ภาพรวม ISO 27001:2022

ISO คืออะไร?

ISO คือ ข้อกำหนดที่มุ่งเน้นให้องค์กรมีระบบการทำงานที่มีมาตรฐาน โดยที่ ISO แต่ละหมายเลขก็จะเน้นไปที่หัวข้อที่แตกต่างกันออกไป เช่น

- ISO 9001 : การผลิตสินค้าหรือบริการที่มีคุณภาพ
- ISO 27001 : รักษาความปลอดภัยของข้อมูลในองค์กร

ISO 27001:2022

START HERE

กำหนดขอบข่ายและขอบเขตของระบบ

กำหนดแนวทางของระบบและแต่งตั้งทีมงานที่ช่วยจัดทำและดูแลระบบ

จัดทำนโยบายและกระบวนการทำงานจากการประเมินความเสี่ยง

กำหนดเป้าหมายของระบบ, จัดเตรียมทรัพยากรที่จำเป็น และกำหนดแนวทางในการบริหารระบบ

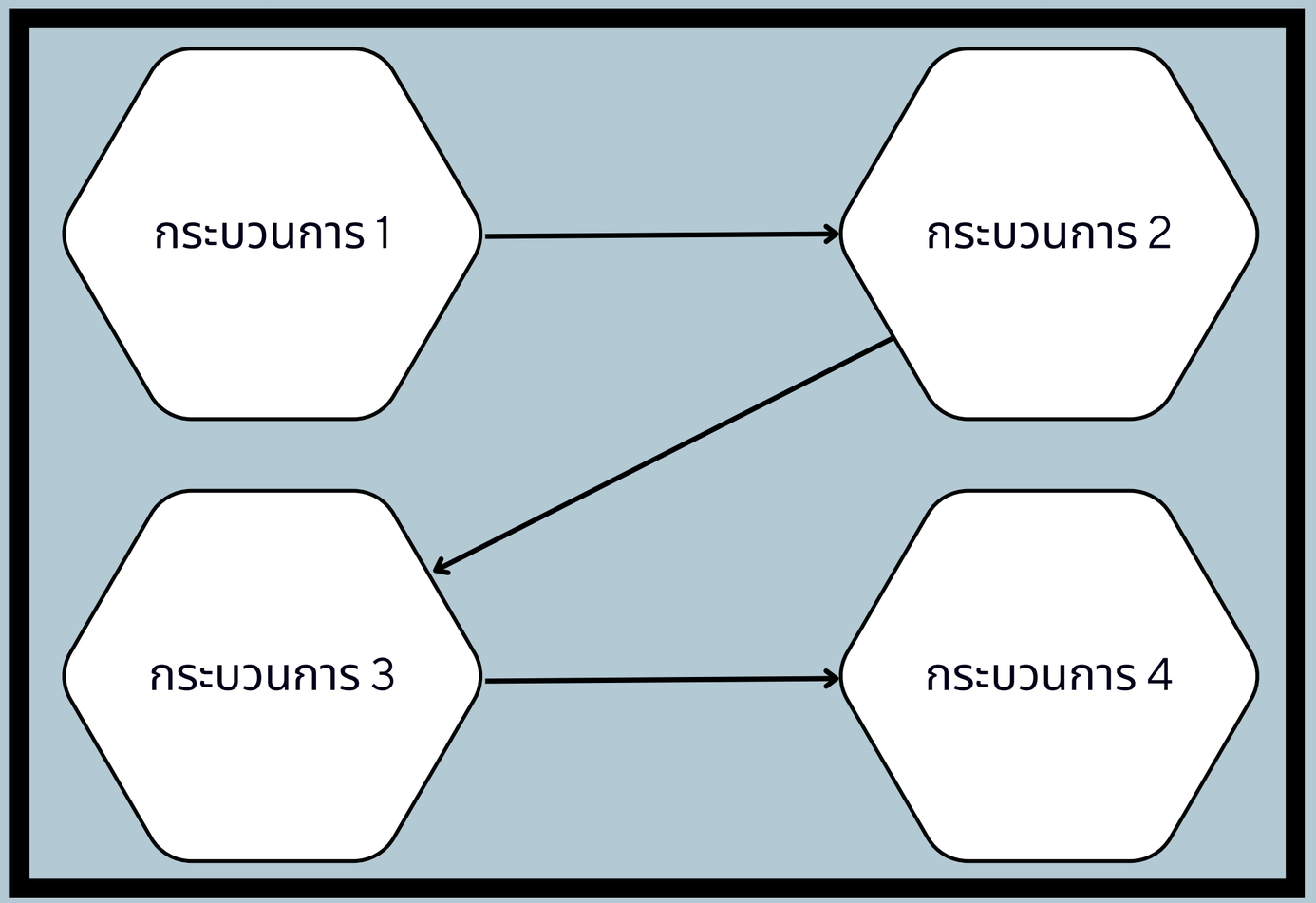
ดำเนินการตามระบบที่จัดทำขึ้น

ตรวจสอบการดำเนินงาน, แก้ไขสิ่งที่ผิดพลาดและพัฒนาระบบอย่างต่อเนื่อง

กำหนดขอบข่าย
และ
ขอบเขตของระบบ

บริบทขององค์กร

ความต้องการของผู้มีส่วนได้ส่วนเสีย

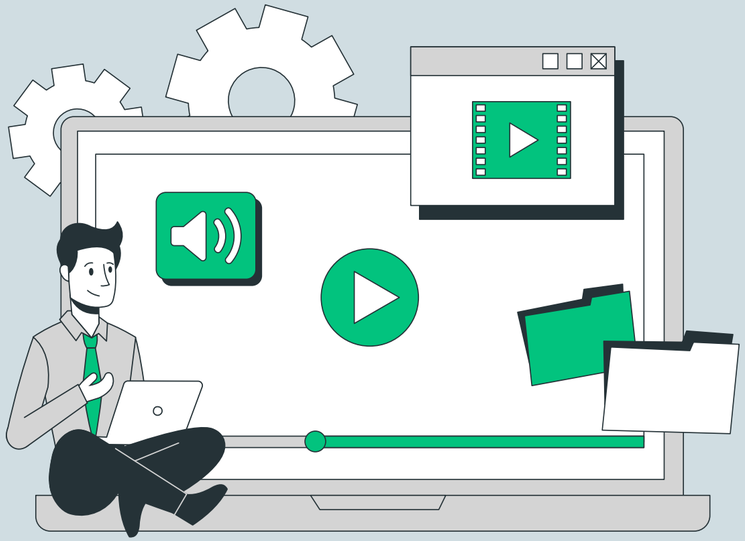


ขอบข่าย/ขอบเขตของระบบบริหาร

กำหนดแนวทางของระบบ และแต่งตั้งทีมงานที่ช่วย จัดทำและดูแลระบบ

ทีมงาน

- จัดทำ
- ดูแล
- รายงานผล



ระบบ

ผู้บริหาร

- ข้อมูลปลอดภัย
- ระบบพร้อมใช้
- พัฒนาต่อเนื่อง

ธรรมาภิบาลข้อมูล

จัดทำนโยบายและกระบวนการทำงานจากการประเมินความเสี่ยง

ประเมินความเสี่ยง → คิดล่วงหน้าว่าจะเกิดปัญหาอะไรบ้าง

ปัญหา

รุนแรงแค่ไหน

เกิดบ่อยแค่ไหน

มาก

น้อย

มาก

น้อย

รับไม่ได้	✗
รับได้	✓

รับไม่ได้ → ทำแผนลดความเสี่ยง

รับได้ → ตั้งนโยบาย/กระบวนการทำงาน เพื่อควบคุม

อ้างอิง → ภาคผนวก A 93 ข้อ

เขียนอธิบายใน → SOA

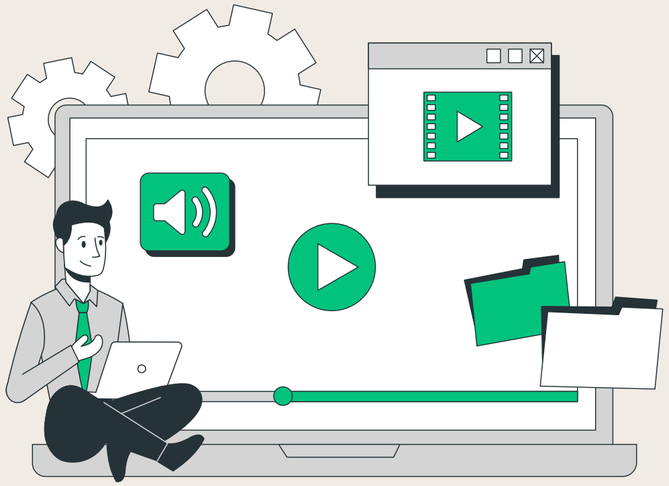
EXAMPLE

ระดับความเสี่ยง = (1 - 25)	ความรุนแรง x โอกาสเกิด (1-5)	(1-5)
1 - 12 รับได้ ✓	1 : ไม่กระทบ	1 : 2 ปี/ครั้ง
15 - 25 รับไม่ได้ ✗	3 : ข้อมูลหลุดในองค์กร ระบบล่ม 1-2 ชั่วโมง	3 : 6 เดือน/ครั้ง
	5 : ข้อมูลหลุดไปนอกองค์กร ระบบล่มเกิน 4 ชั่วโมง	5 : เดือนละครั้ง

EXAMPLE

✓	รับได้	ส่งข้อมูล	ปัญหา → การรับมือ 1. ส่งผิดคน → ทวนสอบก่อนส่ง 2. ส่งข้อมูลเก่า → ทวนสอบ,อัพเดตข้อมูลเสมอ
✗	รับไม่ได้	ระบบ Network	1.ไม่มีอุปกรณ์ป้องกัน (Firewall) → ทำแผนจัดซื้อ Firewall ภายใน 1 เดือน

กำหนดเป้าหมายของระบบ, จัดเตรียมทรัพยากรที่จำเป็น และกำหนดแนวทาง ในการบริหารระบบ



ระบบ

นโยบาย

เป้าหมาย

ข้อมูลปลอดภัย → ข้อมูลรั่วไหล = 0 ครั้ง

ระบบพร้อมใช้ → UPTIME > 99.9%

พัฒนาต่อเนื่อง → อบรมพนักงานปีละ 1 ครั้ง

ทำอะไร
ใครทำ
ทรัพยากรที่ใช้
ระยะเวลา
การวัดผล

→ แผนที่จะทำให้บรรลุผล

การเปลี่ยนแปลง

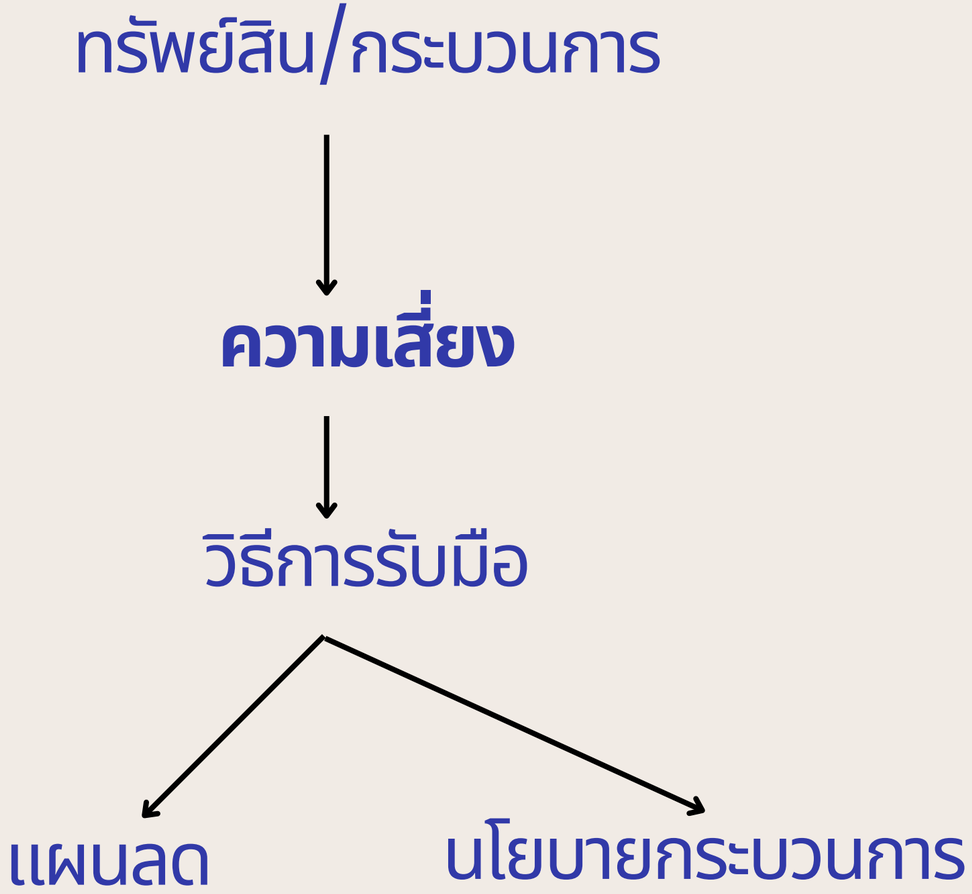
ภายใน – ต้องเปลี่ยนอุปกรณ์
– ปรับกระบวนการทำงานใหม่
– ย้ายสถานที่ทำงาน

ภายนอก – ความต้องการของลูกค้า
– เทคโนโลยีใหม่ๆ
– ภัยคุกคามทางไซเบอร์

วิเคราะห์

ผลกระทบ

สิ่งที่เปลี่ยนแปลง



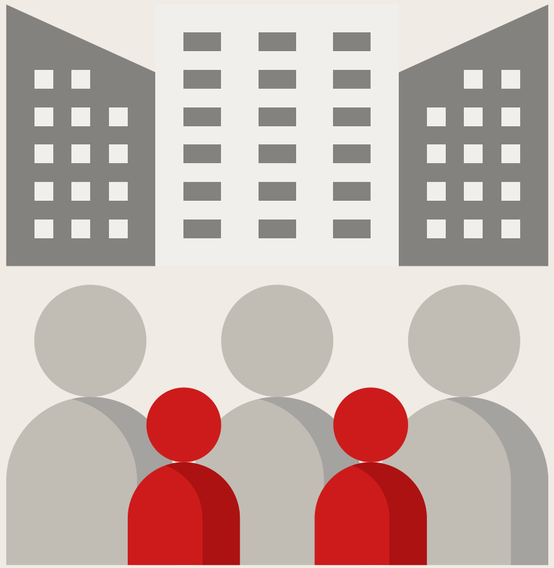
นโยบาย
กระบวนการทำงาน

การมีส่วนร่วม

ผลเสียหากไม่
ทำตาม

พนักงาน

องค์กร



ภายใน

ภายนอก

- สื่อสารอะไร
- เมื่อไร
- ใครสื่อสาร
- สื่อสารอย่างไร

กำหนดแนวทางของระบบเอกสารและข้อมูลในองค์กร (7.5)

- ระบบเอกสารและข้อมูลสามารถแตกต่างกันได้ในแต่ละองค์กร ขึ้นกับขนาดและความซับซ้อนขององค์กร

ระบบเอกสารและข้อมูลจะต้อง

(1) มีการชี้บ่งชัดเจน
(2) อยู่ในรูปแบบที่เหมาะสม
(3) ผ่านการอนุมัติและมีการทบทวนอย่างเหมาะสม
(4) พร้อมใช้งานอยู่เสมอ
(5) มีการจัดเก็บดูแลอย่างเหมาะสม
(6) มีการแจกจ่าย, สามารถเข้าถึงและนำไปใช้งานอย่างเหมาะสม
(7) มีการควบคุมการเปลี่ยนแปลงเอกสารและข้อมูลให้เป็นปัจจุบัน
(8) มีการเรียกคืนเอกสารและข้อมูลที่ล้าสมัยหรือเลิกใช้งาน
(9) มีการทำลายเอกสารและข้อมูลอย่างเหมาะสม

ดำเนินการตามระบบที่จัดทำขึ้น

การดำเนินงานตามระบบบริหารที่วางไว้

หลังจากที่จัดเตรียมระบบบริหารแล้ว ให้ดำเนินงานตามระบบที่วางไว้ (ทำตามนโยบาย, กระบวนการทำงาน, ขั้นตอนการทำงานที่กำหนด) เพื่อให้บรรลุเป้าหมายที่ตั้งไว้ ทั้งพนักงานและบุคคลภายนอกที่ทำงานให้แก่องค์กร และควบคุมการเปลี่ยนแปลงที่อาจจะเกิดขึ้นด้วย (8.1)

ทำการประเมินความเสี่ยงอย่างสม่ำเสมอ

- ทำการประเมินความเสี่ยงตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงเกิดขึ้น (8.2)
- ทำการจัดการกับความเสี่ยงที่ทำการประเมินใหม่อย่างเหมาะสม (8.3)

ตรวจสอบการดำเนินงาน, แก้ไขสิ่งที่ผิดพลาด และพัฒนาระบบอย่างต่อเนื่อง

	Ex1 เป้าหมาย (KPI)	Ex2 ความพึงพอใจของลูกค้า
เฝ้าระวังอะไร	ประชุมรายเดือน	แบบประเมินความพึงพอใจ
↓ วิธีที่ใช้		
↓ ช่วงเวลา	ทุกเดือน	ทุกปี
↓ ใครดำเนินการ	ทีมงานระบบ	พนักงานฝ่ายขาย
↓ วิเคราะห์อย่างไร	ผ่านเป้าหรือไม่	ผ่านเกณฑ์หรือไม่
↓ ใครประเมินผล	ตัวแทนฝ่ายบริหาร	ผู้บริหาร

ตรวจติดตามภายใน

รายงาน

ผู้บริหาร
(ผ่านการทบทวนฝ่ายบริหาร)

แผนการตรวจที่ชัดเจน

- ความถี่
- วิธีการตรวจ
- ผู้รับผิดชอบในการตรวจ
- ข้อกำหนดในการตรวจ
- การรายงานผล

เกณฑ์และขอบข่ายในการตรวจ

- ผลการตรวจประกอบด้วย
  - ผ่าน/ไม่ผ่าน/ข้อเสนอแนะ
- กำหนดหน่วยงานที่รับตรวจให้ชัดเจน
- ผู้ตรวจไม่มีส่วนได้ส่วนเสียกับการตรวจ

ผู้บริหารทำการทบทวนระบบบริหารขององค์กร (9.3)

- ทำการวางแผนที่จะทำการทบทวนระบบบริหารขององค์กรโดยที่ผู้บริหารมีส่วนร่วมด้วย

สิ่งที่นำเสนอต่อผู้บริหาร

- ติดตามผลจากการประชุมครั้งที่แล้ว
- การเปลี่ยนแปลงที่เกี่ยวข้องกับระบบ
- ประสิทธิภาพของระบบ
  - ความไม่สอดคล้องที่เกิดขึ้น
  - ผลของการเฝ้าติดตาม
  - ผลจากการตรวจประเมิน
  - ผลของเป้าหมาย
  - ผลตอบกลับจากผู้มีส่วนได้ส่วนเสีย
- ผลของการประเมินความเสี่ยง/แผนลดความเสี่ยง
- โอกาสในการปรับปรุงระบบ

ข้อสรุปจากผู้บริหาร

- การเปลี่ยนแปลงที่จำเป็น
- สิ่งที่จะนำไปพัฒนาหรือปรับปรุง

การพัฒนาระบบบริหารอย่างต่อเนื่อง (10.1)

- องค์กรต้องทำการพัฒนาระบบบริหารที่จัดทำขึ้นอย่างต่อเนื่อง โดยระบบจะต้องมีความเหมาะสม, เพียงพอ และมีประสิทธิภาพอยู่เสมอ

เมื่อเกิดความไม่สอดคล้อง (ปัญหา)

รับมือ หาว่าปัญหานั้นส่งผลกระทบ

ทบทวนเหตุการณ์

หาสาเหตุ

- ใหม่
- เคยเกิดแล้ว

ทำการจัดการกับสาเหตุของปัญหา

- อุปกรณ์/ซอฟต์แวร์
- นโยบาย/กระบวนการทำงาน

อัพเดตความเสี่ยง

ภาคผนวก A

ภาคผนวก A
(แนวทางในการรักษาความปลอดภัยของข้อมูล)

- ภาคผนวก A สามารถแบ่งออกเป็นหัวข้อย่อยต่างๆได้ดังต่อไปนี้ (A.5 – A.8)
  - A.5 : การควบคุมเชิงนโยบาย (เป็นการควบคุมด้วยนโยบาย)
  - A.6 : การควบคุมเชิงบุคลากร (เป็นการควบคุมสำหรับบุคลากร)
  - A.7 : การควบคุมเชิงกายภาพ (เป็นการควบคุมสำหรับพื้นที่และทรัพย์สินทางกายภาพ)
  - A.8 : การควบคุมเชิงเทคโนโลยี (เป็นการควบคุมด้วยซอฟต์แวร์หรือเทคโนโลยีต่างๆ)

หรือสามารถจัดหมวดหมู่ได้ดังนี้

คน
ทรัพย์สิน
พื้นที่
ข้อมูล
ระบบเครือข่าย
การจัดหาซอฟต์แวร์
ทั่วๆไป

ผู้ให้บริการจาก
ภายนอก

กฎหมาย

ตรวจสอบ/เฝ้าระวัง

เหตุการณ์ผิดปกติ

รักษาความต่อเนื่อง
ของความปลอดภัย
ของข้อมูล

1. คน

1.1 มีกระบวนการในการคัดเลือกบุคลากรที่ชัดเจน
- กำหนดคุณสมบัติของพนักงานในด้านต่างๆ
- กระบวนคัดเลือกพนักงาน
- กระบวนการฝึกอบรมที่จำเป็น

1.2 มีการจัดทำสัญญาการจ้างงานของพนักงานที่ประกอบไปด้วย
- ความรับผิดชอบด้านความปลอดภัยของข้อมูล (พนักงานต้องทำตามนโยบายและกระบวนการที่องค์กรกำหนด)
- บทลงโทษทางวินัยในกรณีที่พนักงานฝ่าฝืนข้อกำหนดด้านความปลอดภัยของข้อมูล
- การรักษาความลับข้อมูลภายหลังจากลาออก

1.3 จัดทำสัญญารักษาความลับกับบุคลากรที่ทำงานให้กับองค์กร (ประจำ/ชั่วคราว) และต้องคอยทบทวนให้มีความเหมาะสมอยู่เสมอ

1.4 ทำการสร้างความตระหนัก และอบรมความรู้ด้านการรักษาความปลอดภัยของข้อมูลแก่พนักงานในองค์กรอย่างสม่ำเสมอ

2.ทรัพย์สิน

2.1 ทำการลงทะเบียนทรัพย์สินและกำหนดผู้รับผิดชอบให้ชัดเจน
2.2 กำหนดกฎในการใช้งานทรัพย์สินให้ชัดเจน ทั้งในส่วนของทรัพย์สินขององค์กร / ทรัพย์สินส่วนตัวที่นำมาใช้งาน
2.3 ทำการติดตั้งซอฟต์แวร์ป้องกันมัลแวร์ และอบรมพนักงานให้มีความตระหนักในด้านของภัยคุกคามและการรับมืออยู่เสมอ
2.4 มีกำหนดการควบคุมการเข้าถึงทรัพย์สินหรือพื้นที่ต่างๆ
- มีกระบวนการให้/ยกเลิกสิทธิในการเข้าถึง (ทั้งแบบธรรมดาและพิเศษ)
- มีการตรวจสอบว่าสิทธิต่างๆที่ให้นั้นเหมาะสมกับผู้ใช้งานหรือไม่
- มีการยืนยันตัวตนก่อนเข้าถึงทรัพย์สิน (เช่นลายนิ้วมือ/บัตรพนักงาน) โดยจะต้องดูแลข้อมูลที่ใช้ในการยืนยันตัวตนตั้งแต่ขั้นตอนการสร้างไปจนถึงการทำลาย

2.ทรัพย์สิน

2.5 หลังจากพนักงานลาออก/เปลี่ยนแปลงการจ้างงาน มีการส่งคืนทรัพย์สินที่ใช้งานอยู่ในขณะนั้น

2.6 จัดทำนโยบายการใช้งานสื่อบันทึกข้อมูลต่างๆที่เคลื่อนที่ได้

2.7 จัดเตรียมอุปกรณ์และระบบสนับสนุนในด้านต่างๆ (ไฟฟ้า, อินเทอร์เน็ต, ระบบฉุกเฉินต่างๆ)

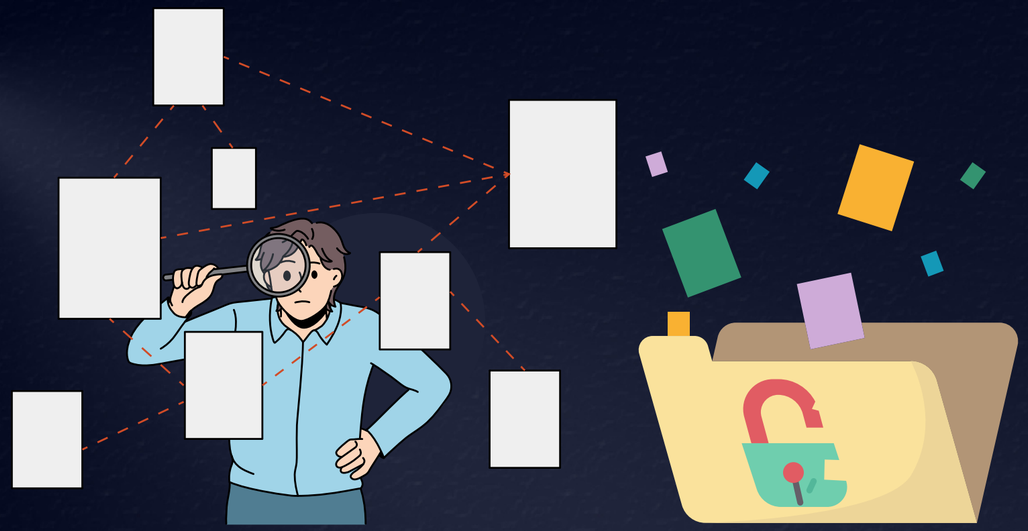
2.8 จัดระเบียบการเดินสายไฟและสายเคเบิลอื่นๆ

2.9 กำหนดนโยบายการดูแลรักษาทรัพย์สินขององค์กร

3.พื้นที่

- 3.1 กำหนดนโยบายในการรักษาความปลอดภัยสำหรับสถานที่ทำงาน (ทั่วไป, เฉพาะคนภายในองค์กร, พื้นที่หวงห้าม)
- 3.2 จัดเตรียมอุปกรณ์สำหรับป้องกันภัยอันตรายที่เกิดจากธรรมชาติและการบุกรุกเข้าพื้นที่ขององค์กร
- 3.3 จัดทำนโยบาย Clear desk / Clear Screen

4.ข้อมูล



4.1 กำหนดประเภทของข้อมูลต่างๆให้ชัดเจน รวมไปถึงการชี้บ่ง, การส่งข้อมูล, การจัดเก็บ, การกำจัดข้อมูลในแต่ละประเภท

4.2 มีกำหนดการควบคุมการเข้าถึงข้อมูลและระบบต่างๆ
- มีกระบวนการให้/ยกเลิกสิทธิในการเข้าถึง (ทั้งแบบธรรมดาและพิเศษ)
- มีการตรวจสอบว่าสิทธิต่างๆที่ให้นั้นเหมาะสมกับผู้ใช้งานหรือไม่
- มีการยืนยันตัวตนก่อนเข้าถึงทรัพย์สิน (เช่น รหัสผ่าน) โดยจะต้องดูแลข้อมูลที่ใช้ในการยืนยันตัวตนตั้งแต่ขั้นตอนการสร้างไปจนถึงการทำลาย

4.3 มีการประยุกต์ใช้การปิดบังและการเข้ารหัสข้อมูล รวมถึงดูแลคีย์ที่ใช้ในการถอดรหัส

4.4 จัดทำนโยบายสำหรับการสำรองข้อมูล และทำการทดสอบกู้คืนข้อมูล

5.ระบบเครือข่าย

5.1 จัดเตรียมอุปกรณ์ป้องกันเครือข่าย (เช่น Firewall) ตามความเหมาะสมกับลักษณะของเครือข่ายขององค์กร

5.3 กำหนด/บล๊อกเว็บไซต์ที่ผู้ใช้สามารถใช้ได้ เพื่อป้องกันมัลแวร์ที่จะมากับเว็บไซต์ต่างๆ

5.2 แยกกลุ่มผู้ใช้ในเครือข่ายตามฝ่าย เพื่อป้องกันความเป็นไปได้ที่จะเข้าถึงเครือข่ายของฝ่ายอื่นๆ ที่นำไปสู่การเข้าถึงระบบและข้อมูลของฝ่ายนั้นๆโดยไม่ได้รับอนุญาต

5.4 กำหนดนโยบายการบริหารระบบเครือข่ายขององค์กรอย่างปลอดภัย เช่น
- ไม่อนุญาติให้บุคคลที่สาม/ภายนอกเชื่อมต่อกับเครือข่ายขององค์กร
- เครือข่ายของแต่ละฝ่ายจะถูกควบคุมโดย Active Directory โดยจะสามารถเข้าถึงได้โดยการยืนยันตัวตนด้วยชื่อผู้ใช้งานและรหัสผ่านเท่านั้น

6. การจัดหาซอฟต์แวร์ (โปรแกรม)

6.1 กำหนดข้อกำหนดด้านความปลอดขั้นพื้นฐานสำหรับซอฟต์แวร์ที่ทางองค์กรทำการพัฒนาหรือจัดหามาใช้ในองค์กร

6.2 จัดทำนโยบายการพัฒนาซอฟต์แวร์อย่างปลอดภัย ตั้งแต่การออกแบบ, การพัฒนา, การทดสอบ ไปจนถึงการติดตั้งและใช้งานจริง

6.3 ควบคุมการพัฒนาซอฟต์แวร์ที่ดำเนินการโดยผู้ให้บริการบุคคลที่สาม/ภายนอกด้วย

7. ทั่วๆไป

7.1 จัดเตรียมนโยบายด้านความปลอดภัยของข้อมูลที่ได้รับการอนุมัติโดยผู้บริหาร และทำการสื่อสารไปยังผู้ที่เกี่ยวข้อง และทำการทบทวนอยู่เสมอ

7.2 จัดเตรียมเอกสารกระบวนการทำงานสำหรับอุปกรณ์/ระบบที่เกี่ยวข้องกับความปลอดภัยของข้อมูลตามความเหมาะสม

7.3 มีการจัดเตรียมคู่มือสำหรับการตั้งค่าทรัพย์สิน/ระบบที่ใช้งาน

7. ทั่วๆไป

7.5 กำหนดนโยบายการใช้งาน Cloud ของทางองค์กร (ตั้งแต่คัดเลือก ไปจนถึงยกเลิกการใช้งาน ทั้งขององค์กรและส่วนตัว)

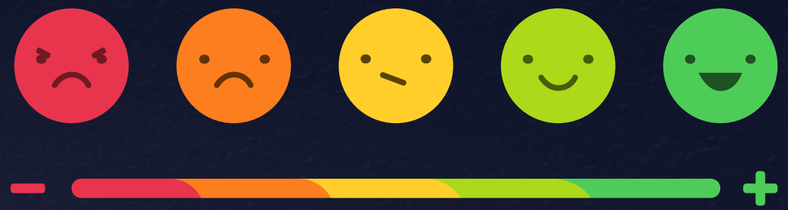
7.6 ควบคุมการติดตั้ง/ลบซอฟต์แวร์ที่ใช้งาน โดยเฉพาะซอฟต์แวร์ที่สามารถแทรกแซงการทำงานของอุปกรณ์/ซอฟต์แวร์อื่นๆได้

7.7 ทุกกิจกรรมที่เกิดขึ้นในองค์กรจะต้องคำนึงถึงผลกระทบต่อระบบบริหารขององค์กรด้วย

8. ผู้ให้บริการภายนอก

8.1 กำหนดความรับผิดชอบในด้านการรักษาความปลอดภัยของข้อมูลกับทางผู้ให้บริการภายนอก (เช่นผ่านทางสัญญาการจ้างงาน/ สัญญารักษาความลับ) รวมถึงบุคคลที่จ้างช่วงต่อด้วย และต้องยอมรับข้อกำหนดก่อนเริ่มงาน

8.2 ทำการประเมินสมรรถนะของผู้ให้บริการบุคคลที่สาม/ภายนอกอย่างสม่ำเสมอ



9. กฎหมาย

9.1 ระบุกฎหมายและข้อกำหนดที่องค์กรต้องปฏิบัติตามและทวนสอบว่าได้ปฏิบัติตามครบถ้วนหรือไม่ รวมไปถึงจัดเก็บบันทึกและเอกสารต่างๆตามที่กฎหมายหรือข้อกำหนดร้องขอด้วย

9.2 ดูแลการใช้งานทรัพย์สินทางปัญญาในองค์กร

10. ตรวจสอบ/เฝ้าระวัง

- 10.1 กำหนดหน้าที่ด้านการรักษาความปลอดภัยของข้อมูลในฝ่าย และคอยตรวจสอบกันเองอยู่เสมอ (นำโดยผู้จัดการฝ่ายทำการตรวจสอบการทำงานของคนในฝ่ายตามลำดับ ทั้งในส่วนของหน้าที่ที่ได้รับมอบหมาย และนโยบายต่างๆ)

- 10.2 ต้องไม่มีตำแหน่งที่ทำงานโดยไม่มีการตรวจสอบโดยบุคคลอื่น

- 10.3 ตรวจสอบระบบบริหารที่จัดทำขึ้นตามระยะเวลาที่กำหนดไว้หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น

10. ตรวจสอบ/เฝ้าระวัง

- 10.4 ทำการเฝ้าระวังความเพียงพอของทรัพยากรอยู่เสมอ และทำการสำรวจความต้องการของทรัพยากร

- 10.5 ตรวจสอบว่าเอกสาร/ข้อมูลต่างๆถูกลบ/ทำลายอย่างเหมาะสม

10. ตรวจสอบ/เฝ้าระวัง

- 10.6 ตรวจสอบช่องโหว่/จุดอ่อนของทรัพย์สิน/กระบวนการทำงาน และหาทางรับมือกับสิ่งเหล่านั้นอยู่เสมอ

- 10.7 จัดเตรียมช่องทางในการอัพเดทข้อมูลเกี่ยวกับภัยคุกคาม/ช่องโหว่ทางไซเบอร์ และจัดทำฐานข้อมูลและทำการวิเคราะห์ข้อมูลว่ามีผลกระทบต่อระบบบริหาร

- 10.8 มีการจัดเก็บ Log การใช้งานของผู้ใช้งานทั่วไปและผู้ดูแลระบบ และทำการตรวจสอบว่าอุปกรณ์ต่างๆที่ใช้งานมีระบบวันที่และเวลาถูกต้อง

- 10.9 มีการตรวจสอบการส่งข้อมูลไปยังภายนอกองค์กร และระบบแจ้งเตือนเมื่อเกิดเหตุการณ์ที่ผิดปกติ

11. เหตุการณ์ผิดปกติ

11.1 จัดทำมาตรการและขั้นตอนในการรับมือกับเหตุการณ์ที่ผิดปกติ (ตั้งแต่การจัดการเบื้องต้น ไปจนถึงการนำสิ่งที่เรียนรู้จากเหตุการณ์นั้นๆนำไปปรับปรุงระบบ)

11.2 แจ้งแนวทางการปฏิบัติตัว/รับมือกรณีที่พนักงานพบเจอเหตุการณ์ผิดปกติที่อาจจะส่งผลกระทบต่อด้านความปลอดภัยของข้อมูล

11.3 จัดเก็บหลักฐานในการจัดการกับเหตุการณ์ที่ผิดปกติที่เกิดขึ้นด้วย

12.แผนความต่อเนื่องทางธุรกิจและการรักษาความปลอดภัยของข้อมูลในระหว่างสถานการณ์ไม่ปกติ

12.1 กำหนดทรัพย์สินที่จำเป็นสำหรับการดำเนินงานขั้นพื้นฐานที่ยอมรับได้ขององค์กร (สามารถส่งมอบสินค้าหรือบริการตามที่คาดหวัง รวมถึงสามารถรักษาความปลอดภัยของข้อมูลในระดับที่ยอมรับได้ในระหว่างสถานการณ์ไม่ปกติ) และทำการจัดเตรียมไว้ให้เพียงพอด้วย

12.2 จัดทำแผนความต่อเนื่องทางธุรกิจและการรักษาความปลอดภัยของข้อมูลในระหว่างสถานการณ์ไม่ปกติในระหว่างสถานการณ์ไม่ปกติ และทำการทดสอบแผนเหล่านั้นด้วย