการที่ไม่จำเป็น ไม่ได้ใช้งาน รวมถึงฟังก์ชั่นและบริการที่ไม่มีการดูแลรักษาความปลอดภัย
     - จำกัดการใช้งานโปรแกรมหรือพารามิเตอร์ที่อาจจะมีผลกระทบสูงต่อระบบรวมทั้งระบบปฏิบัติการ (OS)
     - ให้ทำการเปลี่ยนค่าเริ่มต้นหรือทบทวนการตั้งค่าจากผู้ขาย (Factory Setting) ทันทีที่ทำการติดตั้งเสร็จ โดยเฉพาะที่มีผลกระทบต่อการรักษาความปลอดภัย เช่น Default password
   - การเปลี่ยนแปลงข้อมูลกำหนดค่า ต้องมีการทำ Version Control และต้องผ่านการอนุมัติจากผู้รับผิดชอบและหน่วยงานที่เกี่ยวข้อง โดยผ่านกระบวนการควบคุมการเปลี่ยนแปลง (Change Management)
   - ต้องมีการติดตามตรวจสอบและทวนสอบค่ากำหนดจริงของระบบกับค่าพื้นฐานเป็นระยะ ตามรอบการตรวจสอบขององค์กร และทบทวนการตั้งค่าให้เป็นปัจจุบัน

4.3.5. การสำรองข้อมูล (Backup)

1) การสำรองข้อมูล (Information Backup)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดมาตรการในการสำรองข้อมูล และรอบการสำรองข้อมูลของระบบสารสนเทศที่สำคัญไว้อย่างสม่ำเสมอ เพื่อป้องกันการสูญหายของข้อมูล

- เจ้าของข้อมูลสารสนเทศ ต้องดำเนินการหรือกำหนดให้มีการสำรองข้อมูลสารสนเทศให้เป็นปัจจุบันอย่างสม่ำเสมอ และการทดสอบข้อมูลสำรองอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าจะสามารถนำข้อมูลกลับมาใช้ใหม่ได้เมื่อต้องการ
- ฝ่ายดิจิทัลเทคโนโลยี จะต้องรับผิดชอบในการสำรองข้อมูล และจัดเก็บสื่อสถานที่ที่แตกต่างกันเพื่อป้องกันการสูญเสียข้อมูลจากภัยคุกตามทางไซเบอร์ เช่น Cloud Storage เป็นต้น รวมถึงให้จัดเก็บไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูล

2) สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Redundancy of information processing facilities)
   - องค์กรต้องออกแบบและจัดให้มีระบบรองรับการทำงานต่อเนื่อง (System Resilience) สำหรับอุปกรณ์ประมวลผลสารสนเทศตามระดับความสำคัญของบริการ เช่น แหล่งจ่ายไฟสำรอง ระบบเครือข่ายสำรองหรือเส้นทางเชื่อมต่อสำรอง (Network Redundancy) เพื่อให้ระบบสามารถให้บริการได้อย่างต่อเนื่องและลดผลกระทบจากความขัดข้อง
   - องค์กรต้องจัดทำสัญญาหรือข้อตกลงกับผู้ให้บริการภายนอกโดยกำหนดให้ครอบคลุมมาตรการด้านความมั่นคงปลอดภัยและความต่อเนื่องในการให้บริการ เพื่อให้มั่นใจว่าระบบและอุปกรณ์ประมวลผลสามารถดำเนินงานได้อย่างพร้อมใช้งานตามข้อกำหนดขององค์กร
   - องค์กรควรพิจารณาให้มีศูนย์สำรองข้อมูล (DR Site หรือ Cloud Region สำรอง) ที่แยกออกจากศูนย์ข้อมูลหลัก (Data Center) เพื่อรองรับการดำเนินงานในกรณีที่ศูนย์ข้อมูลหลักไม่สามารถใช้งานได้
   - อุปกรณ์สำรองต้องได้รับการบำรุงรักษาตามรอบที่กำหนด เช่น การตรวจสอบแบตเตอรี่ UPS การทดสอบ Generator และบันทึกผล

4.3.6. การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on Software Installation)

1) การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of software on operational systems)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องจัดทำขั้นตอนปฏิบัติงานและมาตรการควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการจริง เพื่อจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งานและป้องกันการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ใช้งาน
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดรายการซอฟต์แวร์มาตรฐาน (Software Standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ขององค์กรอย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม
   - ผู้ใช้งานต้องปฏิบัติตามกฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์ และไม่ติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ในเครื่องคอมพิวเตอร์ขององค์กร

4.3.7. การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)

1) การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event Logging)
   - ผู้ดูแลระบบ ต้องจัดเก็บข้อมูลบันทึกเหตุการณ์ (Log) ซึ่งเกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศให้เพียงพอต่อการตรวจสอบ
   - ผู้ดูแลระบบ ต้องเฝ้าติดตาม (Monitoring) การใช้งานระบบสารสนเทศ โดยผลของการเฝ้าติดตามจะต้องถูกสอบทานอย่างสม่ำเสมอ เพื่อตรวจหาความผิดปกติ
   - ผู้ดูแลระบบ ต้องควบคุมและกำกับให้มีการบันทึกเหตุการณ์ความผิดพลาด (Fault Logging) ต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ รวมถึงวิเคราะห์ดำเนินการแก้ไข ตลอดจนวางแนวทางป้องกันการเกิดปัญหาซ้ำอีกในอนาคต
2) การป้องกันข้อมูลล็อก (Protection of Log Information)
   - ผู้ดูแลระบบต้องจัดให้มีการป้องกันข้อมูล และระบบการบันทึกและจัดเก็บหลักฐานการใช้งานเกี่ยวกับระบบสารสนเทศจากการถูกเปลี่ยนแปลงแก้ไข ถูกทำความเสียหาย หรือเข้าถึงโดยไม่ได้รับอนุญาต
3) การบันทึกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and Operator Logs)
   - ผู้ดูแลระบบ ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบและผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบ อาทิ เวลาเปิดและปิดระบบ
   - การเปลี่ยนแปลงการตั้งค่าของระบบ ความผิดพลาดของระบบ และการดำเนินการแก้ไข และต้องมีการสอบทานบันทึกกิจกรรมอย่างสม่ำเสมอ
4) การตั้งเวลาระบบสารสนเทศ (Clock Synchronization)
   - ผู้ดูแลระบบ ต้องควบคุม กำกับให้อุปกรณ์สารสนเทศ และระบบสารสนเทศขององค์กรได้รับการกำหนดเวลาให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องและตรงกับเวลาอ้างอิงสากล
   - ผู้ดูแลระบบ ต้องตรวจสอบเวลาของอุปกรณ์สารสนเทศและระบบสารสนเทศขององค์กร รวมถึงปรับปรุงให้เป็นปัจจุบันเสมอ เพื่อป้องกันไม่ให้เกิดการบันทึกเวลาที่ไม่ถูกต้อง

ส่วนที่ 4.5 การบริหารข้อมูลสารสนเทศเพื่อรายงานผลการให้บริการ (Service Reporting Policy)

วัตถุประสงค์

เพื่อให้บริการด้านข้อมูลสำหรับจัดทำรายงานให้กับผู้บริหาร และสนับสนุนการดำเนินงาน ตอบสนองการแข่งขันขององค์กร รวมถึงสนับสนุนให้รายงานต่างๆ มีข้อมูลที่ถูกต้องครบถ้วนและให้ผู้ที่เกี่ยวข้อสามารถใช้งานได้ข้อมูลได้อย่างถูกต้อง

4.5.1. การจัดหาและบำรุงรักษาแหล่งข้อมูลและรายงานผู้บริหาร

1) ส่วนงานภายในองค์กร ต้องจัดให้มีรายงานผลการดำเนินงานและข้อมูลต่างๆ ที่เป็นประโยชน์ต่อการดำเนินธุรกิจแก่ผู้บริหาร เพื่อให้ผู้บริหารใช้เป็นข้อมูลในการตัดสินใจต่อการดำเนินงานได้อย่างรวดเร็วและทันเวลา

2) ส่วนงานภายในองค์กร ควรกำหนดให้ข้อมูลในแหล่งข้อมูลและรายงานผู้บริหารมีความสำคัญระดับข้อมูลลับเฉพาะ (Highly Restricted) และห้ามเผยแพร่ให้ผู้อื่นรับทราบโดยไม่ได้รับอนุญาต
3) ฝ่ายดิจิทัลเทคโนโลยี ต้องจัดหาแหล่งข้อมูลเพื่อสนับสนุนให้แต่ละส่วนงานสามารถนำข้อมูลไปใช้ในการวิเคราะห์หรือวิจัย เพื่อใช้ในการแข่งขันทางธุรกิจได้อย่างรวดเร็ว
4) ฝ่ายดิจิทัลเทคโนโลยี ต้องบำรุงรักษาแหล่งข้อมูลและผลการดำเนินงานและข้อมูลต่างๆ ที่ใช้สำหรับรายงานผู้บริหารให้คงสภาพความถูกต้องและพร้อมใช้อยู่เสมอ
5) ฝ่ายดิจิทัลเทคโนโลยี ต้องสนับสนุนการพัฒนาทักษะของผู้ใช้ข้อมูลแต่ละส่วนงานให้สามารถสร้างรายงานได้อย่างถูกต้องและมีประสิทธิภาพ

4.5.2. การจัดพิมพ์รายงาน

1) กรณีที่ผู้ใช้งานต้องการจัดพิมพ์รายงานข้อมูลที่มีความสำคัญสูง ซึ่งหากถูกเผยแพร่ไปยังผู้ที่ไม่เกี่ยวข้องอาจส่งผลกระทบต่อองค์กรอย่างมีนัยสำคัญ ผู้ใช้งานต้องได้รับความเห็นชอบจากผู้บริหารแต่ละฝ่ายงานที่เป็นเจ้าของข้อมูลก่อนดำเนินการทุกครั้ง
2) ผู้ใช้งานควรมีทะเบียนคุมการพิมพ์รายงาน การจัดส่งรายงาน และการจัดเก็บรายงานต่างๆ ที่ได้จัดพิมพ์แล้วอย่างรัดกุม
3) ผู้ใช้งานควรกำหนดให้มีการลงลายมือชื่อเมื่อมีการรับรายงาน นอกจากนี้ควรทำลายรายงานที่ไม่ได้ใช้งานแล้ว

4.5.3. การเข้าถึงข้อมูลในแหล่งข้อมูล

1) ผู้ใช้งาน ต้องร้องขอสิทธิ์การใช้งานข้อมูลในแหล่งข้อมูล จากส่วนงานซึ่งเป็นเจ้าของข้อมูลก่อนเข้าถึงแหล่งข้อมูลนั้นๆ

4.5.4. การควบคุมคุณภาพของข้อมูลในแหล่งข้อมูล

1) ผู้ใช้งานต้องรับผิดชอบในการทำข้อมูลให้มีความสมบูรณ์ (Data Cleaning) โดยต้องแจ้งขอข้อมูลเพื่อดำเนินการผ่านระบบ e-Memo และส่งมายังฝ่ายดิจิทัลเทคโนโลยี เพื่อให้เจ้าหน้าที่เทคโนโลยีสารสนเทศดำเนินการดึงข้อมูลและปรับปรุงข้อมูลเข้าระบบ
2) กรณีที่ผู้ใช้งานต้องการเปลี่ยนแปลงข้อมูลในแหล่งข้อมูล ผู้ใช้งานต้องจัดเตรียมข้อมูลตามกระบวนการทำข้อมูลให้มีความสมบูรณ์ (Data Cleaning) และแจ้งขอดำเนินการเปลี่ยนแปลงข้อมูลผ่าน e-Memo และส่งมายังฝ่ายดิจิทัลเทคโนโลยี เพื่อให้เจ้าหน้าที่เทคโนโลยีสารสนเทศดำเนินการปรับปรุงข้อมูลในฐานข้อมูล

ส่วนที่ 4.4 ความมั่นคงปลอดภัยข้อมูล (Data Security Policy)

วัตถุประสงค์

เพื่อปกป้องข้อมูลที่ละเอียดอ่อนจากการเข้าถึงโดยไม่ได้รับอนุญาต การสูญหาย หรือการรั่วไหล ทั้งยังคงความพร้อมใช้งานและความสมบูรณ์ของข้อมูล การลบข้อมูลสารสนเทศทำให้มั่นใจได้ว่า ข้อมูลสารสนเทศที่ละเอียดอ่อนจะถูกลบออกจากระบบอย่างถาวรเมื่อไม่จำเป็นต้องใช้อีกต่อไป

4.3.1. ความมั่นคงปลอดภัยข้อมูล (Data Security Policy)

1) การลบข้อมูลสารสนเทศ (Information Deletion)
   - องค์กรต้องกำหนดระยะเวลาการจัดเก็บข้อมูล (Data Retention Period) ให้ชัดเจนสำหรับข้อมูลแต่ละประเภท โดยพิจารณาจากความจำเป็นทางธุรกิจ ข้อกำหนดด้านกฎหมาย และความมั่นคงปลอดภัยสารสนเทศ ทั้งนี้ ข้อมูลที่พ้นความจำเป็นต้องใช้งานต้องถูกจัดการตามกระบวนการลบหรือทำลายข้อมูลอย่างปลอดภัยตามมาตรฐานที่องค์กรกำหนด
   - ข้อมูลที่หมดความจำเป็นต้องใช้งาน ต้องถูกลบตามการกำหนดระยะเวลาการจัดเก็บข้อมูล (Data Retention Period) และข้อกำหนดของกฎหมายที่เกี่ยวข้อง
   - การลบข้อมูลต้องใช้วิธีที่ปลอดภัย เช่น Secure Erase, Cryptographic Erasure หรือการ Overwrite ตามมาตรฐานที่องค์กรกำหนด
   - อุปกรณ์จัดเก็บข้อมูล เช่น Hard Disk, SSD, USB, Storage Media ที่ต้องยกเลิกใช้งาน ต้องถูกลบข้อมูลอย่างปลอดภัยก่อนการขาย ทิ้ง หรือโอนย้าย
   - การลบข้อมูลในระบบคลาวด์ต้องได้รับการรับรองจากผู้ให้บริการ เช่น เอกสารยืนยันการลบข้อมูล (Data Deletion Certificate)
   - ต้องมีการบันทึกหลักฐานการลบข้อมูลและจัดเก็บตามระยะเวลาที่กำหนด
2) การปิดบังข้อมูล (Data Masking)
   - องค์กรต้องใช้เทคนิคการปิดบังข้อมูลเพื่อป้องกันการเปิดเผยข้อมูลสำคัญหรือข้อมูลส่วนบุคคล โดยเฉพาะในกระบวนการทดสอบ พัฒนา หรือการแบ่งปันข้อมูล
   - ข้อมูลที่มีความอ่อนไหวหรือข้อมูลส่วนบุคคล ต้องถูกปิดบังหรือทำให้ไม่สามารถระบุตัวตนได้เมื่อใช้ในสภาพแวดล้อมที่ไม่ใช่ระบบจริง เช่น ระบบทดสอบ (Test) หรือระบบพัฒนา (Dev)
   - องค์กรควรพิจารณาปิดบังข้อมูลเพื่อไม่ให้สามารถระบุตัวตนได้ โดยใช้เทคนิคต่าง ๆ เช่น การแทนค่าข้อมูลจริง (Tokenization) การปิดบังข้อมูล (Data masking) การใช้นามแฝง (Pseudonymization) หรือ การทำข้อมูลนิรนาม (Anonymization)
   - ต้องควบคุมการเข้าถึงข้อมูลที่ปิดบังและข้อมูลต้นฉบับ โดยกำหนดสิทธิ์ให้เฉพาะผู้มีความจำเป็นต้องใช้
   - ต้องมีการทบทวนวิธีการปิดบังข้อมูลเพื่อให้มั่นใจว่าข้อมูลไม่สามารถย้อนกลับเพื่อระบุตัวบุคคลได้
   - ห้ามนำข้อมูลจริงที่มีความอ่อนไหวไปใช้ในสภาพแวดล้อมที่ไม่มีมาตรการป้องกันที่เพียงพอ

3) การป้องกันการรั่วไหลของข้อมูล (Data Leakage Prevention)

- องค์กรต้องกำหนดให้มีมาตรการเฝ้าระวังข้อมูลรั่วไหลตามช่องทางการรับ-ส่งข้อมูล เพื่อป้องกันการรั่วไหลหรือการส่งออกข้อมูลโดยไม่ได้รับอนุญาต เช่น ใช้ระบบหรือเครื่องมือป้องกันการรั่วไหลของข้อมูล (DLP Solutions) เพื่อตรวจจับ ป้องกัน และแจ้งเตือนการเคลื่อนย้ายข้อมูลที่ผิดปกติ
- ต้องมีการกำหนดและควบคุมเส้นทางการส่งข้อมูล รวมถึงมาตรการด้านเทคนิค เพื่อจำกัดช่องทางการนำข้อมูลออกจากองค์กร เช่น การปิดการใช้งานพอร์ต USB บนอุปกรณ์การทำงาน การควบคุมการส่งข้อมูลผ่านอีเมล การจำกัดการใช้บริการ Cloud Storage การควบคุมการถ่ายโอนไฟล์ (File Transfer) และการจำกัดการเชื่อมต่ออุปกรณ์พกพา ทั้งนี้เพื่อป้องกันความเสี่ยงจากการรั่วไหลหรือการนำข้อมูลออกโดยไม่ได้รับอนุญาต
- ข้อมูลความลับที่ส่งออกจากองค์กรต้องได้รับการเข้ารหัส และอนุญาตจากผู้มีอำนาจก่อนทุกครั้ง
- บุคลากรต้องได้รับการอบรมเกี่ยวกับพฤติกรรมที่เสี่ยงต่อการรั่วไหลของข้อมูล เช่น การส่งข้อมูลผิดผู้รับ การแชร์ผ่านช่องทางที่ไม่ปลอดภัย หรือการใช้แอปพลิเคชันที่ไม่ได้รับอนุญาต
- ต้องมีการบันทึกเหตุการณ์เกี่ยวกับข้อมูลรั่วไหล และดำเนินการสอบสวนตามกระบวนการจัดการเหตุการณ์ (Incident Management Process)
- การเข้าถึงข้อมูลสำคัญต้องอยู่ภายใต้หลัก Least Privilege และการตรวจสอบกิจกรรมแบบต่อเนื่อง (Monitoring & Logging)

ส่วนที่ 4.5 การสื่อสารด้านความมั่นคงปลอดภัยสารสนเทศ (Communications Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการบริหารจัดการเครือข่าย และการส่งข้อมูลผ่านระบบเครือข่ายคอมพิวเตอร์ทั้งภายในและภายนอกองค์กรให้มีความมั่นคงปลอดภัย

4.5.1. การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ (Network Security Management)

1) การควบคุมเครือข่าย (Network Controls)

- ผู้ดูแลระบบ ต้องควบคุม กำกับให้มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ เพื่อป้องกันภัยคุกคาม และมีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและแอพพลิเคชั่นที่ทำงานบนเครือข่ายคอมพิวเตอร์ รวมทั้งข้อมูลสารสนเทศที่มีการแลกเปลี่ยนบนเครือข่าย
- ผู้ดูแลระบบต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) โดยมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

- ห้ามใช้งานระบบอินเทอร์เน็ตขององค์กร เพื่อใช้หาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือน หรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับบริษัท
- ห้ามมิให้พนักงาน หรือผู้ใช้งานในเครือข่ายองค์กรกระทำการใด ๆ ในนามขององค์กรผ่านโซเชียลมีเดีย หรือให้เข้าใจว่าเป็นการปฏิบัติในนามขององค์กร เว้นแต่เป็นพนักงาน หรือผู้ใช้งานที่ได้รับอนุญาตจากทางองค์กร แล้วเท่านั้น
- หลีกเลี่ยงการนำเสนอ หรือโพสต์ข้อมูลขององค์กร ในเชิงที่ไม่เหมาะสม หรือที่เป็นความคิดเห็นส่วนตัวเกี่ยวกับองค์กร อันอาจทำให้เกิดความเข้าใจผิดในเครือข่ายสังคมออนไลน์

2) ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of Network Services)
   - ผู้ดูแลระบบ ต้องควบคุมให้มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับของการให้บริการ และความต้องการด้านการบริหารจัดการของการให้บริการเครือข่ายทั้งหมด ลงในข้อตกลงหรือสัญญาการให้บริการด้านเครือข่ายต่างๆ ทั้งที่เป็นการให้บริการจากภายในหรือภายนอก
3) การแบ่งแยกเครือข่าย (Segregation in Network)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องจัดให้มีการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยต้องพิจารณาถึงความต้องการของผู้ใช้งานในการเข้าถึงระบบเครือข่าย ผลกระทบทางด้านความมั่นคงปลอดภัยสารสเทศ และระดับความสำคัญของข้อมูลที่อยู่บนเครือข่ายนั้น

4.5.2. การแลกเปลี่ยนข้อมูลสารสนเทศ (Information Transfer)

1) การแลกเปลี่ยนข้อมูลสารสนเทศ (Information Transfer)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องควบคุม กำกับให้มีขั้นตอนการปฏิบัติงานในการแลกเปลี่ยนข้อมูลสารสนเทศให้เหมาะสมสำหรับประเภทของการสื่อสารที่ใช้และประเภทของข้อมูลลำดับชั้นความลับของข้อมูล
2) ข้อตกลงสำหรับการแลกเปลี่ยนข้อมูลสารสนเทศ (Agreements on Information Transfer)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องควบคุม กำกับให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศทั้งที่เป็นการแลกเปลี่ยนระหว่างหน่วยงานภายในองค์กร และระหว่างองค์กรกับหน่วยงานภายนอกองค์กร
   - การแลกเปลี่ยนข้อมูลสารสนเทศภายในองค์กรกับหน่วยงานภายนอก ต้องได้รับการอนุมัติจากเจ้าของข้อมูลก่อนทุกครั้ง และมีการควบคุมโดยการระบุข้อตกลงเป็นลายลักษณ์อักษร รวมถึงกำหนดเงื่อนไขสำหรับการแลกเปลี่ยน ตลอดจนต้องมีการป้องกันข้อมูลสารสนเทศตามลำดับชั้นความลับข้อมูลอย่างเหมาะสม

3) การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดมาตรการในการควบคุมการรับส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-mail) หรือ EDI (Electronic Data Interchange) หรือ Instant Messaging เป็นต้น โดยข้อความทางอิเล็กทรอนิกส์ที่สำคัญจะต้องได้รับการป้องกันอย่างเหมาะสมจากการพยายามเข้าถึง การแก้ไขการรบกวนทำให้ระบบหยุดให้บริการจากผู้ไม่มีสิทธิ์

4) ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing Application Service on Public Networks)
   - ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่ผ่านระบบให้บริการ การใช้งาน (Application Service) ทั้งในกรณีทั่วไปและกรณีที่ผ่านเครือข่ายสาธารณะ เพื่อป้องกันการกระทำผิดในลักษณะทุจริต (Fraudulent Activities) การทำธุรกรรมที่ไม่สมบูรณ์หรือผิดพลาด (Incomplete Transmission or Miss-Routing) หรือการเปิดเผยคัดลอก หรือเปลี่ยนแปลงแก้ไขข้อมูล โดยไม่ได้รับอนุญาต

4.5.3. การการกรองเว็บไซต์ (Web Filtering)

1) องค์กรต้องจำกัดการเข้าถึงเว็บไซต์ หรือใช้ระบบกรองเว็บไซต์ (Web Filtering System) เพื่อควบคุมการเข้าถึงเว็บไซต์ตามหมวดหมู่ความเสี่ยง เช่น เว็บไซต์อันตราย เว็บไซต์ที่มีมัลแวร์ เว็บไซต์ผิดกฎหมาย หรือเว็บไซต์ที่ไม่เหมาะสม เว็บไซต์หรือโดเมนที่มีพฤติกรรมเสี่ยงด้านความมั่นคงปลอดภัย เช่น Phishing, Botnet, Malware Hosting จะต้องถูกบล็อกโดยอัตโนมัติ
2) การเข้าถึงเว็บไซต์ต้องเป็นไปเพื่อวัตถุประสงค์ทางธุรกิจหรือการปฏิบัติงานขององค์กร
3) เว็บไซต์ที่ไม่เกี่ยวข้องกับการทำงาน เช่น การพนัน ลามกอนาจาร แชร์ไฟล์ผิดลิขสิทธิ์ หรือเนื้อหาที่เสี่ยงต่อภาพลักษณ์องค์กร ต้องถูกปิดกั้น

ส่วนที่ 4.6 การเข้ารหัสข้อมูล (Use of Cryptography)

วัตถุประสงค์

เพื่อกำหนดแนวทางและมาตรการในการใช้เทคโนโลยีการเข้ารหัสข้อมูล (Cryptography) เพื่อรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลขององค์กร รวมถึงป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

4.6.1. การเข้ารหัสข้อมูล (Use of Cryptography)

1) การใช้การเข้ารหัสข้อมูล (General Use of Cryptography)
   - ข้อมูลที่มีความสำคัญหรือข้อมูลส่วนบุคคลต้องได้รับการเข้ารหัสทั้งในขณะจัดเก็บ (Data at Rest) และขณะส่งผ่านข้อมูล (Data in Transit) ตามความจำเป็น

- ต้องใช้วิธีการและอัลกอริทึมการเข้ารหัสที่เป็นมาตรฐานสากล เช่น AES, RSA, SHA-2 หรืออัลกอริทึมที่องค์กรกำหนด และห้ามใช้การเข้ารหัสที่ล้าสมัยหรือมีความเสี่ยง เช่น DES, 3DES, MD5 หรือ RC4
- หากไม่สามารถใช้การเข้ารหัสได้ ต้องใช้วิธีการป้องกันอื่น เช่น Data Masking, Tokenization หรือ Access Control ที่เข้มงวด

2) การเข้ารหัสข้อมูลที่จัดเก็บ (Data at Rest Encryption)
   - อุปกรณ์จัดเก็บข้อมูล เช่น Server, Storage, Laptop, Mobile Device ต้องใช้การเข้ารหัสเต็มดิสก์ (Full-disk Encryption)
   - ข้อมูลสำคัญหรือข้อมูลที่มีการจำแนกชั้นความลับต้องถูกเข้ารหัสก่อนจัดเก็บในระบบคลาวด์หรืออุปกรณ์พกพา
   - ห้ามจัดเก็บข้อมูลสำคัญหรือข้อมูลความลับลงในสื่อไม่ได้เข้ารหัส เช่น USB ที่ไม่มีการป้องกัน
   - สำเนาข้อมูลสำรอง (Backup) ควรถูกเข้ารหัสก่อนจัดเก็บหรือโอนย้าย
3) การเข้ารหัสข้อมูลระหว่างการส่งผ่าน (Data in Transit Encryption)
   - ข้อมูลที่ส่งผ่านระบบเครือข่ายภายในและภายนอกต้องเข้ารหัสผ่านโปรโตคอลที่ปลอดภัย เช่น TLS 1.2+, HTTPS, SSH, IPsec
   - การถ่ายโอนไฟล์ต้องใช้ช่องทางที่เข้ารหัส เช่น SFTP, FTPS, Secure VPN
   - ห้ามส่งข้อมูลสำคัญผ่านช่องทางที่ไม่มีความปลอดภัย เช่น Email แบบไม่เข้ารหัส หรือ Messaging ที่ไม่ได้รับอนุมัติ

4.6.2. การบริหารจัดการกุญแจเข้ารหัส (Cryptographic Key Management)

1) องค์กรต้องมีระบบหรือกระบวนการบริหารจัดการกุญแจเข้ารหัส (Key Management) ที่ครอบคลุมการสร้าง การจัดเก็บ การแจกจ่าย การหมุนเวียน และการทำลายกุญแจ
2) กุญแจเข้ารหัสต้องถูกจัดเก็บในพื้นที่ที่ปลอดภัย เช่น HSM, KMS หรือ Key Vault
3) ต้องกำหนดอายุการใช้งานของกุญแจ (Key Rotation) และต้องมีการเปลี่ยนกุญแจเมื่อพบความเสี่ยง เช่น การรั่วไหลของกุญแจ การเข้าถึงโดยไม่ได้รับอนุญาต การบุกรุกระบบที่จัดเก็บกุญแจ หรือกรณีที่อัลกอริทึมเข้ารหัสที่ใช้งานอยู่ถูกประกาศว่ามีช่องโหว่ด้านความมั่นคงปลอดภัย

ส่วนที่ 4.7 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)

วัตถุประสงค์

เพื่อลดความผิดพลาดในการกำหนดความต้องการ การออกแบบ การพัฒนา และการทดสอบระบบสารสนเทศที่มีการพัฒนาขึ้นใหม่หรือปรับปรุงระบบงานเพิ่มเติม รวมถึงควบคุมให้ระบบงานที่พัฒนาหรือจัดหาเป็นไปตามข้อตกลงที่กำหนดไว้

4.7.1. วงจรชีวิตการพัฒนาอย่างปลอดภัย (Secure Development Life Cycle :SDLC)

1) องค์กรต้องผนวกหลักการด้านความมั่นคงปลอดภัยในทุกขั้นตอนของการพัฒนา ได้แก่
   - การวิเคราะห์ความต้องการ (Requirement Analysis)

- การออกแบบระบบ (System Design)
- การพัฒนา (Development)
- การทดสอบ (Testing)
- การนำขึ้นใช้งาน (Deployment)
- การบำรุงรักษา (Maintenance)

โดยต้องระบุความเสี่ยงด้านความปลอดภัยและมาตรการควบคุมที่จำเป็นตั้งแต่เริ่มต้นโครงการ

2) การออกแบบระบบที่ปลอดภัย (Secure Architecture & Design) ควรใช้หลัก Secure-by-Design เช่น การแบ่งชั้นข้อมูล การควบคุมการเข้าถึง การป้องกัน Injection และการยืนยันตัวตนอย่างเหมาะสม เพื่อให้มั่นใจว่าระบบมีสถาปัตยกรรมที่มั่นคงปลอดภัยตั้งแต่ขั้นตอนการออกแบบ

4.7.2. ความต้องการด้านความมั่นคงปลอดภัยระบบ (Security Requirements of Information Systems)

1) การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification)
   - ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ ส่วนบริหารโครงการเทคโนโลยีสารสนเทศ และหน่วยงานที่ได้รับมอบหมายให้พัฒนา หรือจัดหาระบบสารสนเทศเพื่อนำมาใช้งานในองค์กร ต้องกำหนดคุณลักษณะความต้องการด้านความมั่นคงปลอดภัยสารสนเทศไว้อย่างชัดเจนในระบบที่จะพัฒนาขึ้นมาใช้งาน หรือระบบที่จัดหามาใช้งาน
   - ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ ส่วนบริหารโครงการเทคโนโลยีสารสนเทศ และหน่วยงานที่ได้รับมอบหมายให้พัฒนาหรือจัดหาระบบสารสนเทศ ต้องติดตามการพัฒนาระบบสารสนเทศเพื่อตรวจสอบว่าการพัฒนาระบบสารสนเทศตรงตามความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงความต้องการด้านการใช้งานที่กำหนดไว้
   - ความต้องการด้านความมั่นคงปลอดภัย (Security Requirement) ความต้องการด้านสมรรถนะและประสิทธิภาพของระบบ (Performance Requirement) รวมถึงความต้องการด้านกฎหมายและข้อบังคับที่เกี่ยวข้อง (Legal Requirement) ต้องถูกนำมาพิจารณาอย่างครบถ้วนทั้งในระดับระบบโดยรวมและในระดับองค์ประกอบย่อย (Module) เพื่อให้การออกแบบและพัฒนาระบบเป็นไปอย่างปลอดภัย มีประสิทธิภาพ และสอดคล้องตามข้อกำหนดที่เกี่ยวข้องทั้งหมด

4.7.3. ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาระบบและสนับสนุน (Security in Development and Support Processes)

1) การพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure Development)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดกฎระเบียบสำหรับการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัย และครอบคลุมตลอดทั้งวงจรการพัฒนาระบบสารสนเทศ

- การพัฒนาโค้ดต้องปฏิบัติตามมาตรฐาน Secure Coding ที่องค์กรกำหนด รวมถึงแนวทางจาก OWASP Top 10 และต้องป้องกันช่องโหว่ที่พบบ่อย เช่น Injection, Cross-Site Scripting (XSS), Broken Access Control, CSRF, Insecure Deserialization และช่องโหว่จากการตรวจสอบ Input ที่ไม่ถูกต้อง
- ข้อมูลสำคัญต้องได้รับการจัดการอย่างปลอดภัย โดยห้ามฝังข้อมูลสำคัญใด ๆ เช่น รหัสผ่าน API Key Token หรือ Credentials ลงในซอร์สโค้ด และต้องใช้มาตรการปกป้องเพิ่มเติม เช่น การเข้ารหัสหรือการทำ Masking/Tokenization ตามความเหมาะสมของระดับความอ่อนไหวของข้อมูล
- Source Code ต้องผ่านการตรวจสอบช่องโหว่ด้วยเครื่องมือที่องค์กรกำหนด เพื่อประเมินความเสี่ยงจากโค้ดและ Library หรือ Open-source ที่นำมาใช้ หากตรวจพบช่องโหว่ต้องดำเนินการแก้ไขตามระดับความรุนแรงที่องค์กรกำหนด
- Source Code ต้องถูกจัดเก็บและบริหารจัดการผ่านระบบควบคุมเวอร์ชันที่องค์กรอนุมัติ เช่น Git พร้อมทั้งต้องมีการกำหนดสิทธิ์การเข้าถึงและการอนุมัติการรวมโค้ด (Merge) ตามหลักการแบ่งแยกหน้าที่ (Segregation of Duties: SoD) และต้องผ่านการตรวจทาน (Code Review) โดยผู้ที่ได้รับมอบหมายก่อนการนำขึ้นใช้งานทุกครั้ง

2) หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure System Engineering Principles)
   - ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ ส่วนบริหารโครงการเทคโนโลยีสารสนเทศ และหน่วยงานที่ได้รับมอบหมายให้พัฒนาระบบสารสนเทศ ต้องยึดหลักการความมั่นคงปลอดภัยในการพัฒนาระบบ ดังต่อไปนี้เป็นอย่างน้อย
     - การให้สิทธิ์ต่ำที่สุด (Least Privilege) แก่ผู้ใช้งานระบบสารสนเทศ เพื่อป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต
     - การให้สิทธิ์เฉพาะที่จำเป็นในการปฏิบัติงาน (Need to Know) แก่ผู้ใช้งานระบบสารสนเทศ เพื่อป้องกันการรั่วไหลของข้อมูลสำคัญ
     - การออกแบบระบบให้สามารถป้องกันได้หลายระดับชั้น (Defense In-Depth) เพื่อลดความเสี่ยงของการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
     - การออกแบบในลักษณะเปิด (Open Design) เพื่อให้การพัฒนาระบบมีการใช้กลไกหรืออัลกอริทึม (Algorithm) ที่เป็นมาตรฐานเดียวกันและสามารถตรวจสอบการทำงานได้

3) สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure Development Environment)
   - ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ ส่วนบริหารโครงการเทคโนโลยีสารสนเทศ และหน่วยงานที่ได้รับมอบหมายให้พัฒนาระบบสารสนเทศ ต้องมีการควบคุมสภาพแวดล้อมของการพัฒนาและบูรณาการระบบให้มีความมั่นคงปลอดภัย โดยต้องป้องกันข้อมูลของระบบที่เกิดขึ้นในระหว่างการพัฒนา การรับส่งข้อมูล การสำรองข้อมูล และการควบคุมการเข้าถึงระบบสารสนเทศ

4.7.4. การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced Development)

1) ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดข้อตกลงในการพัฒนาระบบสำหรับหน่วยงานภายนอกที่ทำหน้าที่พัฒนาซอฟต์แวร์เพื่อใช้งานภายในองค์กรอย่างเป็นลายลักษณ์อักษร
2) หน่วยงานที่ได้รับมอบหมายให้ดำเนินการจัดจ้างหน่วยงานภายนอกเข้ามาพัฒนาระบบสารสนเทศให้องค์กร ต้องกำกับดูแล เฝ้าระวัง และติดตามกิจกรรมการพัฒนาระบบที่จ้างหน่วยงานภายนอกเป็นผู้ดำเนินการอย่างสม่ำเสมอ เพื่อป้องกันไม่ให้เกิดความเสียหายใดๆ ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศ

4.7.5. การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System Security Testing)

1) ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ ส่วนบริหารโครงการเทคโนโลยีสารสนเทศ หน่วยงานที่ได้รับมอบหมาย และผู้ใช้งาน ต้องร่วมกันทดสอบฟังก์ชันการทำงานของระบบสารสนเทศ และฟังก์ชันการทำงานด้านความมั่นคงปลอดภัยสารสนเทศในระบบที่ได้รับการพัฒนาขึ้นใหม่ หรือระบบที่มีการเปลี่ยนแปลงทุกครั้ง
2) การทดสอบการพัฒนาระบบสารสนเทศ ต้องดำเนินการทดสอบระหว่างการพัฒนา และก่อนนำระบบขึ้นใช้งานจริง โดยต้องจัดเก็บหลักฐานในการทดสอบระบบสารสนเทศที่ได้รับการพัฒนาขึ้นใหม่ หรือระบบที่มีการเปลี่ยนแปลงอย่างเป็นทางการ
3) การทดสอบเพื่อรับรองระบบ (System Acceptance Testing)
    - ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่หรือที่ปรับปรุงเพิ่มเติม ทั้งที่มาจากส่วนพัฒนาระบบเทคโนโลยีสารสนเทศพัฒนาขึ้น หรือที่มีการจัดหาจากหน่วยงานภายนอก และต้องทดสอบระบบก่อนที่จะนำระบบดังกล่าวมาใช้งานจริง

4.7.6. การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of Development, Testing and Operational Environments)

1) ฝ่ายดิจิทัลเทคโนโลยี ต้องควบคุม กำกับให้มีการแยกส่วนระบบคอมพิวเตอร์ที่มีไว้สำหรับพื้นที่ในการพัฒนาระบบงาน (Development Area) ระบบงานทดสอบ (User Acceptance Test) และระบบที่ให้บริการจริง (Production Environment) ออกจากกันฝ่ายดิจิทัลเทคโนโลยี ต้องควบคุมให้มีการกำหนดสิทธิ์การเข้าถึงในแต่ละสภาพแวดล้อมและจัดให้มีเจ้าหน้าที่รับผิดชอบการปิดระบบงานอย่างชัดเจน โดยต้องรายงานผลการปฏิบัติงานต่อผู้บังคับบัญชา กรณีที่พบปัญหาต้องมีการบันทึกปัญหา และวิธีการแก้ไขรวมถึงรายงานต่อผู้บังคับบัญชาให้ทราบ
2) ฝ่ายดิจิทัลเทคโนโลยี ต้องควบคุมให้มีการกำหนดสิทธิ์การเข้าถึงในแต่ละสภาพแวดล้อม และจัดให้มีเจ้าหน้าที่รับผิดชอบการปิดระบบงานอย่างชัดเจน โดยต้องรายงานผลการปฏิบัติงานต่อผู้บังคับบัญชา กรณีที่พบปัญหาต้องมีการบันทึกปัญหา และวิธีการแก้ไขรวมถึงรายงานต่อผู้บังคับบัญชาให้ทราบ

4.7.7. ข้อมูลสำหรับการทดสอบ (Test Data)

1) การป้องกันข้อมูลสำหรับการทดสอบ (Protection of Test Data)
   - ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ ส่วนบริหารโครงการเทคโนโลยีสารสนเทศ หน่วยงานที่ได้รับมอบหมาย ต้องเลือกข้อมูลสารสนเทศของการทดสอบให้มีความมั่นคงปลอดภัย เพื่อทำให้แน่ใจว่าผลการทดสอบเชื่อถือได้ และต้องหลีกเลี่ยงการใช้ข้อมูลจริง (Production Data) ที่มีอยู่บนระบบให้บริการมาใช้ในการทดสอบ
   - กำหนดให้มีมาตรการควบคุมการใช้งานข้อมูลทดสอบให้มั่นคงปลอดภัย ควบคุมการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น และในกรณีที่มีการนำสำเนาข้อมูลจากระบบใช้งานจริงเพื่อใช้ในการทดสอบต้องมีการควบคุมข้อมูลที่ใช้ทดสอบเหมือนกับการควบคุมข้อมูลที่อยู่ในระบบใช้งานจริง

4.7.8. ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System Change Control Procedures)

1) ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงอย่างเป็นลายลักษณ์อักษร โดยให้ครอบคลุมทั้งวงจรการพัฒนาระบบสารสนเทศ
2) การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ (Technical Review of Applications after Operating Platform Changes)
   - ผู้ดูแลระบบ จะต้องทำการตรวจสอบทางเทคนิคเพื่อวิเคราะห์ถึงผลกระทบที่อาจเกิดขึ้นเมื่อต้องการที่จะเปลี่ยนแปลงหรือปรับปรุงระบบปฏิบัติการ เช่น การเปลี่ยนเวอร์ชั่น และการแก้ไขข้อบกพร่องด้านความมั่นคงปลอดภัย เป็นต้น โดยจะต้องมีการทดสอบบนระบบงานทดสอบ (Test Environment) จนมั่นใจว่าระบบงานต่างๆ ที่ประมวลผลบนเครื่องดังกล่าว สามารถทำงานได้ตามปกติและมีความมั่นคงปลอดภัย จึงจะทำการเปลี่ยนแปลงหรือปรับปรุงบนเครื่องที่ใช้งานจริง (Production Environment)
   - ผู้ดูแลระบบ จะต้องทำการตรวจสอบทางเทคนิคภายหลังการเปลี่ยนแปลงระบบปฏิบัติการบนระบบจริง เพื่อตรวจสอบว่าการเปลี่ยนแปลงไม่มีผลกระทบต่อการทำงานของระบบ และไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยระบบสารสนเทศ

ส่วนที่ 4.8 การจัดการบริหารเปลี่ยนแปลงระบบสารสนเทศ (Change Management Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางการบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ และลดความผิดพลาดในการดำเนินการเปลี่ยนแปลง รวมถึงระบบงานสามารถสนับสนุนธุรกิจขององค์กรได้อย่างต่อเนื่องและมีประสิทธิภาพ

4.8.1. การบริหารจัดการการเปลี่ยนแปลง (Change Management)

1) ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดให้มีการจัดการควบคุม การเปลี่ยนแปลงของระบบสารสนเทศ ที่มีผลต่อความมั่นคงปลอดภัยของระบบสารสนเทศ
2) ต้องมีการกำหนดบทบาทและความรับผิดชอบของแต่ละบุคคลที่เกี่ยวข้องกับกระบวนการควบคุมการเปลี่ยนแปลงอย่างชัดเจน

3) ฝ่ายดิจิทัลเทคโนโลยี ต้องดำเนินการกำหนดประเภทของการเปลี่ยนแปลง (Change Type) เพื่อใช้ในการดำเนินการบันทึก จำแนกประเภท ประเมิน และกำหนดผู้อนุมัติสำหรับคำร้องขอการเปลี่ยนแปลง โดยผู้มีอำนาจอนุมัติให้หมายถึงผู้จัดการส่วนขึ้นไป หรือผู้ที่ได้รับมอบหมายให้มีอำนาจอนุมัติ
4) ฝ่ายดิจิทัลเทคโนโลยี ต้องจัดทำขั้นตอนปฏิบัติงานสำหรับการบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศและให้บันทึกการเปลี่ยนแปลงอย่างเป็นลายลักษณ์อักษร
5) ผู้ร้องขอและผู้ดำเนินการเปลี่ยนแปลง ต้องดำเนินการวิเคราะห์ผลกระทบและความเสี่ยงในการดำเนินการเปลี่ยนแปลง เพื่อเตรียมมาตรการรองรับการเปลี่ยนแปลงในแต่ละกิจกรรม
6) ผู้ที่ร้องขอให้มีการเปลี่ยนแปลงจะต้องจัดทำแผนงานภาพรวม สำหรับการดำเนินการการเปลี่ยนแปลงโดยกำหนดวันเวลาที่ต้องการดำเนินงาน และทรัพยากรที่จำเป็น เป็นต้น และแจ้งให้ผู้ที่เกี่ยวข้องรับทราบถึงแผนการเปลี่ยนแปลง
7) ผู้ดำเนินการเปลี่ยนแปลงต้องจัดทำแผนสำหรับย้อนกลับสู่สภาวะเดิม (Fallback Plan) เพื่อใช้สำหรับแก้ไขการเปลี่ยนแปลงเมื่อต้องการให้กลับสู่สภาวะเดิมหากการเปลี่ยนแปลงไม่สามารถทำได้สำเร็จตามวัตถุประสงค์ที่ต้องการ

ส่วนที่ 4.9 การป้องกันระบบสารสนเทศระหว่างที่ทดสอบการตรวจประเมิน (Protection of information systems during audit testing

วัตถุประสงค์

เพื่อจำกัดผลกระทบจากกิจกรรมการตรวจสอบระบบต่อการปฏิบัติงาน หรือการดำเนินธุรกิจขององค์กร

4.8.1. สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (Information Systems Audit Considerations)

1) มาตรการการตรวจประเมินระบบ (Information System Audit Controls)
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องจัดทำแผนการตรวจสอบระบบสารสนเทศให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้ เช่น แผนการตรวจสอบช่องโหว่ของระบบสารสนเทศ(Vulnerability Assessment) เป็นต้น
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องแจ้งให้หน่วยงานที่เกี่ยวข้องรับทราบก่อนดำเนินการตรวจสอบระบบสารสนเทศทุกครั้ง
   - ฝ่ายดิจิทัลเทคโนโลยี ต้องกำหนดขอบเขตการตรวจสอบทางเทคนิค (Technical Audit Test) ให้ครอบคลุมจุดเสี่ยงที่สำคัญ และต้องควบคุมการตรวจสอบดังกล่าวไม่ให้กระทบต่อการปฏิบัติงานตามปกติ โดยกรณีที่การตรวจสอบระบบสารสนเทศมีโอกาสกระทบต่อความพร้อมใช้งานของระบบ (System Availability) ต้องจัดให้มีการทดสอบนอกเวลาทำการ
   - ผู้ตรวจสอบภายใน มีหน้าที่ในการจัดทำแผนตรวจสอบ วัตถุประสงค์การตรวจสอบ จัดส่งให้กับผู้รับการตรวจสอบ เพื่อให้มีการตกลงแผนการตรวจสอบระหว่างผู้ตรวจสอบและผู้รับการตรวจ ซึ่งเป็นการช่วยจำกัดผลกระทบต่อการปฏิบัติงานหรือการดำเนินธุรกิจจากกิจกรรมการตรวจสอบ

หมวดที่ 5 นโยบายการกำกับดูแลการใช้งานปัญญาประดิษฐ์ (Artificial Intelligence)

วัตถุประสงค์

เพื่อกำหนดหลักการและมาตรการในการพัฒนา ใช้งาน จัดการ และกำกับดูแลเทคโนโลยีปัญญาประดิษฐ์ (AI) ขององค์กรให้เป็นไปอย่างปลอดภัย โปร่งใส มีจริยธรรม สอดคล้องกับข้อกฎหมาย และลดความเสี่ยงจากผลกระทบที่อาจเกิดขึ้นทั้งต่อองค์กร ผู้ใช้งาน และสังคม

5.1. องค์กรต้องกำกับดูแลให้การพัฒนาและการใช้งานเทคโนโลยีปัญญาประดิษฐ์ (AI) มุ่งเน้นสร้างประโยชน์ (Beneficence) ต่อผู้ใช้งาน องค์กร และสังคม โดยต้องมีการประเมินคุณค่า (Value Assessment) และผลกระทบเชิงบวกก่อนการนำ AI ไปใช้ในกระบวนการใด ๆ เช่น การสนับสนุนให้เกิดการตัดสินใจที่ถูกต้องแม่นยำยิ่งขึ้น การเพิ่มประสิทธิภาพในการทำงาน หรือการทำความเข้าใจพฤติกรรมของลูกค้าเพื่อยกระดับการให้บริการและการตลาด ทั้งนี้ การใช้งาน AI ต้องไม่ก่อให้เกิดความเดือดร้อนหรือผลกระทบด้านลบต่อบุคคลใด เช่น การละเมิดความเป็นส่วนตัว การเลือกปฏิบัติ การสร้างอคติ หรือการก่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัย

5.2. ไม่นำข้อมูลภายในของบริษัท ทั้งที่เป็นข้อมูลลับหรือข้อมูลที่ยังไม่เผยแพร่ต่อสาธารณะ มาใช้งานกับระบบ AI โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

5.3. ต้องคำนึงถึงกฎหมาย ข้อบังคับ กฎระเบียบ เมื่อมีการใช้ A.I. เป็นส่วนหนึ่งของการประมวลผลข้อมูลส่วนบุคคลขององค์กร ต้องเป็นไปตามข้อกำหนดด้านความเป็นส่วนตัวของข้อมูล เช่น GDPR (ยุโรป), PDPA (ไทย)

5.4. องค์กรต้องมีการกำกับดูแลเพื่อให้มั่นใจว่าการตัดสินใจของ AI มีความโปร่งใส ตรวจสอบย้อนกลับได้ ปราศจากอคติ และอยู่ภายใต้ความรับผิดชอบที่ชัดเจน โดยต้องมีการทดสอบ ตรวจสอบ และติดตามผลลัพธ์ของ AI เป็นระยะ พร้อมมีผู้รับผิดชอบกำกับดูแล (Human Oversight) ในกรณีที่ AI มีผลกระทบต่อการดำเนินงานหรือการตัดสินใจในระดับสำคัญขององค์กร

บทลงโทษทางวินัย

เพื่อความเป็นระเบียบเรียบร้อยในการปฏิบัติงานของพนักงาน และเพื่อให้เกิดความเป็นธรรมต่อการพิจารณาลงโทษทางวินัย บริษัทฯ จึงกำหนดบทลงโทษทางวินัย โดยพิจารณาและลงโทษตามความหนักเบาของความผิดตามระเบียบข้อบังคับพนักงานของ ซึ่งอาจครอบคลุมถึงทุกสถานะการณ์ได้ ดังนั้นการพิจารณาบทลงโทษจึงอยู่ในดุลพินิจของบริษัทฯ โดยคำนึงถึงการสร้างสรรค์แรงงานสัมพันธ์อันดีเพื่อให้เกิดความเป็นธรรมและความเสมอภาคแก่พนักงานทุกคน

เอกสารแนบท้าย 1 จรรยาบรรณการทำงานของคู่ค้าศุภาลัย

จรรยาบรรณการทำงานของคู่ค้าศุภาลัย

บริษัท ศุภาลัย จำกัด (มหาชน) ("บริษัทฯ") และบริษัทในเครือ (รวมเรียกว่า "ศุภาลัย") มีความมุ่งมั่นอย่างเต็มที่ที่จะดำเนินธุรกิจให้เติบโตอย่างยั่งยืนควบคู่กับการรับผิดชอบต่อสังคม สิ่งแวดล้อม จึงให้ความสำคัญกับการบริการจัดการห่วงโซ่อุปทานและพัฒนาให้เกิดขึ้นอย่างเป็นรูปธรรมผ่านการกำกับดูแลคู่ค้าของศุภาลัย ทั้งนี้ การที่คู่ค้าปฏิบัติตามแนวทางนี้

จะสะท้อนให้เห็นถึงความมุ่งมั่นของคู่ค้าที่จะร่วมมือและก้าวเดินหน้าไปพร้อมกับศุภาลัยเพื่อส่งเสริมการดำเนินธุรกิจระหว่าง คู่ค้า และศุภาลัยให้เป็นไปอย่างยั่งยืน

หลักจรรยาบรรณ หมายถึง การระบุข้อกำหนดด้านจริยธรรมขั้นพื้นฐานและข้อกำหนดในการดำเนินธุรกิจของศุภาลัย สำหรับคู่ค้าของศุภาลัย เพื่อผลักดันและส่งเสริมให้คู่ค้ามีการดำเนินงานอย่างมีจริยธรรม เกิดความรับผิดชอบต่อสังคมมีการดูแลอาชีวอนามัย ความปลอดภัยของลูกจ้าง รวมถึงการให้ความสำคัญต่อการบริหารจัดการสิ่งแวดล้อมอย่างยั่งยืน

คู่ค้ามีหน้าที่รับผิดชอบในการดำเนินการเพื่อให้แน่ใจว่ากรรมการ เจ้าหน้าที่ พนักงาน ตัวแทน ผู้แทน คู่ค้า ผู้รับจ้างและหุ้นส่วนธุรกิจอื่น ๆ ทั้งหมดเข้าใจและมีหน้าที่ปฏิบัติตามข้อกำหนดต่าง ๆ ที่ระบุไว้ในหลักจรรยาบรรณที่ครอบคลุมการบริหารความเสี่ยง จัดการความเสี่ยง รวมทั้งกำหนดแนวทางการควบคุม พร้อมทั้งกำหนดให้มีการติดตามความคืบหน้าในประเด็นเหล่านี้อย่างเป็นรูปธรรม โดยคู่ค้าตกลงที่จะแจ้งให้ศุภาลัยทราบเป็นลายลักษณ์อักษรหากคู่ค้าทราบหรือสงสัยว่ามีการละเมิดหลักจรรยาบรรณนี้

1. **จริยธรรมและความโปร่งใสในการดำเนินธุรกิจ**

1.1. การต่อต้านการให้สินบน/การทุจริต

การแข่งขันอย่างถูกต้องโดยอาศัยคุณสมบัติของผลิตภัณฑ์และบริการของตน คู่ค้าต้องไม่เสนอสัญญาอนุญาต หรือจัดหาผลประโยชน์หรือสิ่งของมีค่าไม่ว่าทางตรงหรือทางอ้อม (รวมถึงแต่ไม่จำกัดเฉพาะของกำนัลหรือธรรมเนียมปฏิบัติทางธุรกิจ) โดยมีจุดประสงค์หรือเพื่อให้ส่งผลที่จะโน้มน้าวบุคคลใดบุคคลหนึ่งให้ปฏิบัติหน้าที่หรือมอบข้อได้เปรียบที่ไม่เป็นธรรมให้แก่ศุภาลัย, คู่ค้าหรือบุคคลอื่น ด้วยเหตุนี้คู่ค้าจะปฏิบัติตามและจะกำหนดให้พนักงาน ตัวแทน และผู้รับจ้างของตนปฏิบัติ

1.2. การปฏิบัติทางธุรกิจที่เป็นธรรม

การไม่มีส่วนเกี่ยวข้องในการดำเนินการใดๆ ที่เป็นการแข่งขันในการปฏิบัติทางธุรกิจที่ไม่เป็นธรรม ไม่ว่าจะดำเนินการในนามของศุภาลัย, คู่ค้า หรือบุคคลอื่นใดก็ตาม ด้วยเหตุนี้คู่ค้าต้องไม่ทำการสมยอมในการเสนอราคา (ฮั้วประมูล) กำหนดราคาร่วมกัน หรือจัดหาหรือแลกเปลี่ยนลูกค้า, เปิดเผยข้อมูลที่ละเอียดอ่อนด้านการแข่งขันของศุภาลัย หรือของคู่ค้า หรือของบุคคลอื่นกับบรรดาคู่แข่งศุภาลัย หรือบรรดาคู่แข่งของคู่ค้า คู่ค้าต้องไม่ใช้อำนาจเหนือตลาดของตนในทางมิชอบ ไม่ว่าจะเพื่อผลประโยชน์ของตนหรือเพื่อผลประโยชน์ของผู้อื่น โดยการปฏิเสธที่จะซื้อขายอย่างเป็นธรรม, มีส่วนร่วมในแนวทาง

ปฏิบัติด้านราคาที่มุ่งขจัดคู่แข่งขันหรือเลือกปฏิบัติ, กำหนดเงื่อนไขการขายหรือจัดหาสินค้าหรือบริการโดยพ่วงกับสินค้าหรือบริการอีกอย่างหนึ่ง หรือดำเนินยุทธวิธีที่ไม่ถูกต้องที่คล้ายกันอื่นๆ คู่ค้าต้องไม่มีส่วนร่วมในแนวทางปฏิบัติด้านการตลาดที่เป็นการหลอกลวงหรือไม่เป็นธรรมอื่นๆ ไม่ว่าจะในนามของศุภาลัย, คู่ค้า หรือบุคคลอื่น ๆ นอกจากนี้ คู่ค้าต้องไม่ให้ข้อมูลอันเป็นเท็จเกี่ยวกับสินค้าหรือบริการของศุภาลัย, ของคู่ค้า หรือของบุคคลอื่น ๆ ในทำนองเดียวกันคู่ค้าต้องไม่ใส่ร้ายป้ายสีคู่แข่งของศุภาลัยหรือคู่แข่งของคู่ค้า หรือสินค้าหรือบริการของพวกเขา

1.3. การรักษาความลับ ปกป้องข้อมูล การคุ้มครองข้อมูลส่วนบุคคล และการดูแลรักษาการบันทึกข้อมูล

การเก็บรักษาความลับ ปกป้องข้อมูล และคุ้มครองข้อมูลส่วนบุคคลให้มีความปลอดภัย โดยใช้มาตรการที่เหมาะสมเพียงพอที่จะการรักษาความปลอดภัยของข้อมูล และจำกัดการเข้าถึงข้อมูลส่วนบุคคล รวมถึงจำกัดเฉพาะความเสี่ยงจากการทำลายทิ้งโดยไม่ได้ตั้งใจ การสูญหาย การแก้ไข การเปิดเผยโดยไม่ได้รับอนุญาตการจัดทำและรักษาบันทึกข้อมูลที่ถูกต้องและสมบูรณ์ เพื่อรับรองถึงการมีความรับผิดชอบ และไม่เปลี่ยนแปลงหรือละเว้นบันทึกข้อมูลใดๆ เพื่อปกปิดหรือแสดงข้อมูลเหตุการณ์ หรือธุรกรรมที่บันทึกเอกสารไว้อย่างเป็นเท็จ บันทึกข้อมูลต้องได้รับการเก็บรักษาและลบทิ้ง

1.4. ความขัดแย้งทางผลประโยชน์

การหลีกเลี่ยงสถานการณ์ใดๆ ที่อาจทำให้ถูกมองว่าเกิดกรณีความขัดแย้งทางผลประโยชน์ขึ้นในทำนองเดียวกันคู่ค้าต้องไม่เข้าทำข้อตกลงทางธุรกิจใด ๆ กับกรรมการ พนักงาน หรือตัวแทนใด ๆ ของศุภาลัย ซึ่งอาจส่งผลต่อการปฏิบัติหน้าที่ที่ไม่เหมาะสมต่อศุภาลัย

2. มาตรฐานด้านคุณภาพ ความต่อเนื่องทางธุรกิจ

2.1. มาตรฐานด้านคุณภาพ การส่งมอบผลิตภัณฑ์และบริการตามข้อกำหนดและข้อตกลงร่วมกัน และให้ความร่วมมือกับศุภาลัยในการพัฒนาคุณภาพผลิตภัณฑ์และบริการ

2.2. ความต่อเนื่องทางธุรกิจ การจัดให้มีแผนความต่อเนื่องทางธุรกิจ เพื่อให้สามารถจัดส่งผลิตภัณฑ์และบริการให้กับศุภาลัยได้อย่างต่อเนื่อง ทั้งกรณีที่ศุภาลัยมีความต้องการผลิตภัณฑ์และบริการเพิ่มขึ้น หรือในกรณีที่การดำเนินงานของคู่ค้าเกิดปัญหาจากการหยุดชะงักของการผลิต

3. สิทธิมนุษยชน

3.1. การปฏิบัติอย่างเท่าเทียม คู่ค้าจะเคารพในความแตกต่าง ความหลากหลาย ของพนักงาน ลูกค้า และบุคคลอื่นๆ ที่มีการติดต่องานกัน ต้องไม่เลือกปฏิบัติบนพื้นฐานของสถานะของบุคคล เช่น เชื้อชาติ สีผิว ศาสนา ชาติกำเนิด เพศ รสนิยมทางเพศ อัตลักษณ์ทางเพศ อายุ ความพิการ บุคลิกลักษณะอื่นใด ๆ รวมถึงความนิยมทางการเมือง

3.2. สถานที่ทำงานที่มั่นคงและปลอดภัย คู่ค้าจะจัดให้มีสถานที่ทำงานที่มั่นคงและปลอดภัยสำหรับพนักงานทุกคนของตน และป้องกันการเกิดอุบัติเหตุแก่พนักงาน ลูกค้า และผู้มาเยือน ผู้บริหารของคู่ค้าจะดำเนินการให้แน่ใจว่ามีการปฏิบัติตามความมุ่งมั่นนี้ในสถานประกอบการและโรงงานทุกแห่งที่คู่ค้าเปิดดำเนินงาน

3.3. ชั่วโมงการทำงาน ค่าตอบแทนและสิทธิประโยชน์ คู่ค้าจ่ายค่าตอบแทนให้แก่ลูกจ้างอย่างเป็นธรรม มุ่งมั่นที่จะเป็นนายจ้างที่มีจริยธรรม เคารพในการมีส่วนร่วมของพนักงาน การให้รางวัลอย่างเป็นธรรม รวมถึงสิทธิประโยชน์ที่ลูกจ้างพึงได้รับ

3.4. การปฏิบัติต่อมนุษย์ คู่ค้าจะเคารพในสิทธิของพนักงานและให้ความมั่นใจแก่พนักงานจะไม่มีการปฏิบัติที่รุนแรง ไม่มีมนุษยธรรมรวมถึงการละเมิดทางร่างกาย วาจา และใจ หรือข่มขู่

3.5. เสรีภาพในการเข้าร่วม คู่ค้าจะเคารพในสิทธิของพนักงานและให้เสรีภาพในการเข้าร่วมสมาคมและการเจรจาต่อรองร่วมกัน

3.6. การปกป้องการใช้แรงงานเด็ก คู่ค้าจะปกป้องการบังคับใช้แรงงานในเด็ก หรือ ในงานที่ผิดกฎหมาย หรือมีอันตราย และส่งผลต่อสุขภาพศีลธรรม ตลอดจนสภาพจิตใจของเด็ก

4. อาชีวอนามัยและความปลอดภัย

การจัดให้มีพื้นที่ปฏิบัติงานและสภาพแวดล้อมในการทำงานที่ปลอดภัย และถูกสุขลักษณะ และป้องกันมิให้พนักงานของตนต้องเผชิญความเสี่ยงด้านความปลอดภัยที่อาจเกิดขึ้นในลักษณะ: (1) การจัดหาอุปกรณ์ป้องกันภัยผู้ทำงานที่เสี่ยงอันตราย (2) ส่งเสริมให้พนักงานรายงานถึงการบาดเจ็บที่เกี่ยวกับงาน (3) จัดประเภทและบันทึกกรณีการบาดเจ็บและความเจ็บป่วยที่เกี่ยวกับงาน (4) จัดให้มีการรักษาพยาบาลที่จำเป็น และ (5) ตรวจสอบและดำเนินมาตรการแก้ไขเพื่อขจัดสาเหตุของการบาดเจ็บและความเจ็บป่วยดังกล่าว

5. สิ่งแวดล้อมและความยั่งยืน

ความพยายามลดผลกระทบที่ไม่พึงประสงค์ต่อชุมชน สิ่งแวดล้อมและทรัพยากรธรรมชาติให้เหลือน้อยที่สุด เพื่อป้องกันสุขภาพและความปลอดภัยของประชาชนทั่วไป โดยกำหนดมาตรการป้องกันและลดผลกระทบทางสิ่งแวดล้อมลดการปล่อยก๊าซเรือนกระจกที่ส่งผลต่อการเปลี่ยนแปลงสภาพภูมิอากาศ

6. ความรับผิดชอบต่อสังคม / การดูแลสังคมและชุมชน

ความใส่ใจคำนึงถึงการจัดให้มีกิจกรรม หรือเข้าร่วม ให้ความร่วมมือกับชุมชนอย่างสร้างสรรค์เพื่อพัฒนาชีวิตชุมชนและสังคมอย่างยั่งยืน

7. ช่องทางการติดต่อ

ศุภาลัยได้จัดเตรียมช่องทางเพื่อที่พนักงานและผู้มีส่วนได้ส่วนเสีย (รวมถึงคู่ค้า ผู้รับเหมาช่วงและพนักงานของพวกเขา) ทำการสอบถามและแจ้งข้อกังวลเกี่ยวกับหลักจรรยาบรรณนี้และหลักปฏิบัติในการดำเนินธุรกิจ ผ่านทางสายด่วนให้ความช่วยเหลือด้านจริยธรรมของศุภาลัย ซึ่งเป็นวิธีการที่เป็นความลับและสามารถแจ้งข้อกังวลโดยไม่ต้องระบุชื่อผู้แจ้ง สายด่วนให้ความช่วยเหลือด้านจริยธรรมของศุภาลัยเปิดให้บริการผ่านช่องทาง Anti-corruption@supalai.com

8. การยืนยันการปฏิบัติตามหลักจรรยาบรรณของศุภาลัย

คู่ค้ารับทราบและตกลงว่าคู่ค้ามีหน้าที่รับผิดชอบในการปฏิบัติตามจรรยาบรรณนี้อย่างเต็มรูปแบบ ทั้งนี้ เพื่อให้เกิดการพัฒนาการบริหารห่วงโซ่อุปทานร่วมกันอย่างเป็นรูปธรรม และสร้างความยั่งยืนต่อคู่ค้าและศุภาลัย ดังนั้น ศุภาลัยทำการประเมินการปฏิบัติตามหลักจรรยาบรรณนี้ ตั้งแต่วันที่มีการลงนามรวมถึงการสำรวจสถานประกอบการของคู่ค้ารวมถึงการขอข้อมูลที่น่าเชื่อถือที่แสดงว่าคู่ค้าปฏิบัติตามหลักจรรยาบรรณนี้

คู่ค้าจะให้ความร่วมมือแก่ศุภาลัยอย่างเต็มที่ในการประเมินดังกล่าว และจะทำการแก้ไขโดยทันที หากพบว่ามีการปฏิบัติใดๆ ที่ไม่เป็นไปตามหลักจรรยาบรรณฯ ในกรณีที่พบการไม่ปฏิบัติตามหลักจรรยาบรรณฯ ศุภาลัยอาจกำหนดให้มีการตรวจสอบอย่างสม่ำเสมอโดยผู้ตรวจสอบอิสระที่คัดเลือกโดยศุภาลัย โดยคู่ค้าตกลงให้มีการตรวจสอบและยอมรับในการชำระค่าใช้จ่ายที่เกิดขึ้น

คู่ค้ารับทราบและยินยอมลงนามรับรองและประทับตราบริษัท

ข้าพเจ้า _____ กรรมการผู้มีอำนาจลงนาม

ของ _____ ยินยอมปฏิบัติตามจรรยาบรรณฯ ข้างต้น

ลายเซ็น _____

วันที่ ___/____/_____

ตราประทับ

เอกสารแนบท้าย 2 แบบประเมินความเสี่ยง IT และ Cyber Security สำหรับผู้รับจ้างภายนอก

SUPALAI

แบบประเมินความเสี่ยงด้าน IT และ Cyber Security
สำหรับผู้รับจ้างภายนอก

<u>ส่วนที่ 1</u> : **รายละเอียดของผู้รับจ้างภายนอก**	**วันที่ประเมิน** .....
ชื่อผู้รับจ้างภายนอก	....
ประเภทของกลุ่มที่เข้าถึงข้อมูลของบริษัทฯ	☐ ผู้ให้บริการงานด้าน IT ☐ ผู้ที่สามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้าของบริษัท ☐ ผู้ที่สามารถเข้าใช้ระบบงานภายในของบริษัทฯ ได้ เช่น ระบบ CM / CRM หรืออื่นๆ ☐ อื่นๆ.....
รายละเอียดงานที่ดำเนินการให้กับบริษัทฯ :	
(1) ชื่อผู้จัดทำ..... ตำแหน่ง..... โทรศัพท์..... E-mail..... ลงชื่อ..... ผู้ทำแบบประเมิน	
(2) ชื่อผู้จัดทำ..... ตำแหน่ง..... โทรศัพท์..... E-mail..... ลงชื่อ..... ผู้ทำแบบประเมิน	

ส่วนที่ 2 : สำหรับผู้รับจ้างภายนอกประเมินความเสี่ยงของธุรกิจตนเอง
กรุณาทำเครื่องหมาย / หรือกรอกข้อมูลคำตอบ และอธิบายรายละเอียดเพิ่มเติม (ถ้ามี)

หัวข้อการประเมิน	รายละเอียดการประเมิน	คำตอบแบบประเมิน และรายละเอียดประกอบการตอบ
① **นโยบาย/มาตรการรักษาความมั่นคงปลอดภัยด้าน IT** (เพื่อให้มั่นใจได้ว่าบริษัทมีการบริหารจัดการความเสี่ยงด้าน IT อย่างเพียงพอ และเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล)	1.1 มีกรรมการ หรือที่ปรึกษา อย่างน้อย 1 ท่าน ที่มีคุณสมบัติอย่างใดอย่างหนึ่ง ดังนี้ - จบการศึกษาในสาขา IT - มีความรู้หรือประสบการณ์ด้าน IT - มีประวัติการอบรมหรือการสัมมนาด้าน IT ในปีล่าสุด เช่น การอบรมเพื่อสร้างความตระหนักด้านความปลอดภัยทางไซเบอร์ เป็นต้น	
	1.2 จัดให้มีนโยบาย/มาตรการรักษาความมั่นคงปลอดภัยด้าน IT (IT Policy / Procedure)	
	1.3 จัดให้มีแผนบริหารจัดการเหตุการณ์ผิดปกติด้าน IT (IT Incident Response Plan) หากเกิดการบุกรุกโจมตีหรือการรั่วไหลของข้อมูลอย่างทันท่วงที	
② **การรักษาความปลอดภัยขั้นพื้นฐาน / แนวปฏิบัติเรื่องการจัดการความเสี่ยงทางไซเบอร์ (Cyber Security Procedure)**	2.1 มีเครื่องมือป้องกันความเสี่ยงด้าน Cyber Security อะไรบ้าง เช่น - Antivirus - Firewall - VPN - การติดตั้ง Patch	
	2.2 มีวิธีการควบคุมการเข้าถึงข้อมูลภายในของบริษัทอย่างไร (Data Access Procedure) ตัวอย่างเช่น - กำหนดหน้าที่ผู้อนุมัติการเข้าถึงข้อมูล (Access) ซึ่งต้องมีการอนุมัติก่อนการยินยอมให้มีการเข้าถึงข้อมูล - กำหนดรูปแบบ / วิธีการยืนยันตัวตน (Authentication) - กำหนดสิทธิ์และมีการบันทึกการเข้าใช้งาน (Authentication, Authorization, and Accounting)	

หัวข้อการประเมิน	รายละเอียดการประเมิน	คำตอบแบบประเมิน และรายละเอียดประกอบการตอบ
③ **ประวัติการถูกโจมตีทางไซเบอร์ หรือระบบเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ (Significant Cyber-Attack History)**	3.1 ประวัติเกี่ยวกับการรั่วไหลของข้อมูล (Data Breach History) ของบริษัท	
	3.2 ประวัติการถูกบุกรุกโจมตี โดย Computer Virus, Ransomware และ Malware ในปีล่าสุด	โปรดระบุ : ○ ไม่พบการบุกรุกโจมตี ○ ตรวจพบการบุกรุกโจมตี แต่สามารถป้องกันได้จากระบบตรวจจับของบริษัท เช่น Firewall, Antivirus, Gateway, Proxy ○ ตรวจพบ Computer Virus ที่อุปกรณ์ผู้ใช้งาน เช่น ระบบ Antivirus เครื่องคอมพิวเตอร์ ○ ตรวจพบ Computer Virus ที่เครื่องแม่ข่ายองค์กร (ไม่นับรวม Gateway) ○ ตรวจพบ Computer Virus แต่ไม่ทราบ/ไม่สามารถระบุได้ว่ามาจากที่ใด ○ อื่น ๆ (โปรดระบุ)..... .....
	3.3 ประวัติการถูกร้องเรียน หรือแจ้งเหตุการณ์ เกี่ยวกับภัยไซเบอร์จากผู้มีส่วนได้เสียในปีล่าสุด เช่น โดนขโมยบัญชีผู้ใช้งาน หรือข้อมูลส่วนบุคคลรั่วไหล เป็นต้น และมีแนวทางแก้ไขอย่างไร	โปรดระบุ : ○ ไม่เคยมีประวัติดังกล่าว ○ เคยมีประวัติ (โปรดระบุเหตุการ และจำนวนครั้งที่ถูกร้องเรียนหรือแจ้งเหตุในปีล่าสุด) ....
④ **การใช้งาน Cloud หรือ Hosting Service**	4.1 ลักษณะรูปแบบที่บริษัทใช้ Cloud Service หรือ Hosting Service	โปรดระบุ : ○ ไม่มีการใช้งาน (ข้ามไปข้อ 5) ○ Private Cloud หรือ Hosting Service หรือบริษัทในเครือ ○ Public Cloud, Hybrid ○ อื่น ๆ (โปรดระบุ)..... .....

หัวข้อการประเมิน	รายละเอียดการประเมิน	คำตอบแบบประเมิน และรายละเอียดประกอบการตอบ
	4.2 จำนวนระบบงาน หรือ Application ที่สำคัญ ที่ใช้ในการประมวลผลหรือสนับสนุนกิจกรรมของบริษัทซึ่งอยู่บน Cloud หรือ Hosting Services ซึ่งเมื่อหยุดชะงักแล้วส่งผลกระทบต่อการดำเนินธุรกิจ	โปรดระบุจำนวนระบบงานหรือ Application ที่สำคัญ ระบบที่(1)..... ระบบที่(2)..... ระบบที่(3)..... โปรดระบุชื่อ Cloud Provider / Hosting Service ที่ใช้บริการอยู่ ....
⑤ **บริษัทมีผู้ให้บริการภายนอกที่สามารถเข้าถึงเครือข่าย/ระบบงานภายในบริษัทได้ (Third Parties, Vendor, Outsourcer, Sub-Contractor)**	5.1 จัดให้มีสัญญาจ้างงานระบุเงื่อนไขหรือข้อตกลงครอบคลุมหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยที่เกี่ยวกับ IT Policy หรือไม่ เช่น มีการระบุความจำเป็นในการทำสัญญาไม่เปิดเผยความลับระหว่างองค์กรกับผู้รับจ้างภายนอก	
	5.2 จำนวนบริษัทผู้ให้บริการภายนอกที่สามารถเข้าถึงเครือข่ายภายในของบริษัทได้ (Third Parties, Vendor, Outsourcer, Sub-Contractor)	โปรดระบุจำนวนผู้ให้บริการภายนอกและประเภทบริการที่ใช้ ○ จำนวนผู้ให้บริการ.....ราย ○ ประเภทบริการ รายที่ 1 ..... รายที่ 2 ..... รายที่ 3..... รายที่ 4.....
	5.3 วิธีการหรือช่องทางที่ผู้ให้บริการภายนอกเข้าถึงเครือข่าย หรือทรัพยากรภายในของบริษัท	โปรดระบุ ○ ผู้ให้บริการต้องเข้ามา Onsite เท่านั้น ○ ผู้ให้บริการสามารถใช้ช่องทางเฉพาะ เช่น Leased Line หรือ VPN เข้ามาให้บริการ ○ อื่น ๆ..... ....

หัวข้อการประเมิน	รายละเอียดการประเมิน	คำตอบแบบประเมิน และรายละเอียดประกอบการตอบ
	5.4 แนวทางการบริหารจัดการ Sub-Contract (การจ้างช่วง) เช่น ○ การแจ้งผู้ประกอบธุรกิจ เมื่อมีการใช้งานหรือเปลี่ยนแปลง Sub-Contract ○ ความรับผิดชอบของผู้ให้บริการในกรณีที่มีการใช้งาน Sub-Contract	
⑥ **การรับประกันความเสียหาย**	6.1 บริษัทได้ทำประกันภัยกรณีเกิดความเสียหายจากภัยคุกคามทางไซเบอร์ไว้ครอบคลุมหรือไม่	
⑦ **การอบรม/สร้างความตระหนัก (Training / Awareness)**	7.1 การจัดทำแผนการอบรมเพื่อสร้างความตระหนักและให้ความรู้แก่พนักงาน ลูกจ้าง ผู้ให้บริการภายนอก หรือผู้ที่เกี่ยวข้องอื่น ๆ เช่น การอบรมด้านนโยบายและขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัยด้าน IT อย่างสม่ำเสมอ	
⑧ **การจัดให้มีผลการตรวจสอบด้าน IT โดยผู้ตรวจสอบภายนอกที่มีความเป็นอิสระและได้มาตรฐานสากล**	8.1 จัดให้มีผู้ตรวจสอบการดำเนินงานและการควบคุมภายในด้าน IT จากหน่วยงานภายนอก	การตรวจสอบตามมาตรฐาน ○ SSAE 18 (SOC 2 Type 2 Report) ○ PCI-DSS Attestation of Compliance (AOC) ○ อื่น ๆ (โปรดระบุ) ....