



# การดำเนินงานด้านการบริหาร ความมั่นคงปลอดภัยไซเบอร์



ผู้ช่วยปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม  
(นายกานตพันธุ์ พิศาลสุขสกุล)



# การดำเนินงานด้านการบริหารความมั่นคงปลอดภัยไซเบอร์

มาตรา 44 จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา 45 มีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน

มาตรา 46 แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการเพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยัง สกมช. รวมถึงแจ้งปรับปรุงข้อมูลกรณีมีการเปลี่ยนแปลง

มาตรา 58 » ต้องตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ รวมถึงพฤติการณ์แวดล้อมของหน่วยงาน ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศ

» มีการแจ้งไปยัง สกมช. และหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว

## พระราชบัญญัติ การรักษาความมั่นคง ปลอดภัยไซเบอร์ พ.ศ. 2562

» เมื่อเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น



# การดำเนินงานด้านการบริหารความมั่นคงปลอดภัยไซเบอร์

นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความ  
มั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ  
และหน่วยงานโครงสร้างพื้นฐานสำคัญทาง  
สารสนเทศ

01

การกำกับดูแลการรักษาความ  
มั่นคงปลอดภัยไซเบอร์  
(Good Governance  
in Cybersecurity)

แต่งตั้งผู้บริหารที่ทำหน้าที่บริหาร  
จัดการความมั่นคงปลอดภัย  
สารสนเทศ (Head of  
Information Security)

02

การบริหารความเสี่ยง  
(Risk Management)

จัดทำกรอบการบริหารความเสี่ยงด้าน  
ความมั่นคงปลอดภัยไซเบอร์  
เก็บรักษารายการความเสี่ยง ระบุไว้ใน  
ทะเบียนความเสี่ยง (Risk  
register) บริการที่สำคัญ  
มีการติดตามความเสี่ยง

03

นโยบาย และแนวปฏิบัติ  
(Policies and Guidelines)

มีการกำหนด และอนุมัตินโยบายใน  
การจัดการความเสี่ยงด้านไซเบอร์  
และการป้องกันบริการสำคัญ

ทบทวนอย่างน้อยปีละ 1 ครั้ง



# การดำเนินงานด้านการบริหารความมั่นคงปลอดภัยไซเบอร์ของ สป.ทส.

## ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

### 1. แผนการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์

- » มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบอิสระภายนอก ปีละ 1 ครั้ง
- » จัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) ของบริการสำคัญ

### 2. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

- » จัดทำระเบียบวิธีปฏิบัติในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- » ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง
- » การจัดการความเสี่ยง (Risk treatment) ควบคุม และป้องกันความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
- » ติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk monitoring and review)
- » การรายงานความเสี่ยง (Risk reporting) รายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงต่อผู้บริหารฯ และทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงอย่างน้อยปีละ 1 ครั้ง

## ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564

### 3. แผนการรับมือภัยคุกคามทางไซเบอร์

- » จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)
- » สื่อสารแผนการรับมือภัยให้ผู้เกี่ยวข้อง
- » ทบทวนแผนการรับมือภัย อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง



# การดำเนินงานด้านการบริหารความมั่นคงปลอดภัยไซเบอร์ของ สป.ทส.

## ประกาศคณะกรรมการกำกับดูแล ด้านความมั่นคงปลอดภัยไซเบอร์

เรื่อง ประมวลแนวทางปฏิบัติและกรอบ  
มาตรฐานด้านการรักษาความมั่นคงปลอดภัย  
ไซเบอร์ สำหรับหน่วยงานของรัฐและ  
หน่วยงานโครงสร้างพื้นฐานสำคัญทาง  
สารสนเทศ พ.ศ. 2564

### การควบคุมการเข้าถึง (Access Control)

- กำหนดให้มีการจำกัดการเข้าถึงบริการที่สำคัญเฉพาะบุคลากร  
กิจกรรม อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต

### การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

- จัดทำมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย  
(Security Baseline Configuration Standards) ของบริการที่  
สำคัญ

## กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

### การจัดการทรัพย์สิน (Asset Management)

- ทำทะเบียนทรัพย์สินของบริการที่สำคัญ และตรวจสอบทะเบียนทรัพย์สิน อย่างน้อย  
ปีละ 1 ครั้ง
- ประเมินความเสี่ยงด้านการรั่วไหลของบริการที่สำคัญ อย่างน้อยปีละ 1 ครั้ง

### การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

- ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง
- ปรับปรุงทะเบียนความเสี่ยง

### การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

- ประเมินช่องโหว่ของบริการที่สำคัญ
- ทดสอบเจาะระบบ (Penetration Testing) ของระบบบริการสำคัญ
- ดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ 1 (หนึ่ง)

### การจัดการผู้ให้บริการภายนอก (Third-Party Management)

- กำหนดให้ผู้ให้บริการภายนอกต้องรับผิดชอบต่อการดูแลรักษาความมั่นคงปลอดภัย  
ไซเบอร์ของบริการที่สำคัญที่เกี่ยวข้อง และมีข้อตกลงระดับการให้บริการ (Service  
Level Agreement)

### การเชื่อมต่อระยะไกล (Remote Connection) กับบริการสำคัญ

- กำหนดมาตรการการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญ



# การดำเนินงานด้านการบริหารความมั่นคงปลอดภัยไซเบอร์ของ สป.ทส.

## ประกาศคณะกรรมการกำกับดูแล ด้านความมั่นคงปลอดภัยไซเบอร์

เรื่อง ประมวลแนวทางปฏิบัติและกรอบ  
มาตรฐานด้านการรักษาความมั่นคงปลอดภัย  
ไซเบอร์ สำหรับหน่วยงานของรัฐและ  
หน่วยงานโครงสร้างพื้นฐานสำคัญทาง  
สารสนเทศ พ.ศ. 2564

### แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

- มีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 ครั้ง

### แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

- จัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ มีการฝึกซ้อมแผน อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง

## กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (ต่อ)

### สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media) กับบริการสำคัญ

- กำหนดให้มีการควบคุมในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา กับบริการที่สำคัญ
- กำหนดให้มีการเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญบนสื่อบันทึกข้อมูลแบบถอดได้

### การสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

- ทำแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) มีการทบทวนแผนงานอย่างน้อยปีละ 1 ครั้ง

### การแบ่งปันข้อมูล (Information Sharing)

- กำหนดขั้นตอนเพื่อแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์และการบรรเทาผลกระทบ โดยติดตั้งระบบ MISP ของ สกมช.

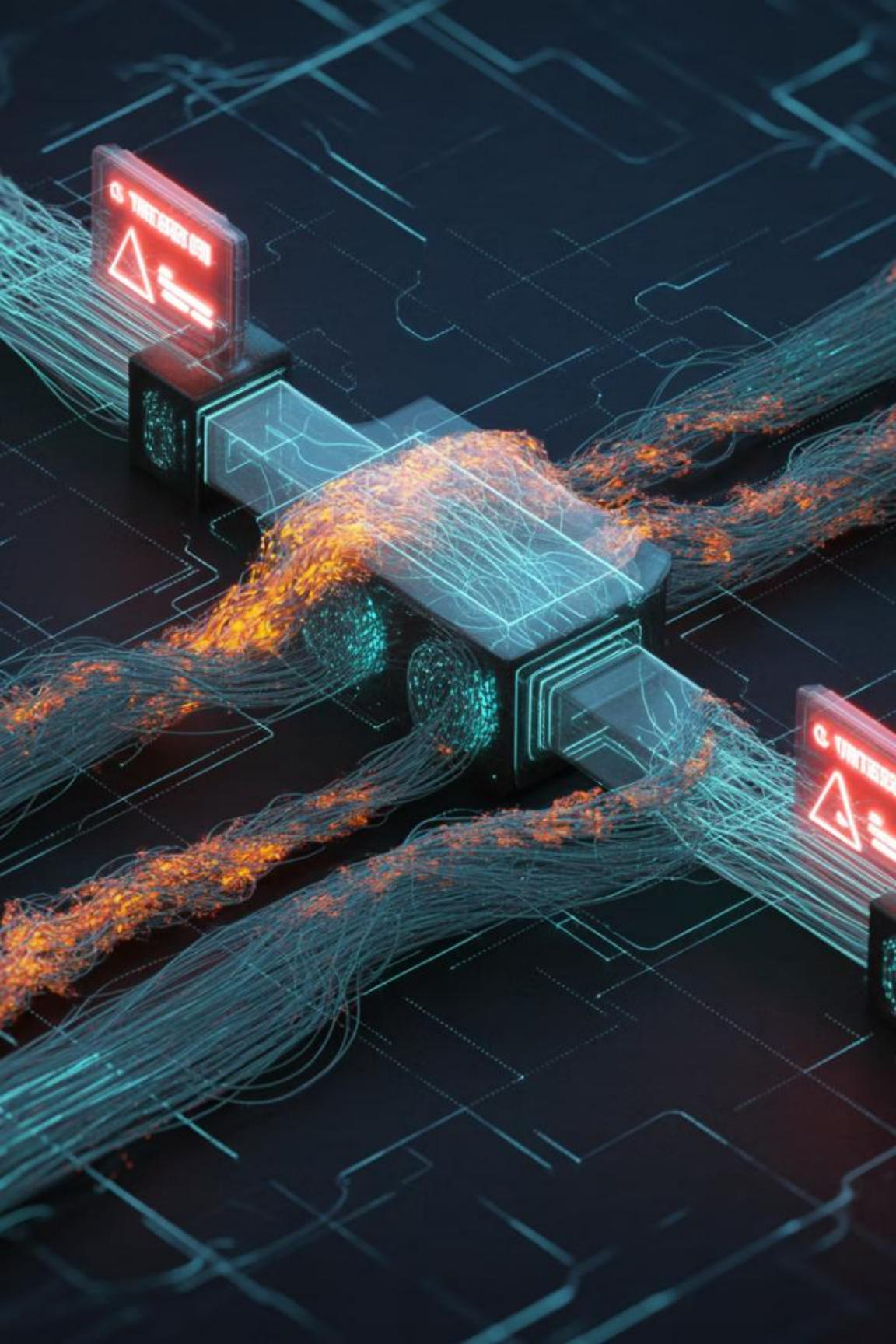
### การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

- จัดทำกระบวนการเพื่อตรวจจับ จัดประเภท วิเคราะห์ และระบุว่ามีภัยคุกคามทางไซเบอร์ และทบทวน อย่างน้อยปีละ 1 ครั้ง

### การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

- เข้าร่วมฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ในระดับชาติ





# ภัยคุกคามทางไซเบอร์ใน หน่วยงานภาครัฐของไทย

- ❑ ปี 2568 ได้รับการประกาศเป็น "ปีแห่งความปลอดภัยทางไซเบอร์" ของประเทศไทย โดยหน่วยงานด้านความปลอดภัยไซเบอร์แห่งชาติและศูนย์ประสานความปลอดภัยคอมพิวเตอร์
- ❑ คาดว่าเศรษฐกิจดิจิทัลไทยจะเติบโตถึง 100 ล้านเหรียญสหรัฐ ภายในปี 2573 ตามแผนยุทธศาสตร์ความปลอดภัยไซเบอร์แห่งชาติ ซึ่งดำเนินการโดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
- ❑ การโจมตีทางไซเบอร์มีจำนวนเพิ่มขึ้นและซับซ้อนมากขึ้น โดยเฉพาะการโจมตีต่อเนื่องขั้นสูงและการโจมตีที่ทำให้ระบบล่ม ซึ่งส่งผลกระทบต่อระบบโครงสร้างพื้นฐานสำคัญของประเทศไทย นับเป็นความท้าทายหลักของหน่วยงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์



# ภัยคุกคามที่มักพบในหน่วยงานภาครัฐ

หน่วยงานภาครัฐไทยกำลังเผชิญกับภัยคุกคามทางไซเบอร์ที่หลากหลายและซับซ้อนมากขึ้น ทั้งการโจมตีผ่านฟิชชิง แรนซัมแวร์แบบหลายชั้น การโจมตีจากรัฐต่างประเทศ และภัยคุกคามที่ขับเคลื่อนด้วยเทคโนโลยี AI (Artificial Intelligence - ปัญญาประดิษฐ์) และ IoT (Internet of Things - อินเทอร์เน็ตของสรรพสิ่ง)



## ฟิชชิงและมัลแวร์

แคมเปญ อีเมลหลอกลวง ที่มีความซับซ้อนสูงเลียนแบบหน่วยงานรัฐ เพื่อขโมยข้อมูลสำคัญ สถิติการโจมตีระบบธนาคารออนไลน์ของรัฐเพิ่มขึ้นถึง 40% ในปีงบประมาณที่ผ่านมา



## แรนซัมแวร์แบบหลายชั้น

กลยุทธ์การเรียกค่าไถ่ข้อมูลแบบซ้อนทับซับซ้อน ผสมผสานทั้งการเข้ารหัสข้อมูลสำคัญ การขู่เปิดเผยข้อมูลลับ และการโจมตีแบบ DDoS (Distributed Denial of Service - การปฏิเสธการให้บริการแบบกระจาย) ไปพร้อมกันเพื่อเพิ่มโอกาสความสำเร็จ



## การโจมตีจากรัฐและ APTs

กลุ่มผู้โจมตีที่ได้รับการสนับสนุนจากรัฐต่างประเทศที่มีทรัพยากรสูง มุ่งเป้าไปที่ข้อมูลความมั่นคงแห่งชาติ นโยบายเศรษฐกิจ และยุทธศาสตร์ด้านการต่างประเทศของไทย APTs (Advanced Persistent Threats - ภัยคุกคามต่อเนื่องขั้นสูง) คือการโจมตีที่มีความซับซ้อนและต่อเนื่องในระยะยาว



## การโจมตีด้วย AI และ IoT

ภัยคุกคามอัจฉริยะที่มีความสามารถในการเรียนรู้และปรับตัว ใช้ระบบปัญญาประดิษฐ์ (AI - Artificial Intelligence) วิเคราะห์และค้นหาช่องโหว่โดยอัตโนมัติ พร้อมใช้ประโยชน์จากอุปกรณ์ IoT (Internet of Things - อินเทอร์เน็ตของสรรพสิ่ง) ที่ขาดการรักษาความปลอดภัยในหน่วยงานรัฐ

# ภัยคุกคามส่งผลกระทบอย่างไรบ้าง

ภัยคุกคามไซเบอร์ส่งผลกระทบรุนแรงต่อภาครัฐทั้งด้านข้อมูล การบริการ ความมั่นคง และการเงิน ก่อให้เกิดความเสียหายที่ครอบคลุมทุกมิติของการทำงานภาครัฐ

## 1 การรั่วไหลของข้อมูล (Data Breach - DB)

ข้อมูลสำคัญของประชาชนและข้อมูลความมั่นคงรั่วไหล ส่งผลต่อความเชื่อมั่นและความปลอดภัยของประเทศ การรั่วไหลของข้อมูลส่วนบุคคล (Personally Identifiable Information - PII) และข้อมูลที่มีชั้นความลับ (Classified Information - CI) เป็นภัยคุกคามระดับสูงต่อหน่วยงานภาครัฐ

## 3 ผลกระทบต่อความมั่นคง (National Security Impact - NSI)

ข้อมูลยุทธศาสตร์อาจถูกโจรกรรม หน่วยงานความมั่นคงสูญเสียความได้เปรียบ เกิดความเสี่ยงต่อความมั่นคงระดับชาติ การโจมตีโดยกลุ่มผู้โจมตีขั้นสูง (Advanced Persistent Threat - APT) และการสอดแนมทางไซเบอร์ (Cyber Espionage - CE) คุกคามความมั่นคงและอธิปไตยของประเทศ

## 2 การหยุดชะงักของบริการ (Service Disruption - SD)

ระบบบริการประชาชนถูกตัดขาด ประชาชนไม่สามารถเข้าถึงบริการสำคัญได้ สร้างความเสียหายทางเศรษฐกิจ การโจมตีแบบปฏิเสธการให้บริการ (Distributed Denial of Service - DDoS) และการโจมตีโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure - CI) ทำให้เกิดภาวะหยุดชะงักของบริการสาธารณะ

## 4 ความเสียหายทางการเงิน (Financial Damage - FD)

งบประมาณสูญเสียจากการถูกโจมตี ค่าใช้จ่ายในการกู้คืนระบบสูง ภาษีประชาชนถูกนำไปแก้ไขความเสียหาย ต้นทุนทางการเงินทั้งทางตรงและทางอ้อม (Direct and Indirect Cost - DIC) รวมถึงค่าใช้จ่ายในการฟื้นฟูและการดำเนินการตามมาตรการรักษาความปลอดภัย (Security Incident Response Cost - SIRC) สร้างภาระทางงบประมาณอย่างมีนัยสำคัญ



# กฎหมายและข้อกำหนดด้านความปลอดภัยไซเบอร์ของไทย

ประเทศไทยได้พัฒนากรอบกฎหมายและข้อกำหนดด้านความปลอดภัยไซเบอร์อย่างต่อเนื่อง เพื่อรับมือกับภัยคุกคามที่เพิ่มขึ้น กฎหมายเหล่านี้ครอบคลุมทั้งการคุ้มครองข้อมูล การจัดการเหตุการณ์ และการกำกับดูแลโครงสร้างพื้นฐานสำคัญ หน่วยงานภาครัฐจำเป็นต้องปฏิบัติตามข้อกำหนดเหล่านี้อย่างเคร่งครัด

| กฎหมาย                                | หน่วยงานรับผิดชอบ                                                                                          | ขอบเขต                                                                     |
|---------------------------------------|------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ 2562  | สกมช. (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ) / NCSA (National Cyber Security Agency) | ดูแลโครงสร้างสำคัญทางสารสนเทศ และจัดการเหตุภัยไซเบอร์                      |
| พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) | PDPC (คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล) / ETDA (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์)                    | ปกป้องข้อมูลส่วนบุคคล คล้าย GDPR (กฎหมายคุ้มครองข้อมูลทั่วไปของสหภาพยุโรป) |
| แนวทางประเมินความปลอดภัยไซเบอร์       | ธนาคารแห่งประเทศไทย (Bank of Thailand)                                                                     | สำหรับสถาบันการเงิน ประเมินความเสี่ยง                                      |
| พ.ร.บ. คอมพิวเตอร์ (แก้ไข 2560)       | กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม                                                                        | ควบคุมอาชญากรรมไซเบอร์ เช่น การแฮ็ก                                        |
| ยุทธศาสตร์ความปลอดภัยไซเบอร์แห่งชาติ  | กระทรวงกลาโหม / สมช. (สำนักงานสภาความมั่นคงแห่งชาติ)                                                       | แนวทางปกป้องโครงสร้างพื้นฐานสำคัญ                                          |
| แนวปฏิบัติ ThaiCERT                   | ThaiCERT (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย) / สกมช.                            | วิธีรับมือเหตุการณ์ไซเบอร์                                                 |



# ประเภทของภัยคุกคามและวิธีการป้องกัน

ตารางนี้แสดงประเภทของภัยคุกคามทางไซเบอร์ที่หน่วยงานรัฐบาลไทยเผชิญอยู่ พร้อมตัวอย่างของการโจมตีและมาตรการป้องกันที่เหมาะสมสำหรับแต่ละภัยคุกคาม การทำความเข้าใจภัยคุกคามเหล่านี้จะช่วยให้หน่วยงานรัฐสามารถวางแผนกลยุทธ์การป้องกันได้อย่างมีประสิทธิภาพ

| Threat Type                                                    | Example                                                   | How to Protect                                                                                                                             |
|----------------------------------------------------------------|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Phishing (การหลอกลวงทางอีเมล)                                  | Email fraud, SMS scam                                     | Email security, awareness training, web filters                                                                                            |
| Ransomware (มัลแวร์เรียกค่าไถ่)                                | Babuk, LYNX                                               | Regular backups, EDR/XDR (Endpoint Detection and Response/Extended Detection and Response) solutions, timely patching, threat intelligence |
| APT (Advanced Persistent Threat - การโจมตีแบบต่อเนื่องขั้นสูง) | Nation-state intrusions                                   | Next-Gen Firewalls, IPS (Intrusion Prevention Systems), Cyber Threat Intelligence, network segmentation                                    |
| Scam Networks (เครือข่ายฉ้อโกง)                                | Call center frauds, traffic hijacking                     | DNS (Domain Name System) security, threat intelligence, takedown services                                                                  |
| Legacy Infrastructure (โครงสร้างพื้นฐานเก่า)                   | Outdated VPN (Virtual Private Network), operating systems | Patch management, vulnerability scanning                                                                                                   |
| Insider Threat (ภัยคุกคามจากบุคคลภายใน)                        | Misuse of privileges, data leaks                          | DLP (Data Loss Prevention), access control, monitoring                                                                                     |
| AI/IoT Threats (ภัยคุกคามจาก AI และ IoT)                       | Deepfakes, IoT (Internet of Things) attacks               | IoT security monitoring, AI-based threat modeling                                                                                          |



# โซลูชันด้านความปลอดภัยไซเบอร์

โซลูชันด้านความปลอดภัยไซเบอร์มีความหลากหลายและครอบคลุมทุกขั้นตอนของการรักษาความปลอดภัย ตั้งแต่การป้องกัน การตรวจจับ การวิเคราะห์ จนถึง การตอบสนองต่อภัยคุกคาม หน่วยงานภาครัฐควรพิจารณาเลือกใช้โซลูชันที่เหมาะสมตามความต้องการและความเสี่ยงขององค์กร



## ระบบป้องกัน (Protect)

- ไฟร์วอลล์รุ่นใหม่ (Next Generation Firewall - NGFW)
- ไฟร์วอลล์สำหรับเว็บแอปพลิเคชัน (Web Application Firewall - WAF)
- ระบบป้องกันการบุกรุก (Intrusion Prevention System - IPS)
- เกตเวย์ความปลอดภัยเว็บ (Security Web Gateway)
- ระบบป้องกันการรั่วไหลของข้อมูล (Data Loss Prevention - DLP)
- ระบบจัดการสิทธิ์ผู้ใช้พิเศษ (Privileged Access Management - PAM)
- การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication - MFA)
- การเข้าถึงเครือข่ายแบบไม่เชื่อใจ (Zero Trust Network Access)



## ระบบตรวจจับ (Detect)

- ระบบตรวจจับและตอบสนองระดับเอนด์พอยต์ (Endpoint Detection and Response - EDR)
- ระบบตรวจจับและตอบสนองแบบขยาย (Extended Detection and Response - XDR)
- ระบบตรวจจับและตอบสนองระดับเครือข่าย (Network Detection and Response - NDR)
- การวิเคราะห์พฤติกรรมผู้ใช้ (User Behavior Analytics)
- แพลตฟอร์มข่าวกรองภัยคุกคาม (Threat Intelligence Platforms)
- เครื่องมือสแกนช่องโหว่ (Vulnerability Scanners)



## ระบบวิเคราะห์ (Analyze)

- ศูนย์ปฏิบัติการความมั่นคงปลอดภัย (Security Operations Center - SOC)
- ระบบจัดการข้อมูลและเหตุการณ์ด้านความปลอดภัย (Security Information and Event Management - SIEM)
- ระบบประสานงาน ทำงานอัตโนมัติ และตอบสนองด้านความปลอดภัย (Security Orchestration, Automation and Response - SOAR)
- เครื่องมือล่าภัยคุกคาม (Threat Hunting Tools)
- ระบบตรวจจับความผิดปกติด้วย AI (AI-Based Anomaly Detection)
- แพลตฟอร์มวิเคราะห์นิติวิทยาศาสตร์ดิจิทัล (Forensic Analysis Platforms)



## ระบบตอบสนอง (Respond)

- แพลตฟอร์มตอบสนองต่อเหตุการณ์ (Incident Response Platforms)
- เครื่องมือนิติวิทยาศาสตร์ดิจิทัล (Digital Forensics Tools)
- โซลูชันสำรองและกู้คืนข้อมูล (Backup & Recovery Solutions)
- ระบบจัดการวิกฤต (Crisis Management Systems)
- เครื่องมือแจ้งเตือนการละเมิดข้อมูล (Breach Notification Tools)
- การฝึกอบรมความตระหนักรู้ด้านความปลอดภัย (Security Awareness Training)



# การป้องกันตามกรอบ NIST

กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ NIST (National Institute of Standards and Technology) เป็นแนวทางที่ได้รับการยอมรับในระดับสากล ช่วยให้องค์กรภาครัฐและเอกชนสามารถประเมิน จัดการ และลดความเสี่ยงด้านไซเบอร์ได้อย่างมีประสิทธิภาพ กรอบนี้แบ่งเป็น 5 ฟังก์ชันหลักที่สามารถดำเนินการพร้อมกันและต่อเนื่อง

## Identify (ระบุ)

การระบุทรัพย์สินดิจิทัลและความเสี่ยง ประกอบด้วย การจัดทำ Asset Management (AM), Business Environment (BE), Governance (GV), Risk Assessment (RA) และ Risk Management Strategy (RM) เพื่อเข้าใจบริบทธุรกิจ และทรัพยากรที่ต้องปกป้อง

## Recover (ฟื้นฟู)

การกู้คืนและดำเนินการต่อเนื่อง ประกอบด้วย Recovery Planning (RP), Improvements (IM) และ Communications (CO) เพื่อฟื้นฟูระบบและบริการให้กลับมาทำงานได้ตามปกติ พร้อมทั้งปรับปรุงแผนจากบทเรียนที่ได้รับ



## Protect (ป้องกัน)

การใช้มาตรการป้องกันที่เหมาะสม รวมถึง Access Control (AC), Awareness and Training (AT), Data Security (DS), Information Protection Processes and Procedures (IP), Maintenance (MA) และ Protective Technology (PT) เพื่อสร้างระบบป้องกันหลายชั้น

## Detect (ตรวจจับ)

ระบบตรวจจับการโจมตีทางไซเบอร์ ประกอบด้วย Anomalies and Events (AE), Security Continuous Monitoring (CM) และ Detection Processes (DP) เพื่อติดตามและวิเคราะห์เหตุการณ์ด้านความปลอดภัยอย่างต่อเนื่อง

## Respond (ตอบสนอง)

แผนตอบสนองต่อเหตุการณ์ไซเบอร์ ประกอบด้วย Response Planning (RP), Communications (CO), Analysis (AN), Mitigation (MI) และ Improvements (IM) เพื่อรับมือกับภัยคุกคามอย่างเป็นระบบและลดผลกระทบ



# โซลูชันที่สอดคล้องกับกรอบ NIST

การประยุกต์ใช้กรอบความมั่นคงปลอดภัยไซเบอร์ NIST อย่างมีประสิทธิภาพจำเป็นต้องเลือกโซลูชันที่เหมาะสมสำหรับแต่ละฟังก์ชัน ตารางต่อไปนี้แสดงโซลูชันด้านความปลอดภัยไซเบอร์ที่ควรพิจารณาสำหรับแต่ละฟังก์ชันของกรอบ NIST เพื่อยกระดับการป้องกันภัยคุกคามทางไซเบอร์แบบครบวงจรสำหรับหน่วยงานภาครัฐไทย

| NIST ฟังก์ชัน | โซลูชันที่แนะนำ                                                                                                                                                                                                          | ประโยชน์ที่ได้รับ                                                                          |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Identify      | SIEM (Security Information and Event Management - ระบบจัดการข้อมูลและเหตุการณ์ด้านความปลอดภัย), CTI (Cyber Threat Intelligence - ข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์)                                                      | ระบุทรัพย์สินดิจิทัลและวิเคราะห์ภัยคุกคามอย่างครอบคลุม                                     |
| Protect       | NGFW (Next-Generation Firewall - ไฟร์วอลล์รุ่นใหม่), WAF (Web Application Firewall - ไฟร์วอลล์สำหรับเว็บแอปพลิเคชัน), DLP (Data Loss Prevention - การป้องกันการรั่วไหลของข้อมูล), Security Web Gateway (ประตูเว็บนิรภัย) | สร้างชั้นป้องกันหลายระดับเพื่อรักษาความปลอดภัยข้อมูลและป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต |
| Detect        | IPS (Intrusion Prevention System - ระบบป้องกันการบุกรุก), EDR (Endpoint Detection and Response - การตรวจจับและตอบสนองที่ปลายทาง), XDR (Extended Detection and Response - การตรวจจับและตอบสนองแบบขยาย)                    | ตรวจจับและวิเคราะห์การโจมตีทางไซเบอร์ในเวลาจริง พร้อมแจ้งเตือนอัตโนมัติ                    |
| Respond       | SOAR (Security Orchestration, Automation and Response - การประสานงาน ระบบอัตโนมัติ และการตอบสนองด้านความปลอดภัย), SOC (Security Operations Center - ศูนย์ปฏิบัติการความปลอดภัย)                                          | ตอบสนองต่อเหตุการณ์ด้านความปลอดภัยอย่างรวดเร็วและเป็นระบบ ลดผลกระทบจากการโจมตี             |
| Recover       | SOC (Security Operations Center - ศูนย์ปฏิบัติการความปลอดภัย), SIEM (Security Information and Event Management - ระบบจัดการข้อมูลและเหตุการณ์ด้านความปลอดภัย), ระบบสำรองและกู้คืนข้อมูล                                  | ฟื้นฟูระบบที่ได้รับผลกระทบ วิเคราะห์สาเหตุรากฐาน และป้องกันการเกิดซ้ำในอนาคต               |



# การเลือกและนำโซลูชันต่างๆมาปรับใช้ในหน่วยงาน

การเลือกและประยุกต์ใช้มาตรการป้องกันต้องมีขั้นตอนที่ชัดเจน เพื่อให้เกิดประสิทธิภาพสูงสุด

กระบวนการปรับใช้โซลูชันด้านความปลอดภัยไซเบอร์ที่มีประสิทธิภาพประกอบด้วย 4 ขั้นตอนหลัก: การประเมินความเสี่ยง การพัฒนาแผนงาน การนำไปใช้และบูรณาการ และการติดตามผลเพื่อปรับปรุงอย่างต่อเนื่อง

## ประเมินความเสี่ยงและความต้องการ

วิเคราะห์ภัยคุกคามเฉพาะของหน่วยงาน รวมถึงทรัพยากรที่มีและข้อจำกัดด้านงบประมาณ

- ทำการประเมินช่องโหว่อย่างสม่ำเสมอ
- จัดลำดับความสำคัญของทรัพย์สินที่ต้องปกป้อง

## ดำเนินการและบูรณาการ

นำโซลูชันมาใช้ตามลำดับความสำคัญ ควบคู่กับการฝึกอบรมบุคลากร

- เริ่มจากระบบสำคัญและขยายไปทั่วองค์กร
- สร้างวัฒนธรรมความปลอดภัยทั่วทั้งองค์กร

1

2

3

4

## พัฒนาแผนงานความปลอดภัย

จัดทำแผนที่สอดคล้องกับกรอบ NIST (National Institute of Standards and Technology - สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ) และนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

- กำหนดมาตรฐานและแนวทางปฏิบัติ
- จัดสรรงบประมาณและทรัพยากรที่จำเป็น

## ติดตามและปรับปรุง

ประเมินประสิทธิภาพของมาตรการอย่างต่อเนื่อง และปรับเปลี่ยนตามภัยคุกคามใหม่

- จัดทำการทดสอบเจาะระบบเป็นประจำ
- รายงานและวิเคราะห์เหตุการณ์ด้านความปลอดภัย



# การเตรียมพร้อมสำหรับอนาคต

การเตรียมความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์สำหรับอนาคตของประเทศไทย มุ่งเน้นการพัฒนาในสี่ด้านหลัก: เศรษฐกิจดิจิทัล การรับมือภัยคุกคาม การพัฒนาบุคลากร และโซลูชันระดับประเทศ



## เศรษฐกิจดิจิทัลที่เติบโตอย่างก้าวกระโดด (DGE - Digital Growth Economy)

คาดการณ์มูลค่าจะเพิ่มขึ้นถึงสองเท่าภายในปี 2573 สร้างโอกาสและความท้าทายใหม่ การพัฒนาเศรษฐกิจดิจิทัลประเทศไทยจะเพิ่มความสามารถในการแข่งขันระดับโลกและขับเคลื่อนนวัตกรรมในทุกภาคส่วน



## รับมือภัยคุกคามที่ซับซ้อนยิ่งขึ้น (CTM - Complex Threat Management)

พัฒนาระบบป้องกันแบบปรับตัวได้เพื่อตอบสนองต่อภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็ว ประเทศไทยกำลังลงทุนในโครงสร้างพื้นฐานที่มั่นคงเพื่อป้องกันการโจมตีทางไซเบอร์รูปแบบใหม่และการโจมตีขั้นสูง



## ยกระดับศักยภาพบุคลากรด้านไซเบอร์ (CWD - Cyber Workforce Development)

สร้างกำลังคนที่มีความเชี่ยวชาญสูงและพร้อมรับมือกับความท้าทายด้านความปลอดภัยไซเบอร์ยุคใหม่ แผนพัฒนากำลังคนด้านไซเบอร์แห่งชาติมุ่งเน้นการเพิ่มจำนวนผู้เชี่ยวชาญที่ได้รับการรับรองมาตรฐานสากล



## โซลูชันระดับประเทศที่ล้ำสมัย (NCS - National Cybersecurity Solutions)

บูรณาการเทคโนโลยีขั้นสูงเพื่อเสริมสร้างความยืดหยุ่นและความแข็งแกร่งทางไซเบอร์ให้ประเทศไทยในระยะยาว โครงการศูนย์ปฏิบัติการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (NCOC) เป็นหนึ่งในความพยายามสำคัญเพื่อยกระดับความพร้อมของประเทศ



# ขอขอบคุณครับ



08-1842-8411



[www.mnre.go.th](http://www.mnre.go.th)



[kantaphan@mnre.go.th](mailto:kantaphan@mnre.go.th)



92 ซอยพหลโยธิน 7 ถนนพหลโยธิน  
เขต/แขวง พญาไท กทม. 10400

