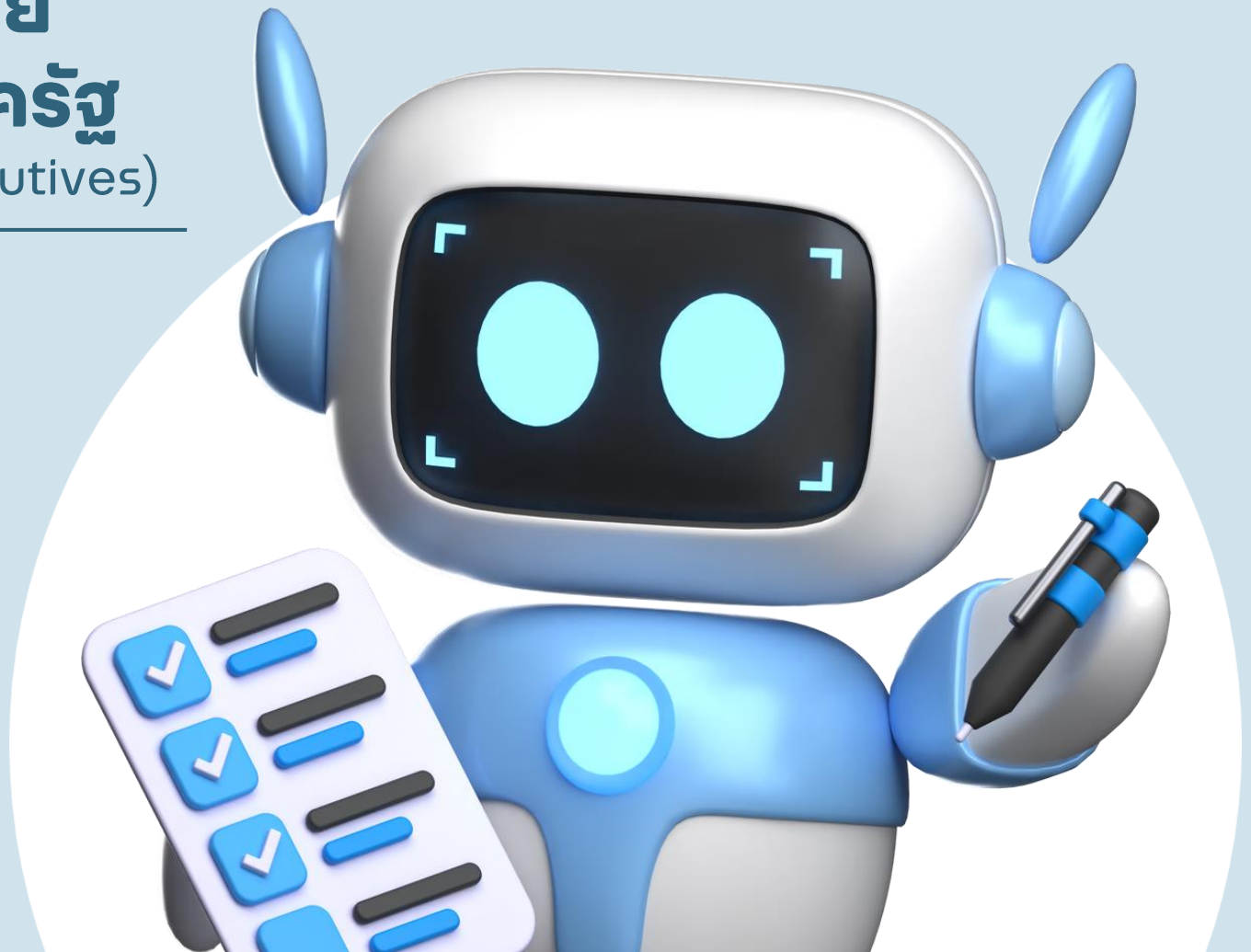
หลักสูตรความมั่นคงปลอดภัย ทางดิจิทัลสำหรับผู้บริหารภาครัฐ

(Digital Security for Government Executives)

วันที่ 14 – 15 สิงหาคม 2568



วัตถุประสงค์การฝึกอบรม

1.1 ให้ความรู้พื้นฐานเกี่ยวกับหลักการรักษาความมั่นคงปลอดภัยไซเบอร์
1.2 สามารถออกแบบและจัดทำนโยบาย/ยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์
1.3 เข้าใจกฎหมายและมาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล

ผู้เข้าร่วม

ข้าราชการและบุคลากรภาครัฐ**ระดับผู้บริหาร 36 คน**

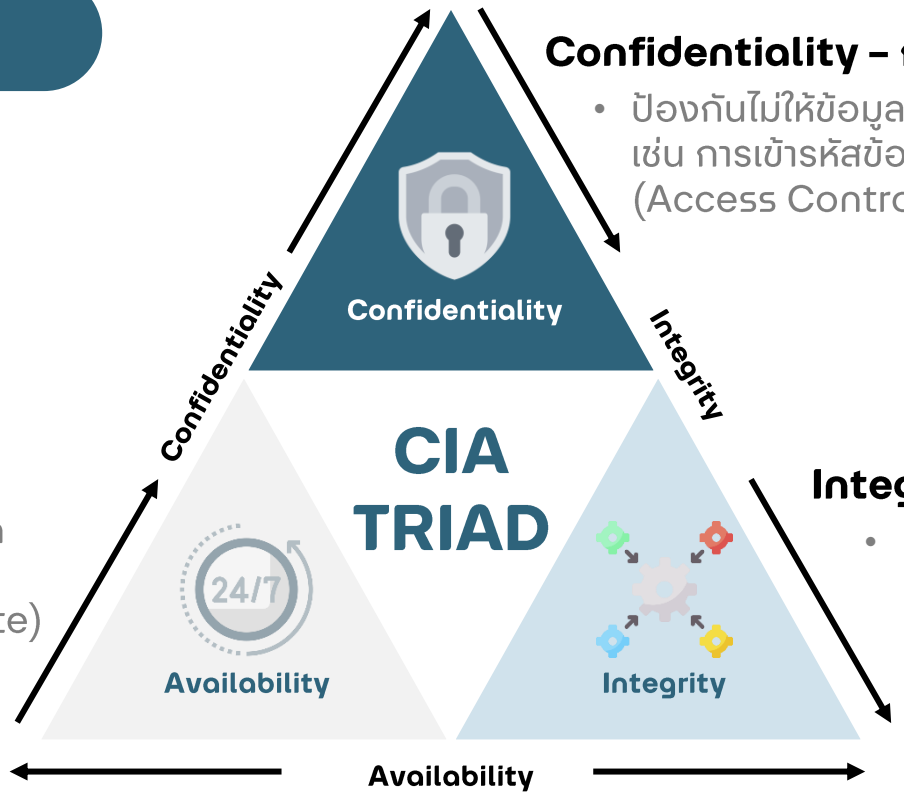
หัวข้อการบรรยาย

- ความรู้พื้นฐานด้านความมั่นคงปลอดภัยดิจิทัล
- ความเสี่ยงและภัยคุกคาม (Risk & Threat Landscape)
- เทคโนโลยีและกลไกความปลอดภัย (Digital Security Technologies & Mechanisms)
- มาตรฐานและกรอบการดำเนินงาน (Standards & Frameworks)
- กฎหมายและข้อบังคับที่เกี่ยวข้อง (Cyber Security Laws)
- การพัฒนานโยบายและยุทธศาสตร์ (Policy & Strategy Development)

ความรู้พื้นฐานด้านความมั่นคงปลอดภัยดิจิทัล

ความมั่นคงปลอดภัยทางดิจิทัลคือการปกป้องข้อมูล สารสนเทศ และระบบจากการเข้าถึง การแก้ไข หรือการทำลายโดยไม่ได้รับอนุญาต

ความเชื่อมโยงของ CIA Model



Confidentiality – การรักษาความลับ

- ป้องกันไม่ให้ข้อมูลรั่วไหลไปถึงผู้ที่ไม่มีสิทธิ์ เช่น การเข้ารหัสข้อมูล การกำหนดสิทธิ์เข้าถึง (Access Control)

Availability – ความพร้อมใช้งาน

- ให้ข้อมูลและระบบพร้อมใช้งานได้ตลอดตามที่ต้องการ เช่น ระบบสำรอง (Backup) ศูนย์สำรองข้อมูล (DR Site) ระบบป้องกัน DDoS

Integrity – ความถูกต้องครบถ้วน

- ทำให้ข้อมูลถูกต้อง ไม่ถูกแก้ไขโดยไม่ได้รับอนุญาต เช่น Digital Signature, Hash Function, การตรวจสอบความถูกต้องของข้อมูล (Data Validation)

ความเสี่ยงและภัยคุกคาม (Risk & Threat Landscape)

แบ่งตามแหล่งที่มา >> ภัยคุกคามภายใน และ ภัยคุกคามภายนอก

ผู้ก่อภัยคุกคาม (Threat Actors)

หมวกดำ (Black Hat)
- มุ่งร้าย
- โจมตีเพื่อผลประโยชน์ส่วนตัว

หมวกเทา (Gray Hat)
- โจมตีแบบไม่มุ่งร้าย แต่ไม่ได้ขออนุญาต

หมวกขาว (White Hat)
- ผู้เชี่ยวชาญด้านความปลอดภัยที่ช่วยป้องกันการโจมตี

แรงจูงใจและช่องทาง (Motives & Attack Vectors)

แรงจูงใจ (Motives)

ระบุเหตุผลในการโจมตี เช่น
- **การเมือง/ปรัชญา :** โจมตีเพื่อแสดงจุดยืน
- **จริยธรรม :** โจมตีเพื่อแก้ไขสิ่งที่เห็นว่าไม่ถูกต้อง
- **แก้แค้น/หยุดชะงัก:** โจมตีเพื่อสร้างความเสียหายหรือหยุดระบบ

ช่องทาง (Attack)

แสดงให้เห็นว่าการโจมตีมาจากไหน
- **อีเมล / SMS / Messaging :** การโจมตีแบบPhishing
- **เครือข่าย :** Wired / Wireless Network
- **อุปกรณ์ :** Removable Devices หรือ Cloud

ผลกระทบที่เชื่อมโยง (Impact Chain Reaction)

ผลกระทบ (Impact)
- การสูญเสียข้อมูล ความเสียหายต่อชื่อเสียง ความเสียหายทางเศรษฐกิจ ซึ่งไม่ได้เกิดแยกกันแบบลอย ๆ แต่มีความเชื่อมโยงกันเป็น **“ลูกโซ่”**

ความเสี่ยงและภัยคุกคาม (Risk & Threat Landscape)

ผลกระทบที่เชื่อมโยง (Impact Chain Reaction)

ผลกระทบที่เชื่อมโยง (Impact Chain Reaction)

การสูญเสียข้อมูล (Loss of Critical Data)

สาเหตุ : การโจรกรรม การรั่วไหลการทำลายข้อมูล

ผลกระทบโดยตรง : ไม่สามารถใช้ข้อมูลในการตัดสินใจหรือให้บริการ

“จุดเริ่มต้น ของความเสียหายทั้งหมด เป็นเหตุการณ์แรกที่เกิดขึ้นและส่งผลกระทบต่อเนื่อง”

ความเสียหายต่อชื่อเสียง (Reputational Damage)

สาเหตุ : เป็นผลสืบเนื่อง จากที่ข้อมูลสูญหายหรือรั่วไหล ทำให้ผู้มีส่วนได้ส่วนเสีย (ประชาชน, คู่ค้า) สูญเสียความเชื่อมั่น

ผลกระทบโดยตรง : ความไว้วางใจลดลง, ยากต่อการทำงานร่วมในอนาคต

"ตัวกลาง ที่เชื่อมระหว่างการสูญเสียข้อมูลกับความเสียหายทางเศรษฐกิจ ชื่อเสียงที่เสียไปจะทำให้ลูกค้าหรือคู่ค้าหันหนี”

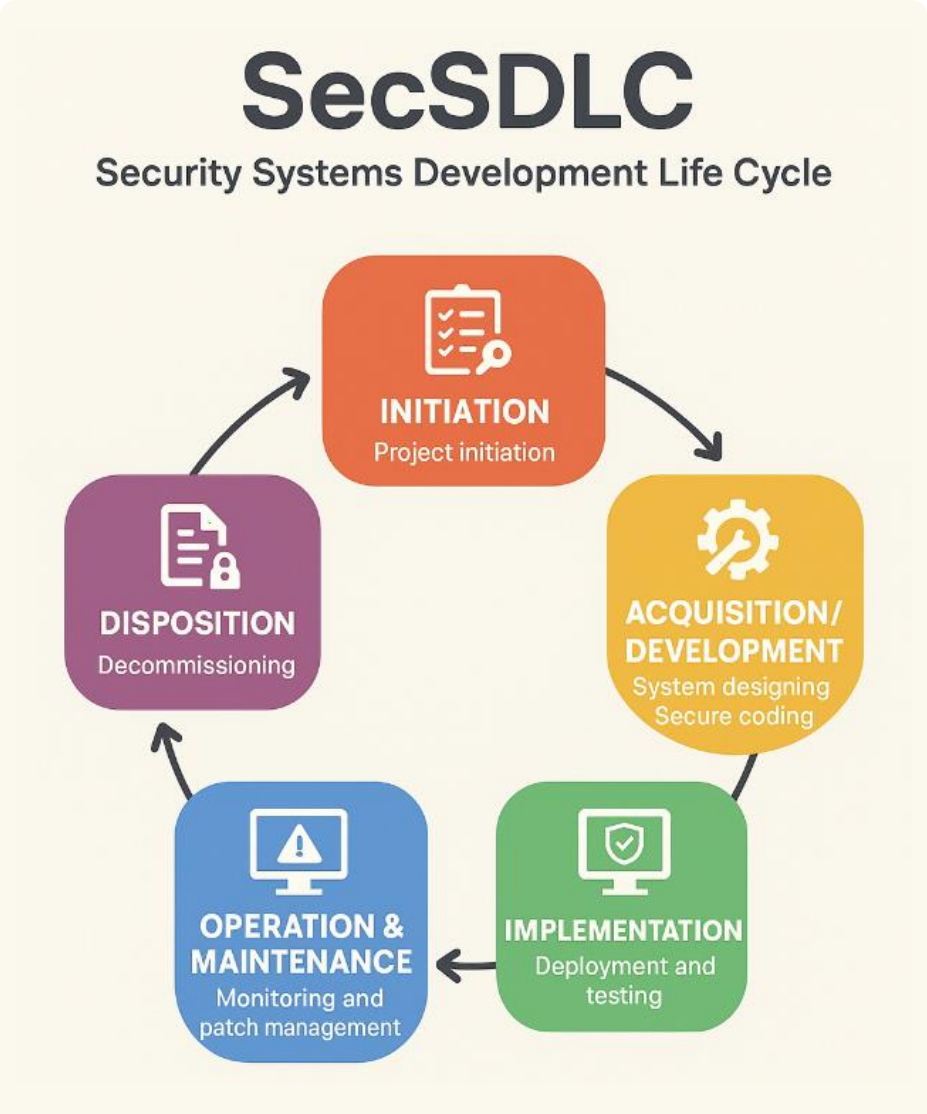
ความเสียหายทางเศรษฐกิจ (Economic Loss)

สาเหตุ : เป็นได้ทั้งผลโดยตรง จากการหยุดชะงักของระบบ หรือเป็น ผลสืบเนื่องจากชื่อเสียงที่เสียหาย

ผลกระทบโดยตรง : ภาระค่าใช้จ่ายเพิ่มขึ้น ประสิทธิภาพการดำเนินงานลดลง (ค่าปรับ , ค่าชดเชย, รายได้ที่เสียไป)

"ปลายทาง ของความเสียหายทั้งหมด เป็นจุดที่ความเสี่ยงแปรเปลี่ยนเป็นความสูญเสียทางการเงินที่จับต้องได้”

เทคโนโลยีและกลไกความปลอดภัย
(Digital Security Technologies & Mechanisms)



กระบวนการที่เป็นหัวใจสำคัญ (Core Process)

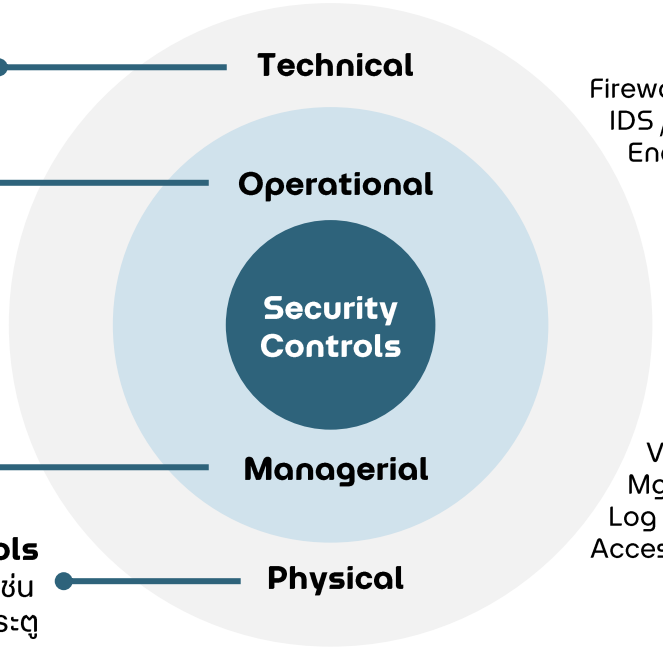
Secure Software Development Life Cycle (SecSDLC): นี่คือกระบวนการพื้นฐานที่สำคัญที่สุด เป็นการผนวกเอาขั้นตอนด้านความปลอดภัยเข้าไปในทุกๆ เฟสของการพัฒนาระบบ ตั้งแต่เริ่มต้นไปจนถึงการบำรุงรักษา

- **เป้าหมาย:** เพื่อให้มั่นใจว่าระบบที่พัฒนาขึ้นนั้นมีทั้ง **คุณภาพ** (Quality) และ **ความปลอดภัย** (Security) ตามมาตรฐานและข้อกำหนดทางกฎหมาย
- **ทีมงานด้านความมั่นคงปลอดภัย:** บุคลากรเหล่านี้คือผู้ขับเคลื่อนกระบวนการทั้งหมด เช่น **CISO** (ผู้บริหารสูงสุดด้านความปลอดภัย), **SOC Analyst** (นักวิเคราะห์ศูนย์ปฏิบัติการด้านความปลอดภัย), และ **Incident Responder** (ผู้ตอบสนองเหตุการณ์)

เทคโนโลยีและกลไกความปลอดภัย
(Digital Security Technologies & Mechanisms)

“ระบบป้องกันหลายชั้น” (Defense-in-Depth) คือแนวคิดหลักในการสร้างความปลอดภัยที่ข้อมูลเน้นย้ำ ซึ่งเปรียบเสมือนการสร้างปราสาทที่มีหลายด่านป้องกัน โดยมี 4 มาตรการควบคุม (Security Controls) ที่ทำงานเสริมกันเป็นระบบ

STRUCTURL VIEW



Technical Controls
ป้องกันการเข้าถึงหรือโจมตี
เช่น Firewall, การเข้ารหัส

Operational Controls
เพื่อให้มาตรการเทคนิคทำงานได้อย่างต่อเนื่อง
เช่น การตรวจสอบ log การ patch ช่องโหว่

Managerial Controls
เพื่อกำหนดทิศทางและความสำคัญ
เช่น นโยบายความปลอดภัย การประเมินความเสี่ยง

Physical Controls
เพื่อป้องกันไม่ให้ผู้ไม่เกี่ยวข้องเข้าถึงระบบหรืออุปกรณ์ได้ เช่น
กล้องวงจรปิด ระบบล็อกประตู

Firewall
IDS / IPS
Encryption

Vulnerability Mgmt
Log Review
Access Control

PROCESS VIEW

การวิเคราะห์ความเสี่ยง (Managerial)
กำหนดทิศทางและนโยบาย

การวางแผนปฏิบัติงาน (Operational)
สร้างขั้นตอนการทำงานให้เป็นไปตามนโยบายนั้น

การใช้เครื่องมือ (Technical)
นำเครื่องมือและเทคโนโลยีมาใช้เพื่อรองรับขั้นตอนที่วางไว้

การป้องกันการเข้าถึง (Physical)
เป็นการสนับสนุนให้ระบบทั้งหมดปลอดภัยจากการเข้าถึงทางกายภาพ

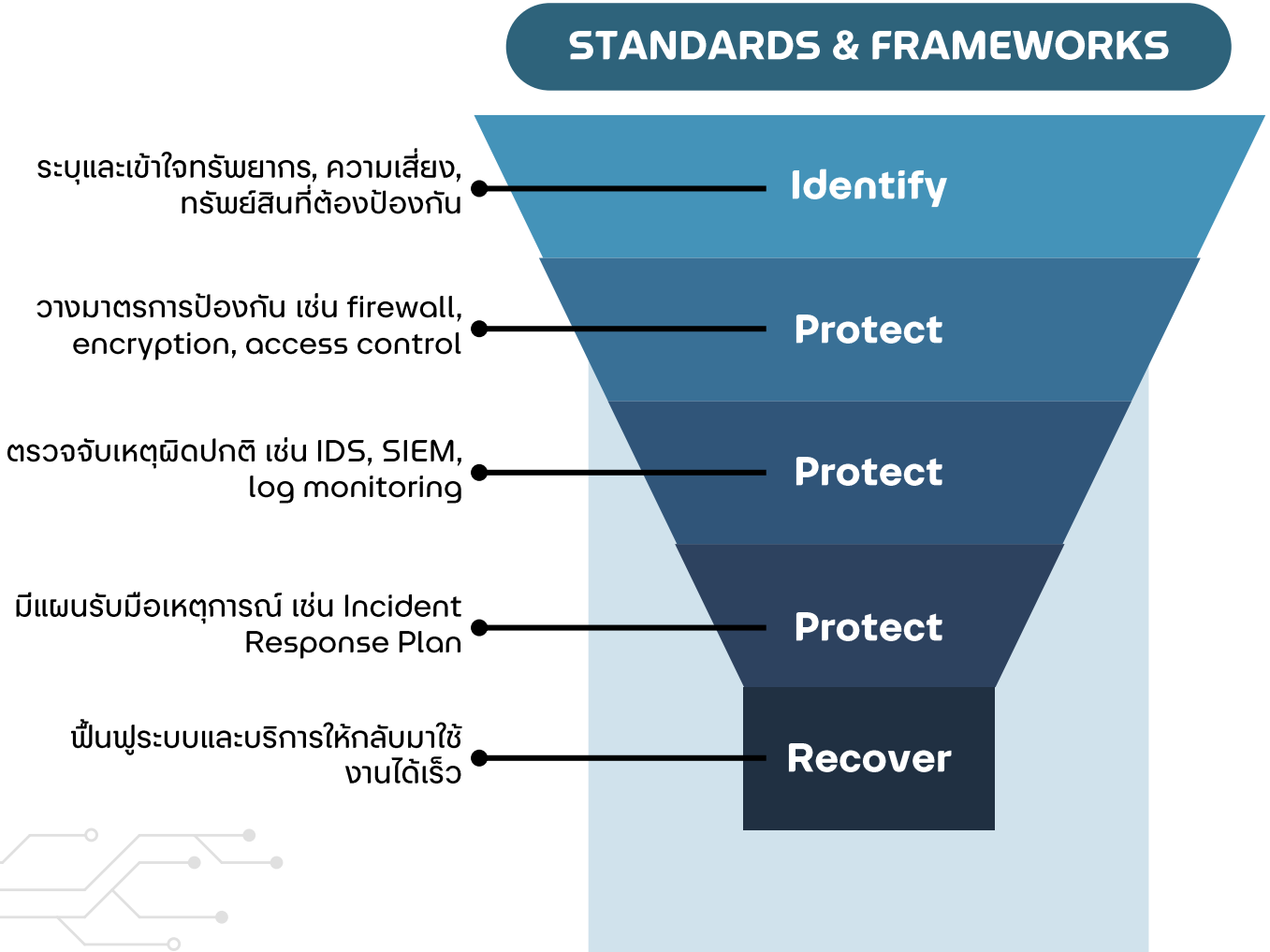
ตัวอย่างการทำงานร่วมกัน เช่น สถานการณ์ ปกป้องฐานข้อมูลประชาชนของหน่วยงาน

Managerial กำหนดนโยบายว่า “ข้อมูลต้องเข้าถึงได้เฉพาะเจ้าหน้าที่ที่ได้รับอนุญาต และต้องเข้ารหัสเสมอ” → Operational จัดขั้นตอนตรวจสอบสิทธิ์ผู้ใช้และบันทึกการเข้าถึงทุกครั้ง → Technical ตั้ง Firewall, ใช้ระบบเข้ารหัส AES, และมีระบบตรวจจับการบุกรุก → Physical จำกัดการเข้าถึงห้อง Server ด้วยการ์ด RFID และกล้องวงจรปิด

มาตรฐานและกรอบการดำเนินงาน (Standards & Frameworks)

NIST Cybersecurity Framework คือ เครื่องมือที่ช่วยให้องค์กรมีความพร้อมในการรับมือกับภัยคุกคามไซเบอร์โดยไม่ส่งผลกระทบต่อภารกิจหลักในระยะยาว

จุดเด่น คือ “แม้โดนก็ไม่ล้ม ฟื้นต่อไว เดินต่อได้”



ISO/IEC 27001 ระบบการจัดการความมั่นคงสารสนเทศ (ISMS)

- เป็นมาตรฐานสากลสำหรับ ระบบการจัดการความมั่นคงสารสนเทศ (ISMS : Information Security Management System) ครอบคลุมทั้ง นโยบาย กระบวนการ บุคลากร และเทคโนโลยี ถ้าหน่วยงานผ่านการรับรอง ISO/IEC 27001 แสดงว่ามีมาตรการด้านความมั่นคงปลอดภัยที่ได้มาตรฐานโลก

bsi ISO/IEC 27001 Information Security Management CERTIFIED

- Information security management
- Risk assessment
- Security controls
- Continuous improvement

กฎหมายและข้อบังคับที่เกี่ยวข้อง (Cyber Security Laws)

พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

เป้าหมายหลัก

1. กำหนดนโยบาย มาตรการ และแนวทางปฏิบัติด้านความมั่นคงไซเบอร์สำหรับหน่วยงานรัฐและโครงสร้างพื้นฐานสำคัญ
2. ป้องกัน ตรวจจับ และรับมือภัยคุกคามทางไซเบอร์อย่างทันท่วงที

ขอบเขตการบังคับใช้

- หน่วยงานรัฐ และองค์กรที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญ เช่น การเงิน พลังงาน โทรคมนาคม

บทลงโทษ / กลไกสำคัญ

- เน้นการกำกับดูแล (Regulatory & Policy) และให้อำนาจคณะกรรมการด้านไซเบอร์แห่งชาติ

พ.ร.บ. การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

เป้าหมายหลัก

1. ระบุพฤติกรรมที่ถือเป็นความผิดเกี่ยวกับคอมพิวเตอร์ (เจาะระบบ, ทำลายข้อมูล, เผยแพร่ข้อมูลผิดกฎหมาย)
2. เน้นความผิดที่กระทบต่อระบบสำคัญ/ชีวิตประชาชน
3. ปรับปรุงกระบวนการสืบสวน (เก็บ log, เอื้อต่อการสอบสวน)

ขอบเขตการบังคับใช้

- ทุกคนที่ใช้ระบบคอมพิวเตอร์ หรืออินเทอร์เน็ต และครอบคลุมถึงอาชญากรรมไซเบอร์ที่มีผลต่อประเทศ

บทลงโทษ / กลไกสำคัญ

- มีบทลงโทษทางอาญา เช่น จำคุก ปรับ สำหรับผู้กระทำความผิด และมาตรการด้าน log เพื่อติดตาม

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

เป้าหมายหลัก

1. กำหนดมาตรฐานการเก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคล โดยต้องได้รับความยินยอม
2. มอบสิทธิให้เจ้าของข้อมูล (แจ้ง, เข้าถึง, แก้ไข, ลบ, เพิกถอนความยินยอม)
3. บังคับให้แจ้งเหตุละเมิดข้อมูลภายใน 72 ชม. และกำหนดบทลงโทษรุนแรง

ขอบเขตการบังคับใช้

- หน่วยงานรัฐและเอกชนที่เก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคลของประชาชน

บทลงโทษ / กลไกสำคัญ

- มีบทลงโทษทั้งทางแพ่ง อาญา และปกครอง เช่น ปรับสูงสุดหลายล้านบาท, จำคุก, และการชดเชยความเสียหาย (ศาลสามารถสั่งเพิ่มได้สองเท่า)

การพัฒนานโยบายและยุทธศาสตร์ (Policy & Strategy Development)

แนวทางเชิงปฏิบัติ (implementation approach) สำหรับการพัฒนานโยบายและยุทธศาสตร์

การพัฒนานโยบาย (Policy Development)

1.1 ระบุวัตถุประสงค์และขอบเขต → Policy Statement
1.2 กำหนดมาตรการ 3 ด้าน → เทคโนโลยี / การบริหาร / บุคลากร
1.3 สื่อสารและอบรมบุคลากร

วิธีการ / เครื่องมือ

- รวบรวมข้อกำหนด กฎหมาย มาตรฐาน
- Manual, e-Learning, Workshop, Training

การพัฒนายุทธศาสตร์ (Strategy Development)

2.1 วิเคราะห์ความเสี่ยง และสภาพแวดล้อม → Risk Assessment, SWOT, PESTEL, Threat Modeling
2.2 กำหนดแผนงาน → ป้องกัน, ตรวจจับ, ตอบสนอง
2.3 วางแผนฟื้นฟูระบบ → Recovery Plan, BCP, Simulation

วิธีการ / เครื่องมือ

- Risk Assessment
- Security Monitoring
- Incident Response SOP
- Disaster Recovery / BCP
- Tabletop Exercise

การทบทวนและปรับปรุง (Review & Update)

ทบทวนปีละ 1 ครั้ง หรือเมื่อมีภัยคุกคามเทคโนโลยี/กฎหมายใหม่ → Lessons Learned & Record

วิธีการ / เครื่องมือ

- รอบการ Review Audit & Feedback
- Continuous Improvement

ข้อเสนอแนะเชิงนโยบายด้านความมั่นคงปลอดภัยทางดิจิทัล

เพื่อให้การดำเนินงานของกรมทรัพยากรธรณีสอดคล้องกับการเปลี่ยนผ่านสู่รัฐบาลดิจิทัล และสามารถรับมือภัยคุกคามทางไซเบอร์ที่ซับซ้อนมากขึ้น จึงมีข้อเสนอเชิงนโยบาย ดังนี้

1

- **กำหนดนโยบายความมั่นคงปลอดภัยไซเบอร์** โดยจัดทำนโยบายอย่างเป็นทางการสอดคล้องกับ พ.ร.บ. ความมั่นคงไซเบอร์ และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มุ่งเน้นการปกป้องฐานข้อมูลทรัพยากรธรณี ซึ่งเป็นข้อมูลสำคัญของชาติ

2

- **พัฒนายุทธศาสตร์และแผนปฏิบัติการ** โดยใช้มาตรฐานสากล เช่น NIST CSF และ ISO/IEC 27001 และจัดทำ Roadmap การบริหารความเสี่ยงทั้งระยะสั้นและระยะยาว

3

- **เสริมสร้างศักยภาพบุคลากรและวัฒนธรรมความปลอดภัย** โดยจัดการฝึกอบรมต่อเนื่องสำหรับผู้บริหารและเจ้าหน้าที่ และปลูกฝังวัฒนธรรมการรักษาความปลอดภัยสารสนเทศภายในองค์กร

4

- **จัดตั้งระบบบริหารจัดการเหตุการณ์ด้านไซเบอร์ (Incident Response)** จัดทีมงานเฉพาะด้านและคู่มือการปฏิบัติเมื่อเกิดเหตุ และทำการซ้อมแผนเป็นประจำ เพื่อให้พร้อมรับมือสถานการณ์จริงเป็นประจำ

5

- **ปรับปรุงระบบเทคโนโลยีสารสนเทศให้มั่นคงปลอดภัย** จัดหาเครื่องมือด้านความปลอดภัย เช่น Firewall, IDS/IPS, DLP และพัฒนาระบบสำรองและกู้คืนข้อมูล เพื่อรับประกันความต่อเนื่องในการปฏิบัติงาน

6

- **สร้างความร่วมมือกับหน่วยงานภายนอก** ประสานงานกับ DGA, ThaiCERT และหน่วยงานกำกับดูแลที่เกี่ยวข้อง แลกเปลี่ยนข้อมูลและแนวปฏิบัติที่เป็นมาตรฐาน

ประโยชน์ที่คาดว่าจะได้รับ

- **เสริมสร้างความมั่นคงปลอดภัยด้านข้อมูลทรัพยากรธรณี** ช่วยให้สามารถวางมาตรการป้องกันการรั่วไหล การแก้ไข หรือการโจรกรรมข้อมูล ซึ่งหากรั่วไหลอาจสร้างผลกระทบทางเศรษฐกิจและความมั่นคงของชาติ

1

- **เพิ่มขีดความสามารถในการบริหารความเสี่ยงไซเบอร์** สามารถประเมินและจัดลำดับความสำคัญของความเสี่ยงที่กระทบต่อระบบสารสนเทศของกรม ช่วยให้การจัดทำยุทธศาสตร์ความมั่นคงปลอดภัยด้านไซเบอร์ของกรมมีทิศทางที่ชัดเจน เตรียมความพร้อมต่อภัยคุกคามไซเบอร์ในอนาคต ลดโอกาสความเสียหายที่จะเกิดขึ้นทั้งด้านข้อมูล ชื่อเสียง และงบประมาณของหน่วยงาน

2

- **ลดความเสี่ยงทางกฎหมายและบทลงโทษที่อาจเกิดขึ้น** จากการละเมิดกฎหมายไซเบอร์ หรือการละเมิดข้อมูลส่วนบุคคล

3

- **สนับสนุนการทำงานเชิงบูรณาการกับหน่วยงานภาครัฐอื่น**ในฐานะหน่วยงานสนับสนุนเชิงข้อมูลที่ปลอดภัย น่าเชื่อถือ และพร้อมต่อการแลกเปลี่ยนข้อมูลระดับประเทศ

4

THANK YOU

ศูนย์เทคโนโลยีสารสนเทศ

กองอนุรักษ์และจัดการทรัพยากรธรณี