การรักษาความปลอดภัยของเทคโนโลยีสารสนเทศ

ความมั่นคงปลอดภัยของข้อมูลสารสนเทศ = ข้อมูล + สินทรัพย์ที่เกี่ยวข้อง

นิยามศัพท์ :

“การรักษาความมั่นคงปลอดภัยไซเบอร์” คือ มาตรการที่กำหนดขึ้น เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

“ภัยคุกคามทางไซเบอร์” คือ การกระทำโดยมิชอบ โดยใช้คอมพิวเตอร์/ ระบบคอมพิวเตอร์/ โปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดภัยประทุษร้าย ต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ และข้อมูลอื่นๆที่เกี่ยวข้อง

“ไซเบอร์” คือ ข้อมูลและการสื่อสารที่เกิดจากการใช้บริการ หรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเตอร์เน็ต หรือโครงข่ายโทรคมนาคม

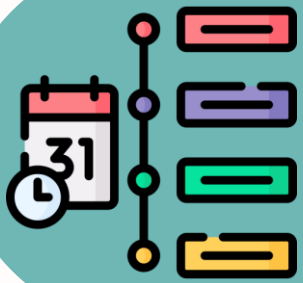
C
I
A

พื้นฐานปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์

1. **Confidentiality** การรักษาความลับของข้อมูล คือ การระบุสิทธิในการเข้าถึงข้อมูล
2. **Integrity** การรักษาความถูกต้องของข้อมูล คือ การระบุสิทธิของการแก้ไขข้อมูล
3. **Availability** ความพร้อมใช้งานของข้อมูล คือ ข้อมูลพร้อมให้เข้าถึงตลอดเวลา

แนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2564

1. แผนการตรวจสอบ โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน ผู้ตรวจสอบอิสระภายนอก
2. การประเมินความเสี่ยง
3. แผนการรับมือภัยคุกคามทางไซเบอร์



แผนการตรวจสอบ อย่างน้อยปี 1 ครั้ง โดยมีขอบเขต

1. กระบวนการจัดทำ และผลการวิเคราะห์ทางธุรกิจ
2. บริการที่สำคัญที่หน่วยงานเป็นเจ้าของและใช้บริการ
3. การปฏิบัติตาม พ.ร.บ แนวปฏิบัติ มาตรฐาน

การรักษาความมั่นคงปลอดภัยไซเบอร์

1. การปฏิบัติตามข้อกำหนด เพื่อยืนยันความเพียงพอ และประสิทธิผลของการควบคุม
2. ติดตามความเสี่ยง และภัยคุกคามที่ได้ระบุ และความเหมาะสมของการควบคุม เพื่อลดความเสี่ยงและภัยคุกคาม

หลักในการตรวจสอบเนื้อหาข้อมูล/ เอกสาร

1. ความสมบูรณ์ => มีข้อมูลเอกสารหลักฐานเป็นลายลักษณ์อักษร
2. ความถูกต้อง => สอดคล้องกับแหล่งข้อมูลที่มีความน่าเชื่อถือ
3. เป็นปัจจุบัน => ต้องเป็นปัจจุบันทันสมัย
4. ความสอดคล้อง, สม่ำเสมอ => มีความสอดคล้องเชื่อมโยงในตัวเอง และเอกสารอื่นๆที่เกี่ยวข้อง

ตรวจสอบตามข้อกำหนด

1. พ.ร.บ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มี 12 ตัวควบคุม

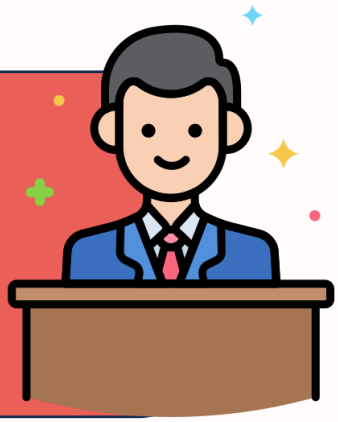
2. นโยบายบริหารจัดการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำหรับทางสารสนเทศ ประกอบนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) มี 16 ตัวควบคุม

3. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มี 72 ตัวควบคุม

ตัวอย่าง การตรวจประเมินด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1. บทบาทผู้บริหาร ด้านนโยบายบริหารจัดการของไซเบอร์ และมาตรฐานการควบคุมตาม พ.ร.บ ไซเบอร์ พ.ศ. 2562

- นโยบาย/ โครงสร้าง CSMS และการกำหนดบทบาทหน้าที่
- ทิศทางการบริหารจัดการ วิสัยทัศน์ พันธกิจ กลยุทธ์ และวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์
- ปัจจัยภายใน/ ภายนอก เกี่ยวข้องกับวัตถุประสงค์องค์กร
- การสนับสนุนทรัพยากรที่จำเป็น และการปรับปรุงต่อเนื่อง

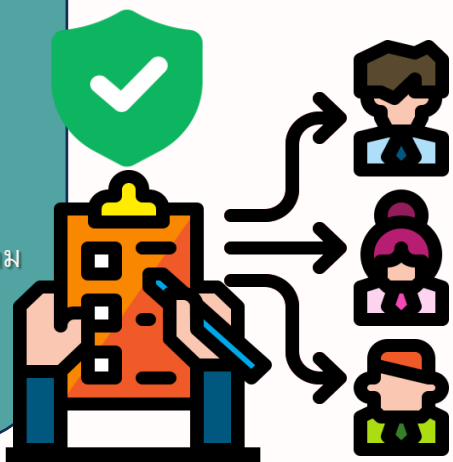


2. การควบคุมเอกสาร

- กระบวนการควบคุม
- การประกาศใช้เอกสาร
- การสื่อสารถึงหน่วยงานที่เกี่ยวข้อง

3. มาตรฐานควบคุมตาม พ.ร.บ ไซเบอร์ พ.ศ. 2562

- วิธีการจัดการทรัพย์สิน
- หลักฐานทะเบียนทรัพย์สิน
- วิธีประเมินความเสี่ยงไซเบอร์ของบริการที่สำคัญ
- วิธีการประเมินช่องโหว่ของการบริการที่สำคัญ
- วิธีการทดสอบระบบ รวมถึงผลการทดสอบใบรับรองจากผู้ให้บริการทดสอบ
- ข้อตกลงระดับการให้บริการ เงื่อนไขของสัญญาจ้าง
- การประเมินความเสี่ยงเกี่ยวกับงานบริการ
- สิทธิการเข้าถึงของบุคคลและอุปกรณ์
- มาตรฐานกำหนดค่าขั้นต่ำด้านไซเบอร์
- มาตรฐานการเชื่อมต่อระยะไกล
- ขั้นตอนเพื่อแบ่งปันข้อมูล
- กลไกกระบวนการตรวจจับเหตุการณ์ทางไซเบอร์
- แผนการรับมือภัยคุกคาม
- แผนการสื่อสารในภาวะวิกฤต
- หลักฐานการมีส่วนร่วมในการฝึกซ้อมรับมือภัยคุกคาม
- แผนความต่อเนื่องทางธุรกิจ
- หลักฐานการสอบทานแผนของผู้ให้บริการภายนอก
- หลักฐานการฝึกซ้อม BCP



แผนรับมือเหตุภัยคุกคามทางไซเบอร์

- ป้องกัน (เตรียมการ)
- ตรวจจับและวิเคราะห์
- ระงับ ปราบปราม และฟื้นฟู (กำจัดและกู้คืน)
- กิจกรรมภายหลังการแก้ปัญหา (ทบทวน)

1. การดำเนินมาตรการ เพื่อเตรียมการป้องกันการเกิดภัยคุกคามทางไซเบอร์

2. ขั้นตอนตรวจจับ และวิเคราะห์ภัยคุกคามทางไซเบอร์

3. ขั้นตอนการระงับภัยคุกคามทางไซเบอร์

4. ขั้นตอนการดำเนินการภายหลังการแก้ปัญหา

กรอบระเบียบที่เกี่ยวข้อง

1. พ.ร.บ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
2. ประกาศคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
   - เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) พ.ศ. 2564
   - เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)
   - เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ
   - เรื่อง หน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานควบคุมหรือกำกับดูแล
   - มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ระบบคลาวด์ พ.ศ. 2567