มหาวิทยาลัยเชียงใหม่
CHIANG MAI UNIVERSITY
CMU

ECCMU
EMPLOYEE COUNCIL
CHIANG MAI UNIVERSITY
สภาพนักงาน มหาวิทยาลัยเชียงใหม่

ITSC CMU
Information Technology Service Center
Chiang Mai University

สภาพนักงาน
มหาวิทยาลัยเชียงใหม่ พ.ศ.๒๕๐๗

การเตรียมความพร้อมด้านการรักษาความมั่นคงปลอดภัย

# ให้กับข้อมูลส่วนบุคคล

# ความรู้เรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับผู้ดูแลระบบ


## สหรัฐฯ ประกาศภาวะฉุกเฉิน
## บ.ท่อส่งน้ำมันถูกแฮ็ก

### CISCO โดนแฮ็กโดยแก๊งแรนซัมแวร์ YANLUOWANG

August 11, 2022 Cisco, Database Security, Network Security, Products, Security

Cisco ออกมายอมรับว่า ได้ถูกแก๊งแรนซัมแวร์ Yanluowang ลุกล้ำเข้ามาในเครือข่ายขององค์กรจริง เหตุการณ์เกิดขึ้นเมื่อช่วงปลายเดือนพฤษภาคมที่ผ่านมา และยังถูกรีดไถจากไฟล์ข้อมูลที่ถูกโจรกรรมออกไป


*Credit : bleepingcomputer.com*

MARKET THINK

## โรงงาน Toyota ในญี่ปุ่นทั้งหมด
## ต้องหยุดการผลิตชั่วคราว เพราะ


## เคยถูกโจมตีทางไซเบอร์ แต่ไม่รู้ว่ามีอยู่


## เซิร์ฟเวอร์ และฐานเก็บข้อมูลล่มเหตุเพราะ
## โดน Ransomware โจมตี

# Top Trends in Cybersecurity, 2022

01 Attack surface expansion

02 Identity system defense

03 Digital supply chain risk

04 Vendor consolidation

05 Cybersecurity mesh

06 Distributed decisions

07 Beyond awareness

gartner.com



## Cyber Security Trends

- Attacks Against Cloud Services
- Integration of AI and Machine Learning
- Organizational Behavior
- Rise in IoT Devices
- Increasing Threat of Deepfakes
- Explosion of BYOD and Mobile Devices
- Rise in Cyber

Aite Novarica

## TOP 10 TRENDS in Cybersecurity, 2022

*Escalating Stakes Drive Increasing Investments*


01 **Ransomware** becomes the weapon of nation-state cyber

02 **DataSecOps** becomes a real thing

03 **Security data lake** and **SOAR** solution combinations begin to push SIEM solutions underwater

04 **Managed incident** response takes the market by storm

05 **Governments** double down on cybersecurity

06 Firms move full speed ahead with **zero-trust deployment**

07 **Shift-left security** is noble but not enough to eliminate cyberattacks

08 **Cybersecurity M&A** will thrive in 2022

09 **The MSSP market** grows through aggressive acquisition

10 Firms mature their approach to **model risk management**

Source: Aite-Novarica Group | www.aite-novarica.com

SelectHub

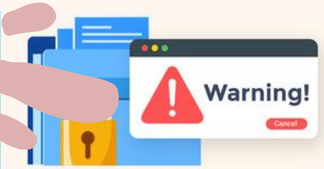
# หน้าที่ ผู้ประมวลผลข้อมูลส่วนบุคคล

Responsibilities of a Data Processor

กฎหมายกำหนดหน้าที่เฉพาะสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล 2562 มาตรา 40 ดังนี้

1. ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติตาม พ.ร.บ. นี้

2. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น




3. จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด


4. จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเฉพาะเมื่อเข้าเงื่อนไขที่มาตรา 41 กำหนด

หากผู้ประมวลผลข้อมูลส่วนบุคคลไม่ปฏิบัติตาม ต้องระวางโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล



# หน้าที่ ผู้ควบคุมข้อมูลส่วนบุคคล

Responsibilities of a Data Controller

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 37 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล 2562

1. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือโดยมิชอบ

2. ในกรณีต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือโดยมิชอบ

3. จัดให้มีระบบตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาเก็บรักษา หรือที่ไม่เกี่ยวข้อง หรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวม หรือเจ้าของข้อมูลร้องขอ หรือเจ้าของข้อมูลได้ถอนความยินยอม


4. แจ้งเหตุละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้า ภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลให้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย

5. ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลอยู่นอกราชอาณาจักร ต้องแต่งตั้งตัวแทนเป็นหนังสือ ซึ่งตัวแทนต้องอยู่ในราชอาณาจักรและต้องได้รับมอบอำนาจให้กระทำการแทนโดยไม่มีข้อจำกัดความรับผิดใด ๆ ที่เกี่ยวกับการเก็บ รวบรวม หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคล

** ผู้ควบคุมข้อมูลส่วนบุคคลยังมีหน้าที่อื่นที่ต้องดำเนินการ โดยมีรายละเอียดตามมาตราที่เกี่ยวข้อง

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

- **Security Concept & Governance**
- **Asset Security**
- **Identity and Access Management**
- **Communication/Network Security**
- **Security Architecture and Engineering**
- Security Assessment and Testing
- Security Operations
- Software Development Security


• Security Concept & Governance
• Asset Security
• Identity and Access Management
• Communication/Network Security
• Security Architecture and Engineering
• Security Assessment and Testing
• Security Operations
• Software Development Security

Fundamental Principles of Security

# หลักการพื้นฐาน


Confidentiallity

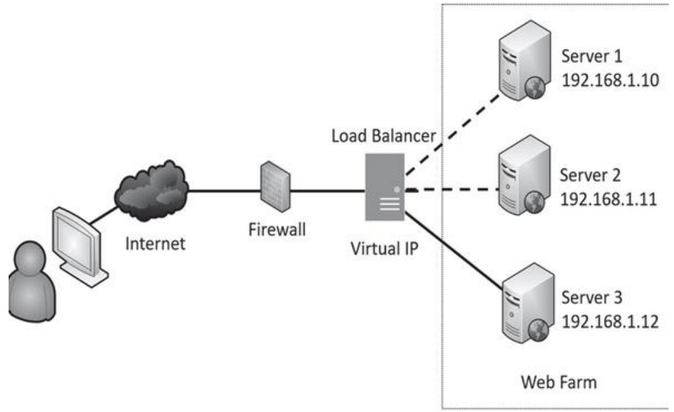
- เข้าถึงเฉพาะที่จำเป็น
- ป้องกันการเข้าถึงที่ไม่อนุญาต
- Data ในทุก State
- ภัยที่เกี่ยวข้อง Social Engineering,Breaking Encryption
- ป้องกัน IAA,Encryption,Data Classification,Access controls,User Awareness

Integrity

- accuracy & reliability
- unauthorized modification
- ป้องกัน Hashing,Digital signatures,Certificates, Change control

Availability

- เข้าถึงได้เมื่อต้องการ
- ความเชื่อถือมั่นใจในระบบ
- performance ต้องได้
- ป้องกันแก้ไข Cyber Resilience BCP,DR,Redundancy,Fault tolerance



# เป้าหมาย cyber security
# ป้องกันความเสี่ยงทุกรูปแบบ

## Threat

ภัยการโจมตีไปยังจุดอ่อนของระบบ

## Vulnerability

จุดอ่อนของระบบทำให้เกิดการโจมตี software hardware people physical

## Risk

โอกาสที่ Threat จะโจมตี Vulnerability ต้องมีการทำ Risk Management หรือ Mitigation เพื่อลดโอกาสและผลกระทบจากการโจมตี

# Control Types

- Technical Controls - Technology
- Administrative Controls - Management
- Physical Controls - Physically touch

Technical Controls

- Encryption
- Antivirus
- IPS
- Firewall
- Access Control
- IAA

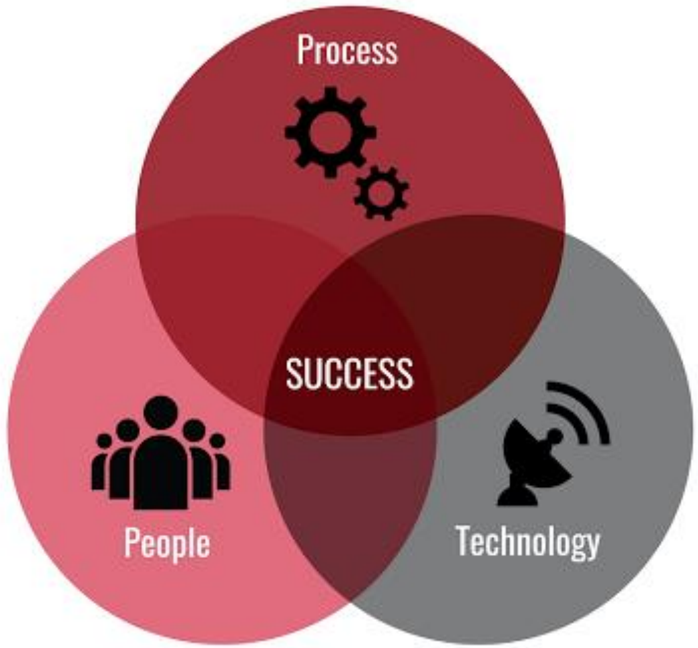
Administrative Controls

- Risk Management
- Vulnerability Accessments
- Penetration tests
- Awareness & Training
- Change Management
- BCP

## Security Policy

- Standards
- Procedures
- guidelines
- Threat Modeling
- Identifying Threats
- Reduction/Risk Analysis
- Prioritization & Response

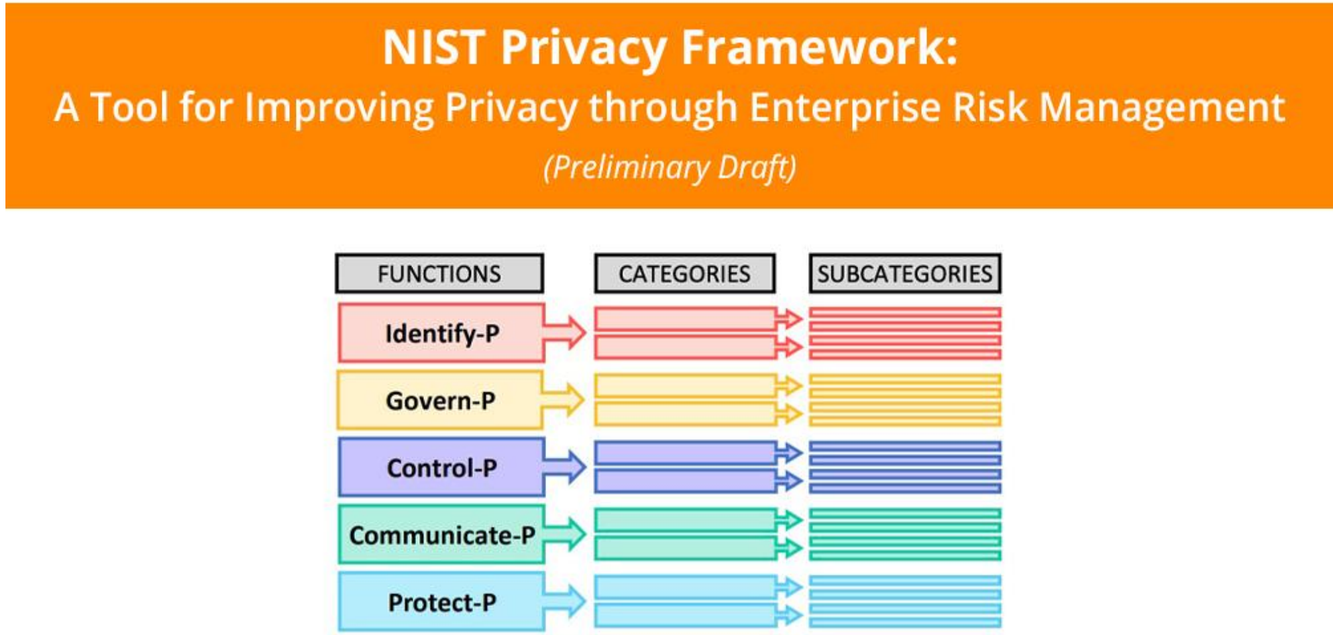
## GOVERNANCE

# Security Frameworks

แต่ละ Frameworks เอาหลายๆ องค์ประกอบมารวมเข้าด้วยกันในมุมมองที่แตกต่างกัน ส่วนใหญ่ใช้แนวคิดแบบ Layer มีแนวทางเอกลักษณ์ของตนเอง และมีเป้าหมายเดียวกันคือ CIA

- ISO/IEC 27000 series ISMS developed by ISO&IEC
- Zachman Framwork - Enterprise architectures by John Zachman
- TOGAF - EA by The Open Group
- COBIT5 - business framework for IT enterprise management and governance (ISACA)
- NIST SP 800-53 - set of controls checklist U.S. federal by National Institute of Standards and Technology
- ITIL - IT Service management by United Kingdom's Office of Government Commerce
- ฯลฯ



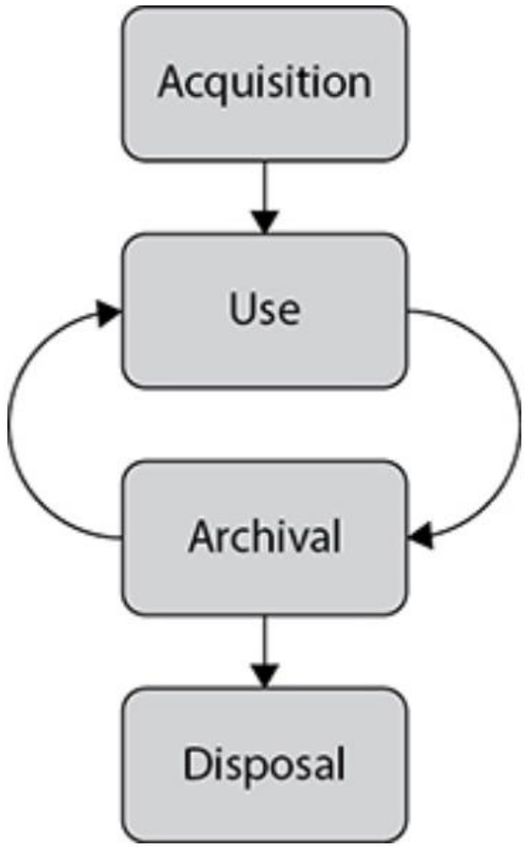

• Security Concept & Governance
• Asset Security
• Identity and Access Management
• Communication/Network Security
• Security Architecture and Engineering
• Security Assessment and Testing
• Security Operations
• Software Development Security

# Data is a precious thing

## Asset

- worth to organization
- people , partners , equipment, facilities, reputation , information
- asset needs to be protected
- information life-cycle
- Threat to information
- mitigating the risks

## LIFE CYCLE




Information Life Cycle

- Acquisition

สร้าง

- Use

ใช้

- Archival -> Backup

เก็บ

- Disposal

ทำลาย

- **Security Concept & Governance**
- **Asset Security**
- **Identity and Access Management**
- **Communication/Network Security**
- **Security Architecture and Engineering**
- Security Assessment and Testing
- Security Operations
- Software Development Security

Authentication

# Authentication Concepts

- Identification

subject claiming , subject provide identity to system, unique identities

Authentication

- Subject(User) Proves identity(Password), second step,

Authorization

- Access to resources granted based on proven identity

defense-in-depth

- multiple security control
- multilayered defense system
- minimizes probability

# Factor of Authentication


### Something you know

- Username & Password

### Something you have

- smart card,rfid,HW Token

### Something you are

- biometric->fingerprint,retinal,iris,voice,facial

### Somewhere you are

- location using geolocation,IP,MAC,GPS

### Something you do

- gestures on touch screen,keystrokes

- **Security Concept & Governance**
- **Asset Security**
- **Identity and Access Management**
- **Communication/Network Security**
- **Security Architecture and Engineering**
- Security Assessment and Testing
- Security Operations
- Software Development Security

Packet Filtering Firewalls

Proxy Firewalls

Next-Generation Firewalls

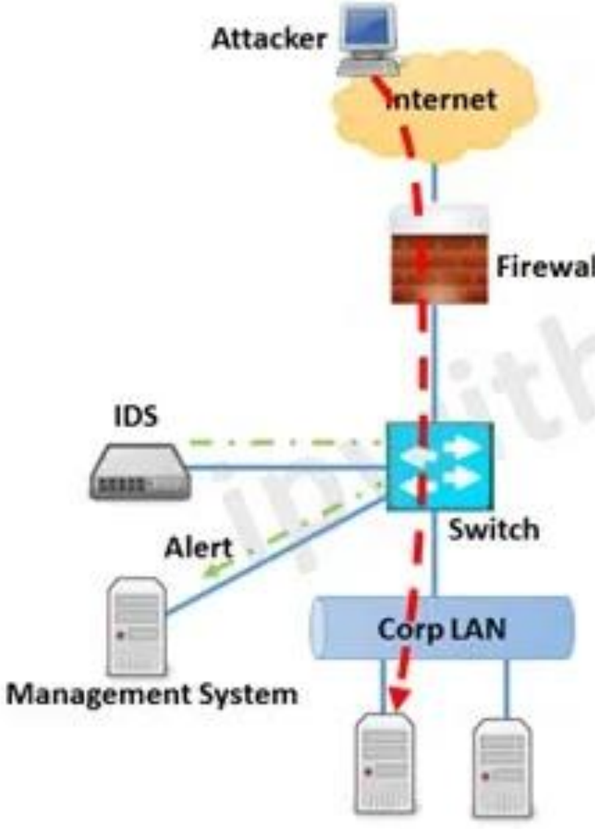
Circuit-level Gateways


Unified Threat Management Firewalls

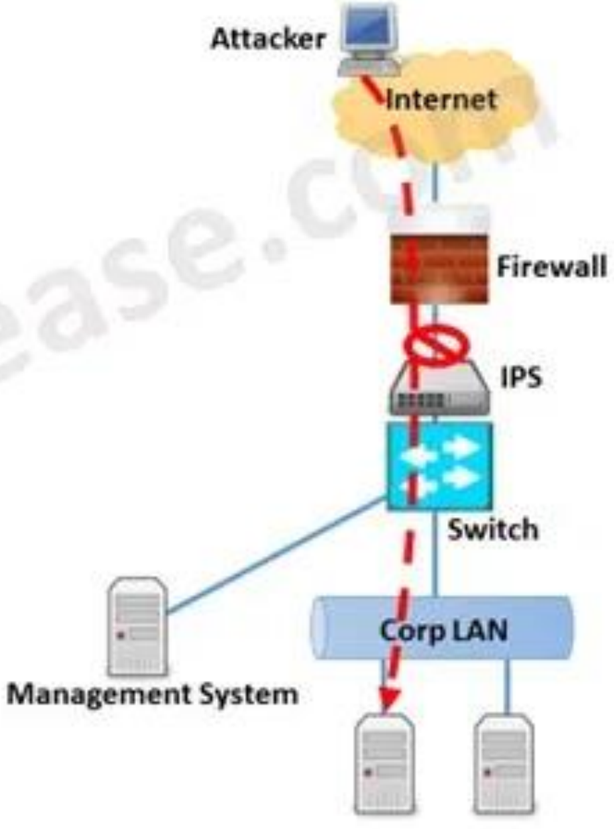
Stateful inspection Firewalls

# IDS vs IPS

## Intrusion Detection System




## Intrusion Prevention System



# Types of Wireless Encryption

**WEP**

It is an old and original wireless **security standard** which can be cracked easily

**WPA**

Uses **a 48 bit IV, 32 bit CRC** and TKIP encryption for wireless security

**WPA2**

WPA2 uses AES (128 bit) and **CCMP** for wireless data encryption

**WPA2 Enterprise**

It integrates **EAP standards** with WPA encryption

**TKIP**

A security protocol used in **WPA** as a replacement for **WEP**

**AES**

It is a **symmetric-key encryption**, used in WPA2 as a replacement of TKIP

**EAP**

Uses **multiple authentication** methods, such as token cards, Kerberos, certificates,etc.

**LEAP**

It is a proprietary **WLAN authentication** protocol developed by Cisco

**RADIUS**

It is a **centralized authentication** and authorization management system

**802.11i**

It is an **IEEE standard** that specifies security mechanisms for 802.11 wireless networks

**CCMP**

CCMP utilizes **128-bit keys,** with a 48-bit initialization vector (IV) for replay detection

- **Security Concept & Governance**
- **Asset Security**
- **Identity and Access Management**
- **Communication/Network Security**
- **Security Architecture and Engineering**
  - **Security Model,Cryptography,Physical Security**
- Security Assessment and Testing
  - Software Testing,Security Testing,Threat Modeling
- Security Operations
  - Asset Management,BCP,Log&Incident Management
- Software Development Security
  - SDLC,DB Architecture,DEV Methods

# กรอบการดำเนินการการรักษาความมั่นคงปลอดภัยไซเบอร์

# กฎหมายที่เกี่ยวข้องกับไอที

- พรบ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ 2544
- ร่าง พรบ ว่าด้วยการพัฒนาโครงสร้างพื้นฐานสารสนเทศ 2543
- พรบ ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ 2550->2560
- พรบ ระบบการชำระเงิน 2560
- พรบ คุ้มครองข้อมูลส่วนบุคคล 2562
- **พรบ การรักษาความมั่นคงปลอดภัยไซเบอร์ 2562**

# พรบ การรักษาความมั่นคงปลอดภัยไซเบอร์ 2562

28 พ.ค. 2562

ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

ต่อระบบคอมพิวเตอร์ หน่วยงานโครงสร้างพื้นฐานฯ ที่สำคัญ

ไม่สามารถทำงานได้เป็นปกติ

กระทบต่อการให้บริการประชาชน ความสงบเรียบร้อยภายในประเทศ

หน่วยงานควบคุมหรือกำกับดูแล

# พรบ การรักษาความมั่นคงปลอดภัยไซเบอร์ 2562

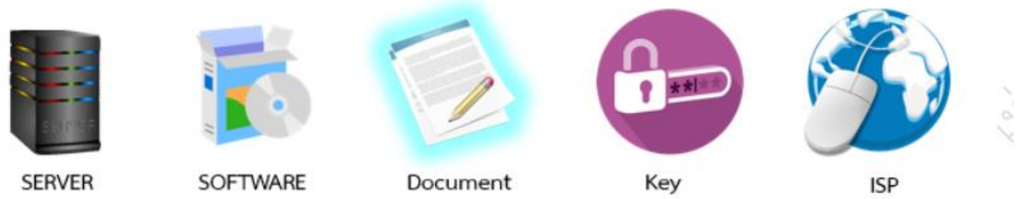
# ความมั่นคงปลอดภัยสารสนเทศ

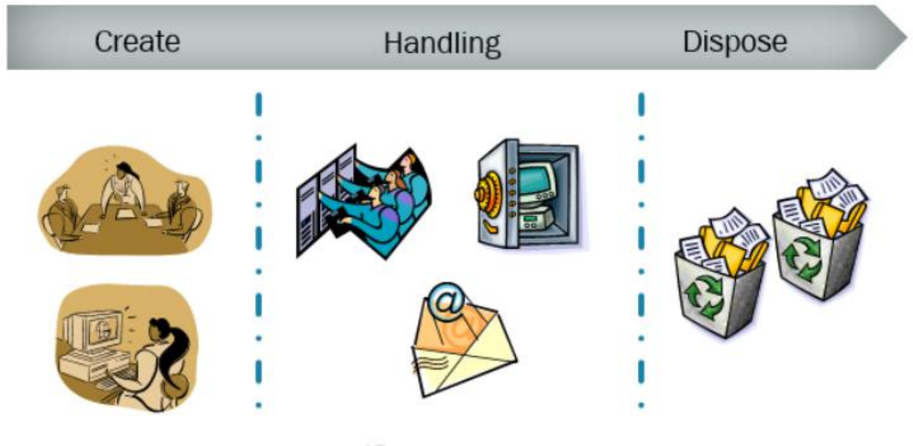
## สารสนเทศ (INFORMATION)

- สารสนเทศ (Information) คือ ทรัพย์สินสารเทศที่อยู่ในรูปแบบของ แอนะล็อก ดิจิทัล หรือทรัพย์สินทางปัญญา คำพูด การสื่อสารด้วยภาพ

## INFORMATION LIFE CYCLE


## สารสนเทศในรูปแบบต่าง ๆ

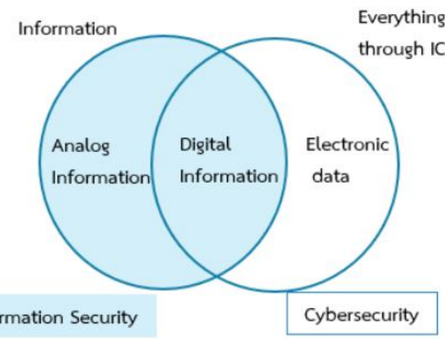


# Information Security vs Cyber Security

**ความแตกต่างระหว่าง INFORMATION SECURITY และ CYBER SECURITY**

- Information security จะปกป้องข้อมูลที่อยู่ในรูปแบบของ Digital Information และ Analog Information ซึ่งจะครอบคลุมไปถึง Physical ที่ทำหน้าที่เก็บรักษา Digital Information
- Cyber security จะปกป้องทุกสิ่งที่สามารถเข้าถึงข้อมูลได้ผ่าน cyberspace ซึ่งจะเป็นข้อมูลอิเล็กทรอนิกส์




| Information Security | Cybersecurity |
|---|---|
| ปกป้อง electronic data และ physical data | ปกป้อง electronic data เท่านั้น |
| รักษาความปลอดภัยข้อมูลเพื่อการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งาน | ปกป้องข้อมูลที่มีค่าและมีความเสี่ยงที่จะถูกแฮก หรือถูกจารกรรม |
| ป้องกันข้อมูลจากช่องทางอื่นๆ นอกเหนือจาก cyberspace | ป้องกันภัยคุกคามจาก cyberspace เท่านั้น |
| มุ่งเน้นการเข้าถึง และคงไว้ซึ่งความลับและความถูกต้องของข้อมูล | มุ่งเน้นการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตจากระบบเครือข่ายเครื่องคอมพิวเตอร์แม่ข่าย |

# ความมั่นคง ปลอดภัยสารสนเทศ

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

หรือ ISO/IEC27001:2013 คือ ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เป็นมาตรฐานสากลเน้นการบริหารจัดการข้อมูลสารสนเทศสำคัญให้มีความมั่นคงปลอดภัย

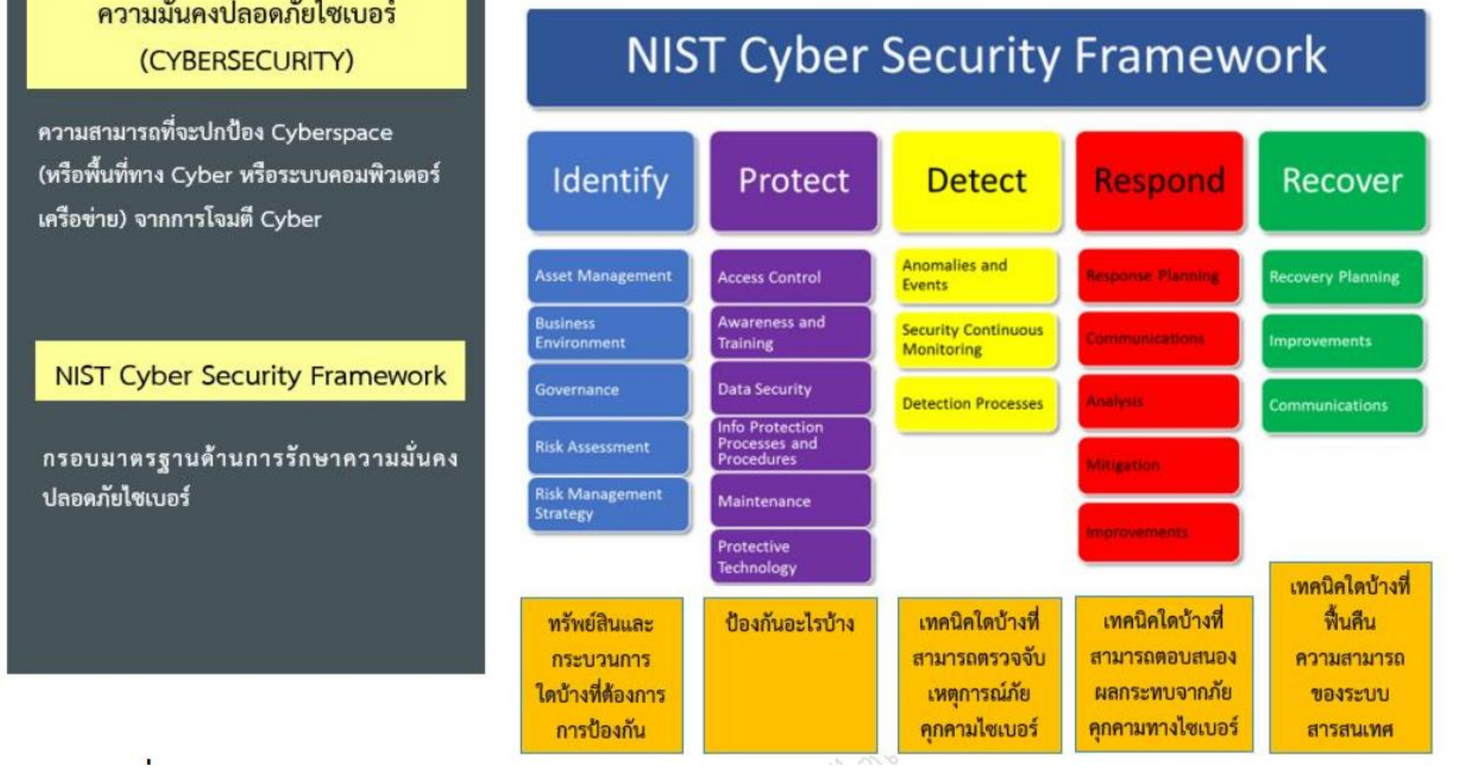
# NIST Framework

**ความมั่นคงปลอดภัยไซเบอร์ (CYBERSECURITY)**

ความสามารถที่จะปกป้อง Cyberspace (หรือพื้นที่ทาง Cyber หรือระบบคอมพิวเตอร์ เครือข่าย) จากการโจมตี Cyber

**NIST Cyber Security Framework**

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์



## CYBERSECURITY FRAMEWORK

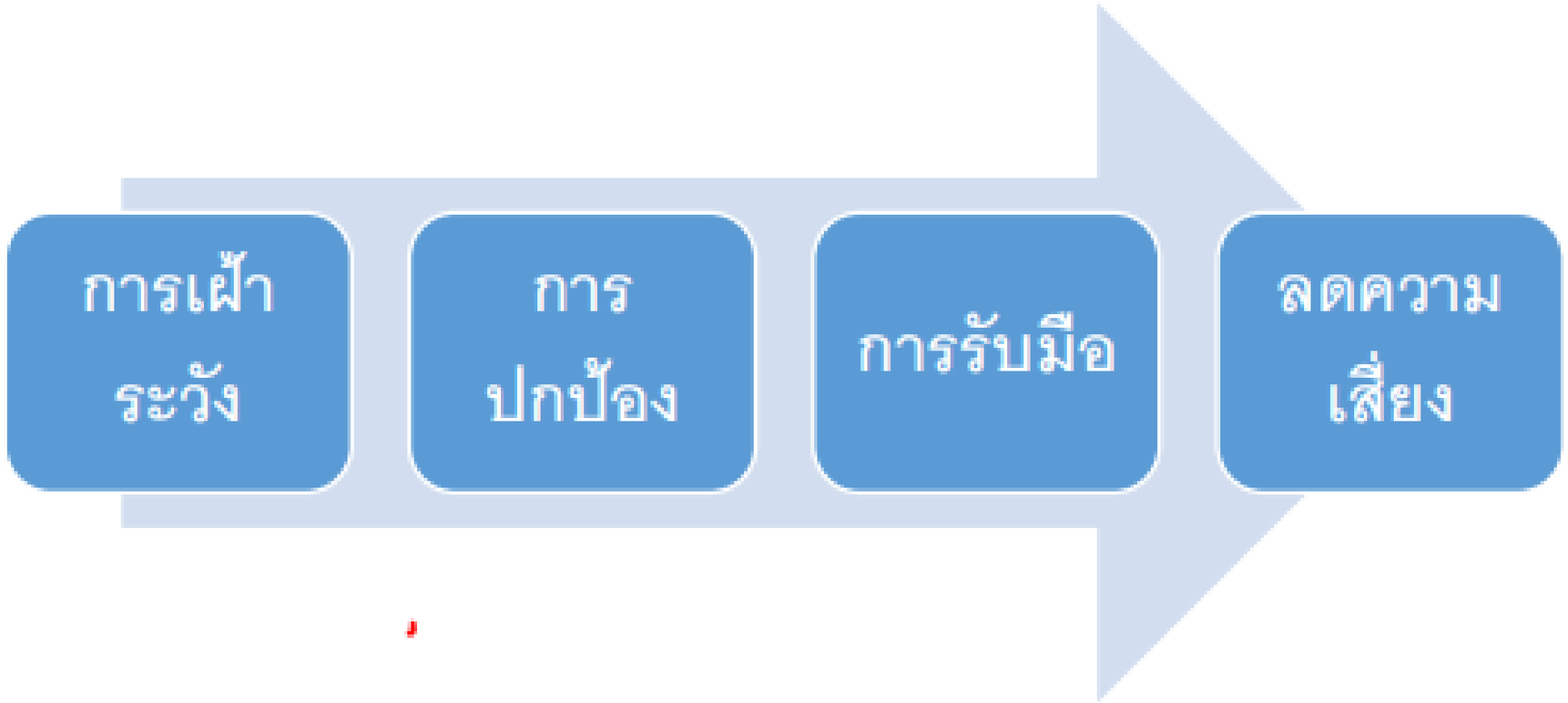
- Technical Controls
- Non-technical Controls

## NIST Framework

The US National Institute of Standards and Technology (NIST)

เป็นหน่วยงานหนึ่งของกระทรวงพาณิชย์สหรัฐ ที่สนับสนุนและรักษามาตรฐานความปลอดภัย ในหลายๆ ด้านเพื่อปกป้องระบบขององค์กร

| IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER |
|---|---|---|---|---|
| Technical controls (Vulnerability scanning, Monitoring ...) | Technical controls (Firewall, AWL, AV, IPS, DC, network segmentation, ....) | Technical controls (IPS, IDS, SIEM, Security Dashboard ...) | Technical controls (IPS, Recovery CD, ...) | Technical controls (Back-up Control Center, ...) |
| Non-technical controls (Assessments, Risk management) | Non-technical controls (Security Policies & Procedures) | Non-technical controls (Security monitoring) | Non-technical controls (Security incident response, Disconnection management) | Non-technical controls (Data recovery, Disaster recovery) |




# พรบ การรักษาความมั่นคงปลอดภัยไซเบอร์ 2562

# หน่วยงานที่เกี่ยวข้อง

**“โครงสร้างพื้นฐานสำคัญทางสารสนเทศ”**

หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

**“หน่วยงานของรัฐ”**

หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่นรัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ

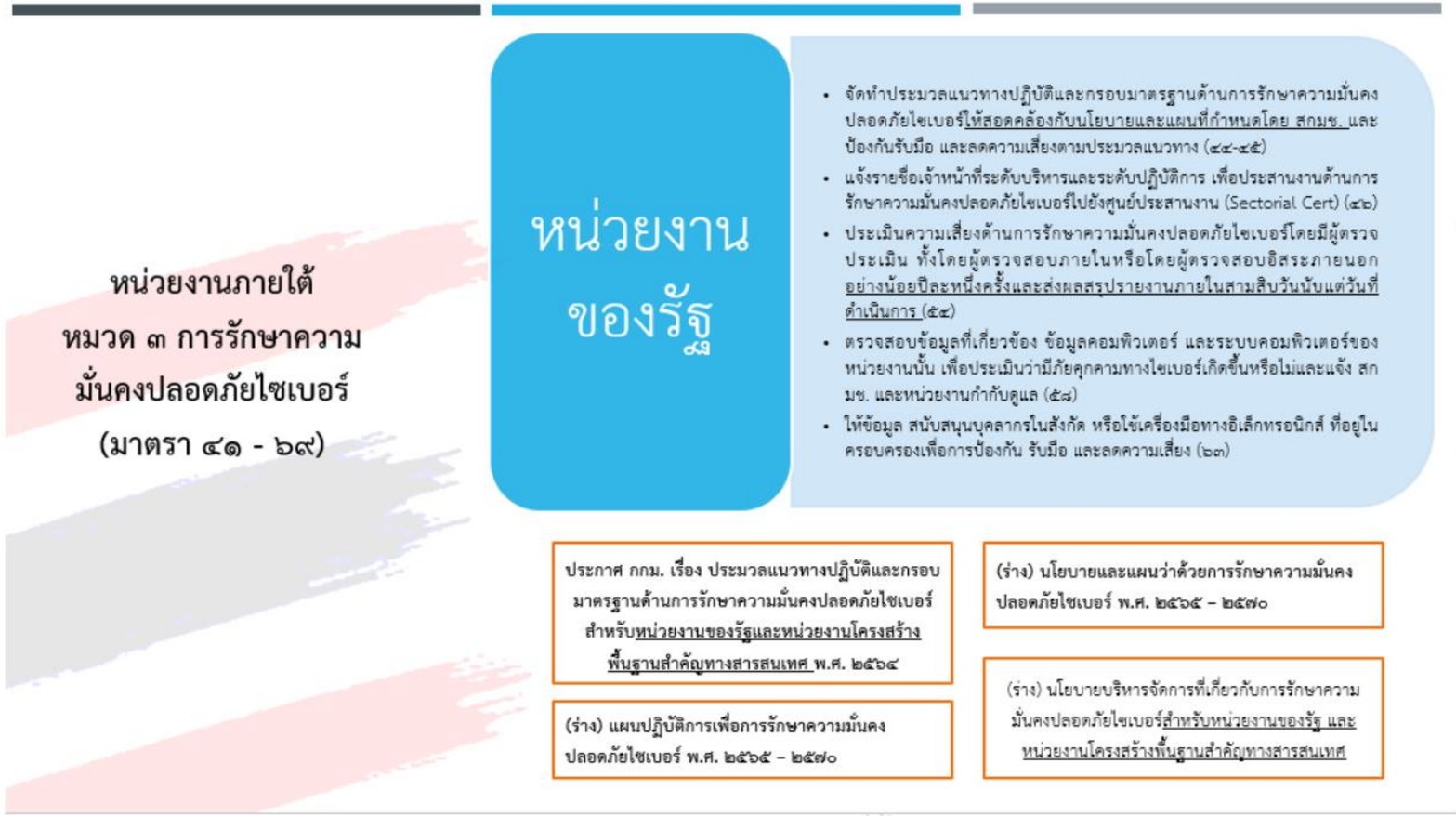
**“หน่วยงานควบคุมหรือกำกับดูแล”**

หมายความว่า หน่วยงานของรัฐ หน่วยงานเอกชน หรือบุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐ หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

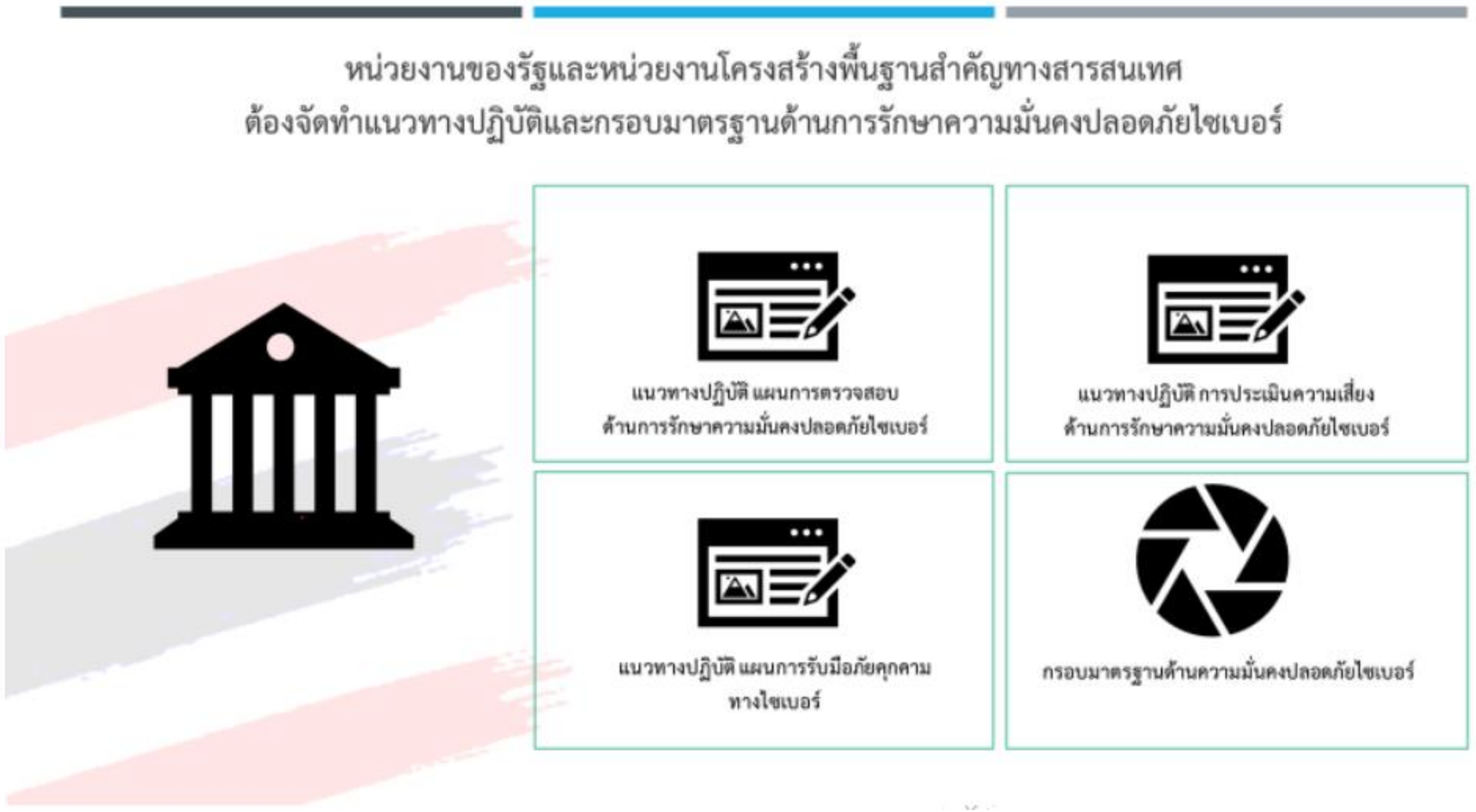
**“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ”**

หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

# หน่วยงานหมวด 3



# แนวทางปฏิบัติกรอบมาตรฐาน



# ประมวลแนวทางปฏิบัติ

# การจัดการทรัพย์สิน

# การประเมินช่องโหว่

## การประเมินช่องโหว่และการทดสอบเจาะระบบ
## (VULNERABILITY ASSESSMENT AND PENETRATION TESTING)

(Identify)

จัดทำนโยบายและแนวปฏิบัติการบริหารจัดการช่องโหว่ระบบ (VULNERABILITY MANAGEMENT PROCEDURE)

3 ต้องทำการประเมินช่องโหว่และควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญ ของหน่วยงานของรัฐ และหน่วยงาน CII

4 ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) โดยเฉพาะอย่างยิ่งระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing)

5 ขอบเขตทดสอบเจาะระบบ (Scope of a Penetration Test) ต้องครอบคลุม

การทดสอบเจาะระบบของโฮสต์

การทดสอบเจาะระบบเครือข่าย

การทดสอบเจาะระบบแอปพลิเคชัน

## การทำให้ระบบมีความแข็งแกร่ง (SYSTEM HARDENING)

(Protect)

จัดทำเอกสารมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย

1 ต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ทั้งหมดของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงาน CII ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับ

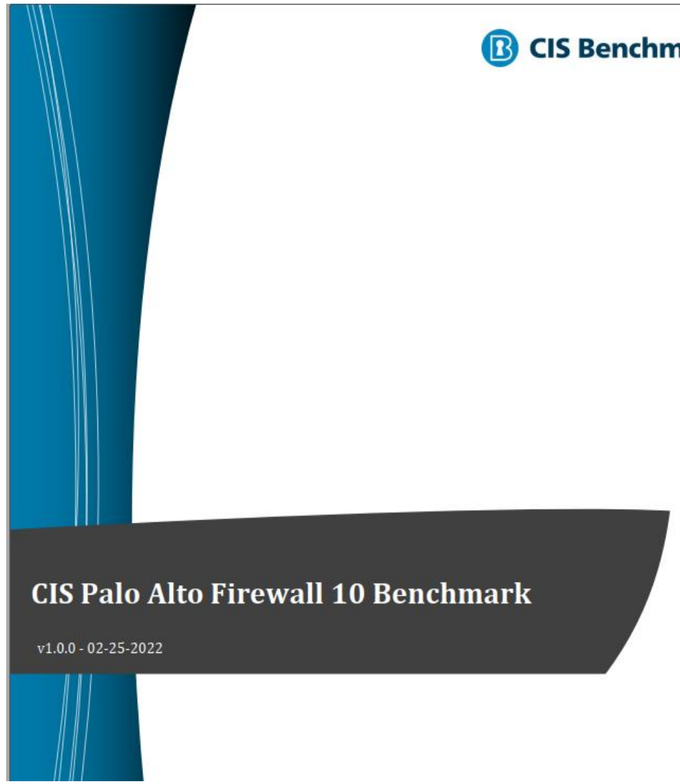
ระบบปฏิบัติการ

แอปพลิเคชัน

อุปกรณ์เครือข่าย

# Security Baseline& System Hardenging

# Security Baseline& System Hardenging




| | | | |
|---|---|---|---|
| | management profiles (Automated) | ☐ | ☐ |
| 1.2.5 | Ensure valid certificate is set for browser-based administrator interface (Automated) | ☐ | ☐ |
| **1.3** | **Minimum Password Requirements** | | |
| 1.3.1 | Ensure 'Minimum Password Complexity' is enabled (Automated) | ☐ | ☐ |
| 1.3.2 | Ensure 'Minimum Length' is greater than or equal to 12 (Automated) | ☐ | ☐ |
| 1.3.3 | Ensure 'Minimum Uppercase Letters' is greater than or equal to 1 (Automated) | ☐ | ☐ |
| 1.3.4 | Ensure 'Minimum Lowercase Letters' is greater than or equal to 1 (Automated) | ☐ | ☐ |
| 1.3.5 | Ensure 'Minimum Numeric Letters' is greater than or equal to 1 (Automated) | ☐ | ☐ |
| 1.3.6 | Ensure 'Minimum Special Characters' is greater than or equal to 1 (Automated) | ☐ | ☐ |
| 1.3.7 | Ensure 'Required Password Change Period' is less than or equal to 90 days (Automated) | ☐ | ☐ |

# แผนการรับมือภัยคุกคามทางไซเบอร์

## 2.1 แผนการรับมือภัยคุกคามทางไซเบอร์

โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

| ลำดับที่ | บทบาท | หน้าที่รับผิดชอบ | ช่องทางการติดต่อ |
|---|---|---|---|
| 1. | Help Desk | รับเรื่องและประสานงานเหตุการณ์ภัยคุกคาม | Email (helpdesk@cmu.ac.th) |
| 2. | เจ้าหน้าที่ตอบสนองต่อเหตุการณ์ภัยคุกคามระดับ 1 | วิเคราะห์เหตุการณ์ภัยคุกคามเบื้องต้น | Email (CS_Ana1@cmu.ac.th) |
| 3. | เจ้าหน้าที่ตอบสนองต่อเหตุการณ์ภัยคุกคามระดับ 2 | วิเคราะห์เหตุการณ์ภัยคุกคามขั้นสูง | Email (CS_Ana2@cmu.ac.th) |
| 4. | SOC Manager | ตัดสินใจในการดำเนินการแก้ไขปัญหาภัยคุกคาม | Email (CS_manager@cmu.ac.th) |

โครงสร้างการรายงานเหตุการณ์

| ลำดับที่ | หน้าที่รับผิดชอบ | ช่องทางการติดต่อ | ภายในเวลา |
|---|---|---|---|
| 1. | รับเรื่องและประสานงานเหตุการณ์ภัยคุกคาม | Email | 1 ชั่วโมง |
| 2. | วิเคราะห์เหตุการณ์ภัยคุกคาม | Email , MS-Team | 3 ชั่วโมง |
| 3. | ตัดสินใจในการ | Email , MS-Team,โทรศัพท์ | 3 ชั่วโมง |

# แผนฟื้นฟูความเสียหาย

2.2 แผนการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

| BCP Activity/Process by Threat | |
|---|---|
| **หมายเลขแผนงาน** | BCP 0001 |
| **เหตุการณ์** | เครื่องแม่ข่ายที่ให้บริการ WEB-SERVER ถูกโจมตีจาก Ransomware |
| **ผลกระทบ** | ระบบ Public information (PI) สำหรับให้บริการประชาชนทั่วประเทศไม่สามารถให้บริการได้ |
| **แนวทางการรับมือกับเหตุการณ์** | ตรวจสอบ Traffic ที่มีการเข้าใช้งานโปรโตคอล SMB ที่เข้าสู่ WEB-Server อย่างผิดปกติ เช่น การเข้าถึงโปรโตคอลดังกล่าวจาก Network ภายนอก |
| **สิ่งที่ต้องจัดเตรียม** | ระบบ Monitor วิเคราะห์ และแจ้งเตือน Traffic ที่วิ่งเข้าสู่ WEB-Server โดยเฉพาะการตรวจสอบการเข้าใช้งานผ่านโปรโตคอล SMB |
| **เวลาที่ต้องใช้ในการกู้คืนระบบ** | 12 ชั่วโมง |

| กระบวนการรับแจ้งเหตุการณ์ | | | | | |
|---|---|---|---|---|---|
| **ลำดับ** | **เวลาสิ้นสุดกิจกรรม (ชม.)** | **Predecessor** | **ขั้นตอนการดำเนินงาน** | **หมายเหตุ/เอกสารอ้างอิง** | **ดำเนินการโดย** |
| **Phase 1: Incident Response** | | | | | |
| 1 | T0 | ผู้ใช้งาน | รับแจ้งเหตุระบบไม่สามารถเข้าถึงได้เนื่องจากได้รับผลกระทบจาก Ransomware | **เอกสารบันทึกการแจ้งเหตุผ่านระบบ** | **Help Desk** |

# (ร่าง)แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(ร่าง)

แนวนโยบายและแนวปฏิบัติ

ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

มหาวิทยาลัยเชียงใหม่

พ.ศ. 2565

# โครงสร้าง

1. คำนิยาม
2. User Responsibilities
3. Assets Management
4. Physical & Environment Security
5. Access Control
6. Network Access Control
7. OS & Software Utilities
8. Application Access Control
9. Backup & Recovery
10. Security Incident Management
11. Compliance & Legal Requirements

# เจตนารมณ์

- หลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐพ.ศ.2549
- มาตรา 5 “ส่วนงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับส่วนงานของรัฐหรือโดยส่วนงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้”
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของส่วนงานของรัฐ พ.ศ. 2553
- ส่วนงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของส่วนงานเป็นลายลักษณ์อักษร
- ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยเชียงใหม่ เป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัยจากภัยคุกคามในทุกด้าน และสามารถดำเนินงานได้อย่างต่อเนื่อง
- เห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
- มาตรฐาน แนวปฏิบัติ ขั้นตอนปฏิบัติ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
- Standard & Guideline ***

# คำนิยามศัพท์ฯ

## ส่วนที่ 1 คำนิยามศัพท์ที่ใช้ในแนวปฏิบัติ (Definition)

คำนิยามศัพท์ที่ใช้ในแนวนโยบายแนวปฏิบัตินี้ ประกอบไปด้วย

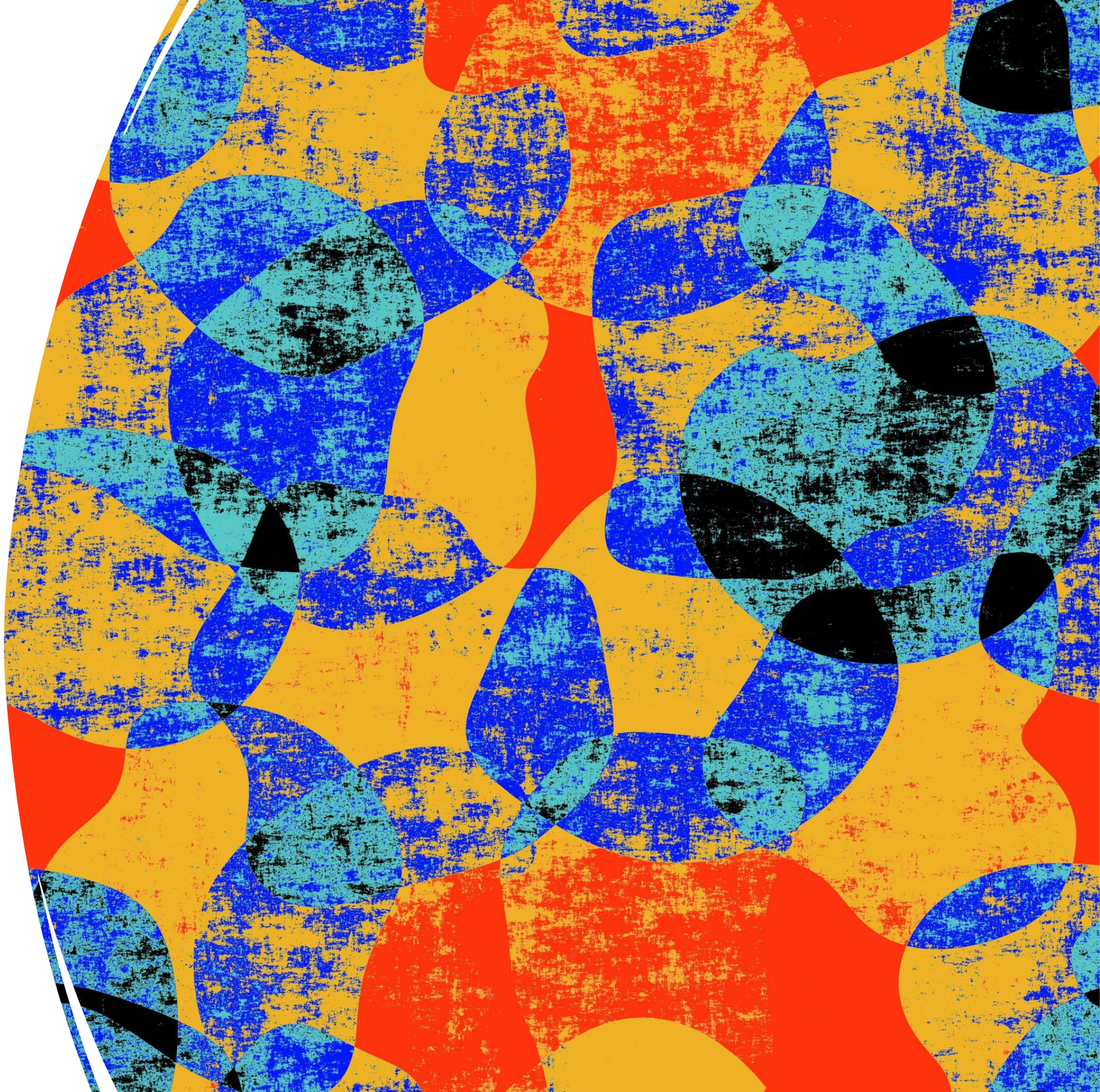
1. **มหาวิทยาลัย** หมายถึง มหาวิทยาลัยเชียงใหม่
2. **ส่วนงาน** หมายถึง ส่วนงานวิชาการ ส่วนงานอื่น ตามพระราชบัญญัติมหาวิทยาลัยเชียงใหม่ พ.ศ. 2551 มาตรา 9 การแบ่งส่วนงานมหาวิทยาลัย
3. **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่
4. **ระบบเทคโนโลยีสารสนเทศ (Information Technology System)** หมายถึง ระบบเทคโนโลยีสารสนเทศประกอบด้วยเทคโนโลยีฮาร์ดแวร์ ซอฟต์แวร์ และระบบเครือข่ายที่ส่วนงานนำมาใช้ประโยชน์ในการดำเนินงาน การวางแผนบริหาร การสนับสนุนการศึกษาและให้บริการการศึกษา และควบคุมการติดต่อสื่อสารซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ระบบเครือข่าย โปรแกรมข้อมูลและสารสนเทศ เป็นต้น
5. **ผู้ใช้งาน** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งานเข้าถึงหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยเชียงใหม่ โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (role) ของผู้ใช้งาน มีรายละเอียดดังนี้

| ลำดับ | ตำแหน่ง | บุคลากร | บทบาทหน้าที่ |
|---|---|---|---|
| 1 | ผู้ดูแลระบบ (System Administrator) | • บุคลากรที่ได้รับมอบหมายให้ดูแลระบบคอมพิวเตอร์ระดับมหาวิทยาลัย<br>• บุคลากรที่ได้รับมอบหมายให้ดูแลระบบคอมพิวเตอร์ระดับส่วนงาน | เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (CMU Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) |
| 2 | นักพัฒนาระบบสารสนเทศ (Management | • ทีมพัฒนาระบบสารสนเทศของมหาวิทยาลัย<br>• ทีมพัฒนาระบบสารสนเทศของส่วน | เป็นบุคลากรหรือองค์กรที่ได้รับมอบหมายให้พัฒนาระบบสารสนเทศของมหาวิทยาลัย หรือของส่วนงาน หรือเจ้าของข้อมูลระบบที่พัฒนา |

# 2. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน User Responsibilities

- บทบาทหน้าที่ ควบคุม ป้องกัน การเข้าถึงและเปิดเผยข้อมูล
- รับผิดชอบปกป้องรักษาข้อมูล
- มาตรการปฏิบัติงาน

1. ควบคุมทรัพย์สินและการใช้งานระบบ
2. ข้อกำหนดของผู้ดูแลระบบ
3. ข้อกำหนดการใช้ระบบสารสนเทศ + Utilities
4. ข้อกำหนดรหัสผ่าน



# 3. การบริหารจัดการทรัพย์สินสารสนเทศ Information Technology Assets Management

- บัญชีทรัพย์สิน IT
- ระเบียบหลักเกณฑ์การใช้งาน
- ผู้รับผิดชอบ
- ขั้นตอน บันทึกการใช้งาน สถานที่

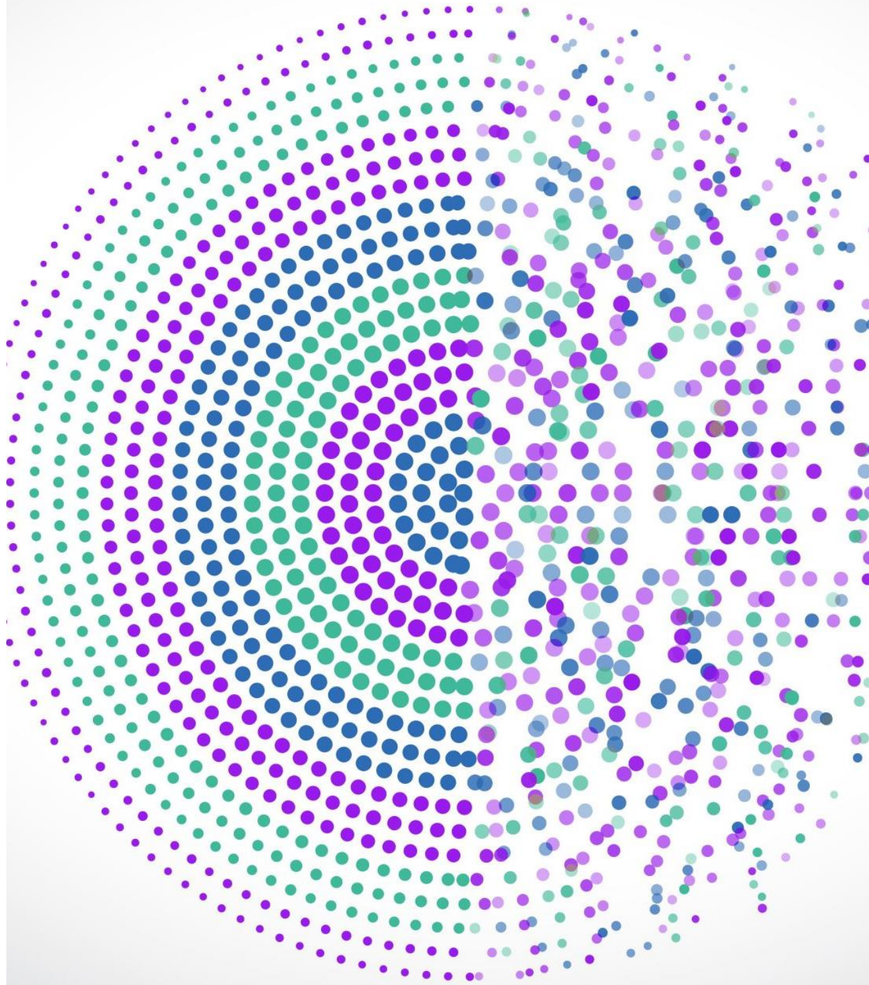
1. ความรับผิดชอบของผู้ใช้งาน
2. ผู้ใช้งานเชื่อมต่อเครือข่าย
3. ผู้ใช้งานกับอีเมล
4. Information Classification

# 5. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

Access Control for Networking, Computer System and Information System

- การระบุยืนยันตัวตน
- สิทธิ์การเข้าถึงตามระดับชั้น ความเหมาะสม
- แนวปฏิบัติชัดเจน

1. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่าย .....
2. แนวปฏิบัติ Remote Access



# 6. การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

## Network Access Control

- แนวปฏิบัติ MA Network
- ป้องกันความเสียหายต่ออุปกรณ์และข้อมูล
- ทำงานอย่างต่อเนื่อง
- ควบคุมการเข้าถึง ใช้บริการ

1. แนวปฏิบัติการควบคุมการเข้าถึงและใช้บริการ Network
2. การยืนยันตัวตนกรณีอยู่นอกเครือข่าย
3. ระบุอุปกรณ์เครือข่าย
4. ป้องกันพอร์ตแอดมิน
5. Network Segregation
6. Network Connection Control
7. Network Routing Control
8. การเชื่อมต่อเครือข่าย

# ๑. การสำรองข้อมูลและการกู้คืนข้อมูล

## Data Backup and Recovery

- ข้อปฏิบัติการสำรองและกู้คืน
- สำรองข้อมูลอย่างถูกต้อง
- กู้คืนระบบได้ในกรณีที่จำเป็น
- เพื่อให้ระบบทำงานต่อไปได้

1. แนวปฏิบัติในการ Backup
2. ข้อกำหนดการ Backup
3. แนวปฏิบัติการ Restore
4. IT Contingency Plan
5. แผน B ฉุกเฉิน

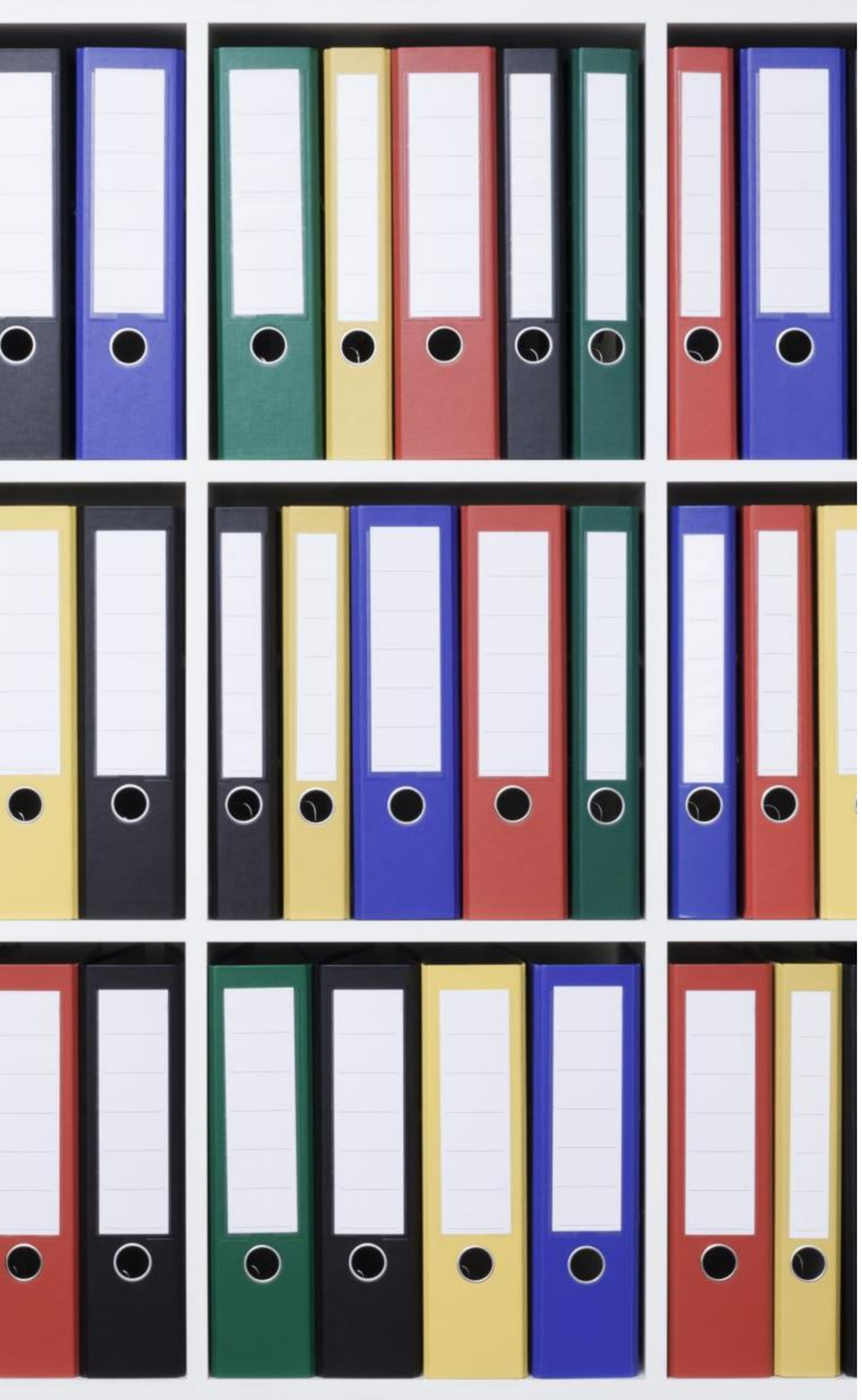
| รายการ | ข้อมูลที่ต้องสำรอง | ความถี่ในการสำรองข้อมูล |
|---|---|---|
| Mail Server | • ค่า Configuration | • ก่อนและหลังการเปลี่ยนแปลง |
| | • ข้อมูลอีเมล | • อย่างน้อย 1 สัปดาห์ |
| Web Server | • ค่า Configuration | • ก่อนและหลังการเปลี่ยนแปลง |
| | • ข้อมูลเผยแพร่บนเว็บไซต์<br>• ไฟล์ Web Application | • อย่างน้อย 1 สัปดาห์ |
| Database Server | • ค่า Configuration | • ก่อนและหลังการเปลี่ยนแปลง |
| | • ข้อมูลของระบบฐานข้อมูลของระบบที่สำคัญ | • อย่างน้อย 1 สัปดาห์ |
| Firewall Server | • ค่า Configuration | • ก่อนและหลังการเปลี่ยนแปลง |
| | • ข้อมูลกฎของ Firewall | • อย่างน้อย 1 สัปดาห์ |
| MIS Web Server | • ไฟล์ upload ข้อมูล MIS Application<br>• ไฟล์ Web Application | • อย่างน้อยเดือนละ 1 ครั้ง |
| MIS Database Server | • ค่า Configuration | • อย่างน้อยเดือนล่ะ 1 ครั้ง |
| | • Backup ฐานข้อมูล | • อย่างน้อยวันละ 1 ครั้ง |
| Server อื่นๆ เช่น ระบบงานต่างๆ | • ค่า Configuration | • ก่อนและหลังการเปลี่ยนแปลง |
| | • ข้อมูลบนเครื่องแม่ข่ายอื่นๆ | • อย่างน้อย 1 สัปดาห์ |

# 10. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์

## Information Security Incident Management

- กระบวนการรองรับเพื่อลดความรุนแรง
- วางแผนประเมินความเสี่ยง
- เตรียมความพร้อม+ขั้นตอนการปฏิบัติงาน

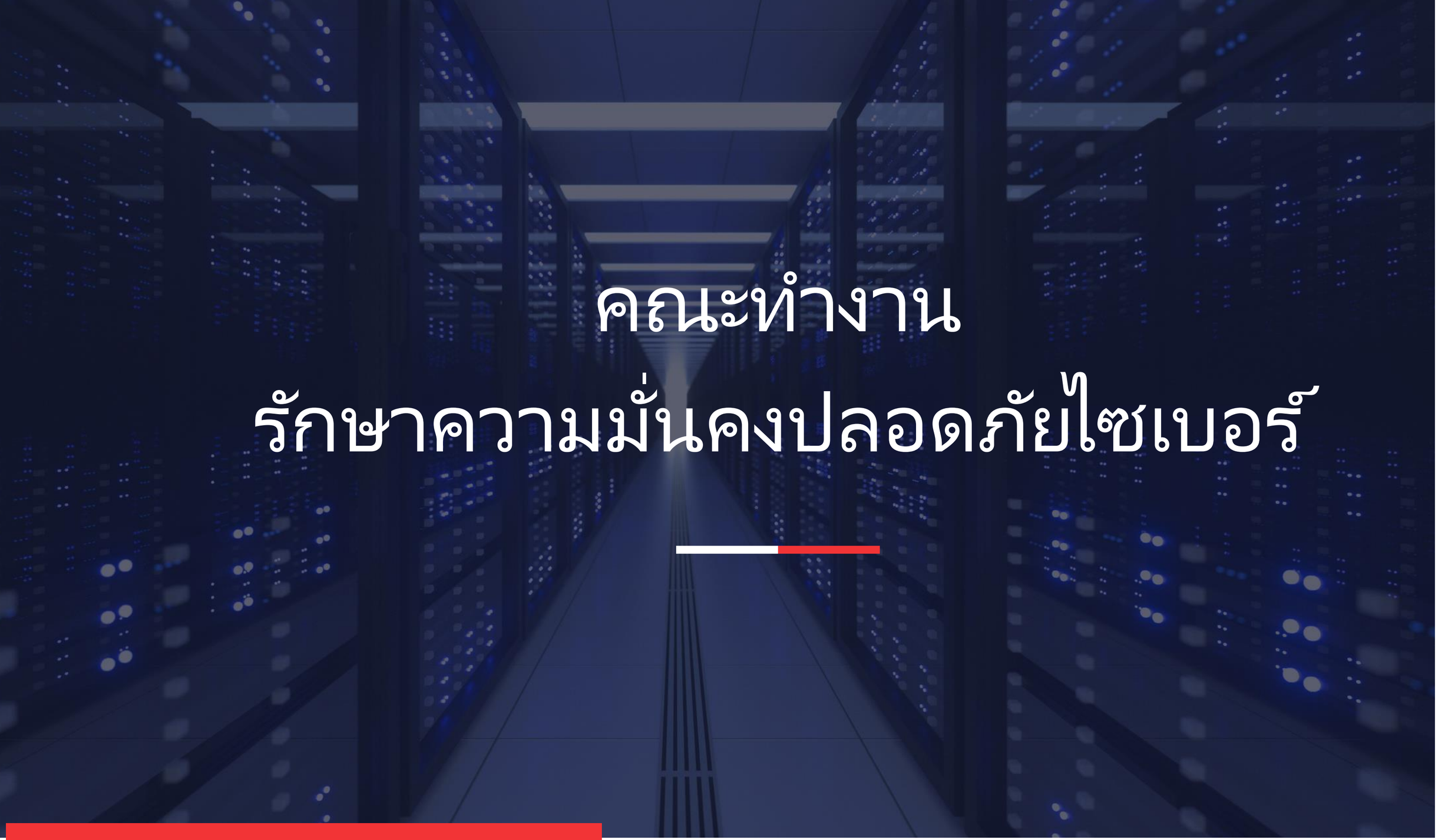
1. แนวปฏิบัติในการทำ Security Incident
2. BCP
3. บริหารความเสี่ยง ส่วนงาน มหาวิทยาลัย



## 11. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Compliance with Legal Requirements)

- ตรวจสอบ+ประเมินผล
- ส่งเสริมความรู้ความเข้าใจ
- การเตรียมความพร้อม

1. แนวปฏิบัติของผู้บริหารและเจ้าหน้าที่
2. ตรวจสอบ+ประเมินผล
3. User Awareness



# คณะทำงาน
# รักษาความมั่นคงปลอดภัยไซเบอร์

# คณะทำงานความมั่นคงปลอดภัยไซเบอร์

# (CSC: Cyber Security Center)

## มหาวิทยาลัยเชียงใหม่

ส่วนงาน สำนักบริการเทคโนโลยีสารสนเทศ

## CSC จัดตั้งขึ้นเพื่อ:

เป็นศูนย์กลางในการรับมือกับเหตุภัยคุกคามไซเบอร์ต่างๆ ที่เกิดขึ้นภายในระบบเครือข่ายของมหาวิทยาลัยเชียงใหม่ พร้อมทั้งพัฒนาคุณภาพด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่มหาวิทยาลัยและส่วนงานต่างๆ ภายในมหาวิทยาลัยเชียงใหม่

# คณะทำงานความมั่นคงปลอดภัยไซเบอร์

- งานปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์
- งานนโยบายและแผนความมั่นคงปลอดภัยทางไซเบอร์
- งานติดตามและประเมินผล

**1. บริการเชิงรับเพื่อตอบสนองภัยคุกคาม (Incident Response)**

- ตรวจสอบติดตามและรับแจ้งเหตุภัยคุกคาม
- การรับมือและแก้ไขเหตุภัยคุกคาม ณ สถานที่เกิดเหตุ (on site)
- การสนับสนุนการรับมือและแก้ไขเหตุคุกคาม
- การประสานงานเพื่อรับมือและแก้ไขเหตุภัยคุกคาม

**2. บริการเชิงรุกเพื่อป้องกันภัยคุกคาม (Protect)**

- การแจ้งเตือนและเผยแพร่ข้อมูลข่าวสาร
- ตรวจสอบช่องโหว่ของระบบ (Network / Servers / e-Mail Phishing, App data)
- สร้างความรู้ความตระหนักด้านภัยคุกคามไซเบอร์แก่ผู้ใช้งาน

**3. บริการบริหารคุณภาพทางด้านความมั่นคงปลอดภัย (Security Standard)**

- การดำเนินการตามแนวนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ
- การดำเนินการตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศอื่นๆ
- ตรวจสอบและประเมิน
- ให้คำปรึกษา
- ประสานงานด้านกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

# แผนการบริการฝ่าย CSC

| แผนงาน | ความถี่ |
|---|---|
| 1) Vulnerability Assessment หน่วยงานต่าง ๆ | 1 ครั้ง ต่อ ปี |
| 2) Penetration Testing ระบบที่มีความสำคัญ | > 1 ระบบ ต่อ ปี |
| 3) วิเคราะห์ปัญหาการถูกหลอกลวงข้อมูล e-mail phishing | 1 ครั้ง ต่อ ปี |
| 4) จัดฝึกอบรมความรู้ทางเทคนิคให้ทันสมัย (กลุ่ม IT-Admin) | 2 ครั้ง ต่อ ปี |
| 5) จัดฝึกอบรมสร้างความตระหนัก (นักศึกษา บุคลากรทั่วไป) | 2 ครั้ง ต่อ ปี |
| 6) ติดตาม ตรวจสอบประเมิน ให้คำแนะนำปรับปรุงด้านความปลอดภัยไซเบอร์ กับหน่วยงานต่างๆ | 1 ครั้งต่อปี |
| 7) สรุปผลการดำเนินงาน จัดทำรายงานประจำปี | 1 ครั้งต่อปี |
| 8) ทบทวน ปรับปรุงมาตรการความมั่นคงปลอดภัยไซเบอร์ (Review Security Policy) | 1 ครั้ง ต่อ ปี |
| 9) จำลองสถานการณ์ เพื่อแก้ไขเหตุการณ์ กู้คืนระบบ | 2 ครั้งต่อ ปี |
| 9) สรุปวิเคราะห์ข้อมูลจากเหตุการณ์ที่เกิดขึ้น | 1 ครั้ง ต่อ เดือน |
| 10) ประชาสัมพันธ์ ให้ข้อมูลข่าวสาร ผ่านทางช่องทางสื่อสารต่าง ๆ | > 1 ครั้ง ต่อ สัปดาห์ |
| 11) เตรียมพร้อมรับสถานการณ์ | ตลอดเวลา |

1

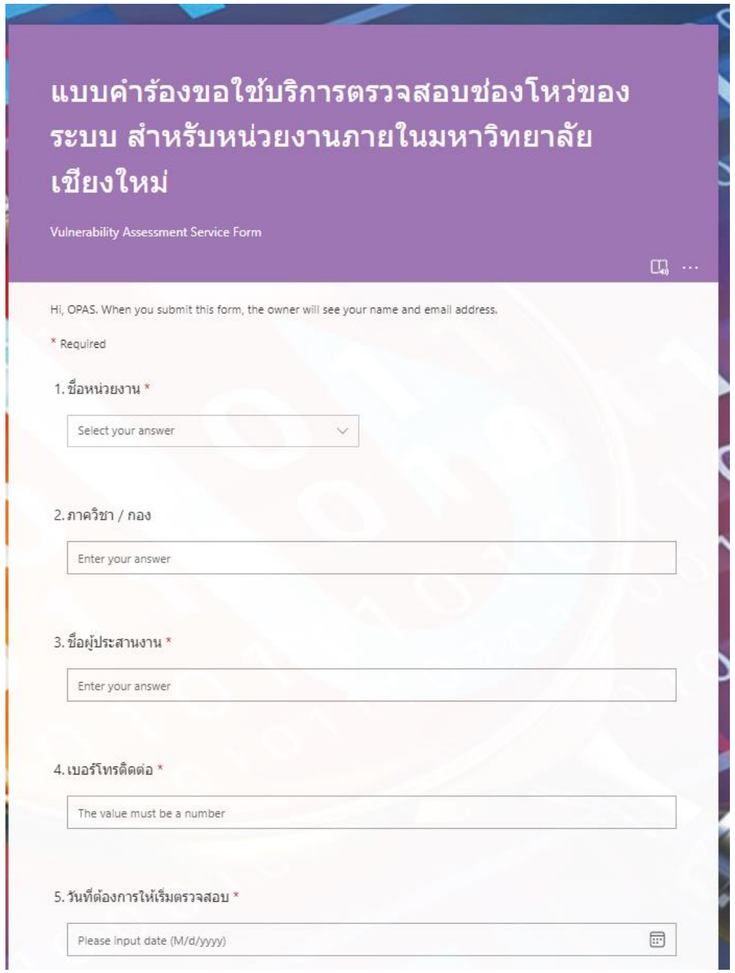
# Vulnerabilities Assessment Service

การตรวจสอบช่องโหว่ (เครือข่าย / เครื่องแม่ข่าย)


SECURITY
มีช่องโหว่ตรงไหน
ให้เราช่วยหา
ITSC CMU
Information Technology Service Center
Chiang Mai University
สอบถามข้อมูลเพิ่มเติม One Stop Service โทร. 053-943800 กด 1 หรือ https://csoc.cmu.ac.th

# เครื่องมือที่ใช้ตรวจสอบช่องโหว่

ลงทะเบียนใช้บริการ(cmu.to/vareg)



# การรายงานผลการสแกนช่องโหว่ผ่านอีเมล

FW: Nessus Scan Results: **คณะการสื่อสารมวลชน**

Translate message to: English | Never translate from: Thai

SANTI SIANGWONG

[redacted] TANCHANPONG; OPAS MUENSAEN; THOMHATHAI JINO

เรียน คุณ [redacted]

สำนักบริการเทคโนโลยีสารสนเทศมหาวิทยาลัยเชียงใหม่ ขอส่งผลรายงานประเมินผลความเสี่ยงจากช่องโหว่ของระบบเ
ของเครื่องแม่ข่ายคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย และอุปกรณ์ที่เกี่ยวข้อง เพื่อให้ท่านได้ทราบถึงความเสี่ยง หรือช่องโหว่ไ
มัลแวร์ (Malware) หรือ ไวรัส (Virus) เข้ามาโจมตีได้จึงขอรายงานการสแกนหาช่องโหว่ที่พบเจอจากการที่ท่านได้แจ้งหมายเล
มาก่อนหน้านี้ ทั้งนี้อาจจะเนื่องจากระบบที่อาจไม่ได้รับการติดตั้ง Patch อย่างเหมาะสมหรือช่องโหว่ที่เกิดจากการปรับตั้งค่าการ
ถูกโจรกรรมข้อมูล หรือการสูญเสียข้อมูลสำคัญข้อมูลรายงานการสแกนช่องโหว่ ตาม file ที่แนบมา

**โดยขอให้ท่านรีบดำเนินการหลังการ ทราบผลการ สแกนหาทั้งช่องโหว่ที่มีอยู่ในระบบโดยอาจดำเนินการดังต่อ**

**ปิดช่องโหว่ Hardening**
**1.Update Services Pack and Patch**
**2.Upgrade Programs**
**3.Update Configure**
**4.Disable Unused Services**

ด้วยความเคารพอย่างสูง
สำนักบริการเทคโนโลยีสารสนเทศมหาวิทยาลัยเชียงใหม่

**From:** Nessus Server [mailto:no-reply-nessus@cmu.ac.th]
**Sent:** Monday, April 25, 2022 1:23 AM
**To:** OPAS MUENSAEN <opas.m@cmu.ac.th>; SANTI SIANGWONG <santi.s@cmu.ac.th>
**Subject:** Nessus Scan Results: คณะการสื่อสารมวลชน

1

## Nessus Scan Report

Mon, 25 Apr 2022 01:22:37 SE Asia Standard Time

Nessus completed the scan **คณะ** [redacted] Please click here to view and edit the scan results.

**Report Summary**

**Plugins: Top 5**

| Severity | Plugin Id | Name |
|---|---|---|
| Critical | 158900 | Apache 2.4.x < 2.4.53 Multiple Vulnerabilities |
| Critical | 153583 | Apache < 2.4.49 Multiple Vulnerabilities |
| Critical | 153584 | Apache < 2.4.49 Multiple Vulnerabilities |
| Critical | 56997 | VMware ESX / ESXi Unsupported Version Detection |
| Critical | 57603 | Apache 2.2.x < 2.2.13 APR apr_palloc Heap Overflow |

**Hosts: Top 5**

| Host | Critical | High | Medium | Low | Info | Total |
|---|---|---|---|---|---|---|
| 202.28.[redacted] | 11 | 19 | 45 | 1 | 63 | 139 |
| 202.28.[redacted] | 6 | 2 | 11 | 0 | 94 | 113 |
| 202.28.[redacted] | 1 | 5 | 9 | 0 | 48 | 63 |
| 202.28.[redacted] | 1 | 2 | 19 | 1 | 81 | 104 |
| 202.28.[redacted] | 0 | 1 | 7 | 0 | 65 | 73 |

**Suggested Remediations (TOP 10)**

**Taking the following actions across 3 hosts would resolve 76% of the vulnerabilities on the network:**

| Action to take | Vulns | Hosts |
|---|---|---|
| Apache 2.4.x < 2.4.53 Multiple Vulnerabilities: Upgrade to Apache version 2.4.53 or later | 110 | 2 |

# วิเคราะห์ผล

- หลังจากการตรวจสอบช่องโหว่ครบทุกส่วนงานแล้วจะทำการวิเคราะห์และประเมินหาช่องโหว่ที่มีความร้ายแรงเสี่ยงสูงและหาแนวทางแก้ไขปัญหาร่วมกัน
- และหลังจากการแก้ไขปัญหาแล้วควรมีการสแกนช่องโหว่อีกครั้งเพื่อพิสูจน์ว่าช่องโหว่ได้รับการแก้ไขแล้ว
- ควรมีการวางแผนเพื่อให้ความรู้แก่ผู้ดูแลระบบไอทีของส่วนงานเป็นประจำอย่างต่อเนื่องสม่ำเสมอตลอดปี

# Vulnerability Report

- 41 หน่วยงาน อาสารับการประเมิน VA

| ชื่อหน่วยงาน |
|---|
| สำนักบริการเทคโนโลยีสารสนเทศ |
| คณะวิจิตรศิลป์ |
| คณะวิศวกรรมศาสตร์ |
| คณะบริหารธุรกิจ |
| คณะวิทยาศาสตร์ |
| คณะรัฐศาสตร์และรัฐประศาสนศาสตร์ |
| สำนักพัฒนาคุณภาพการศึกษา |
| คณะวิทยาศาสตร์ |
| สำนักงานมหาวิทยาลัย |
| บัณฑิตวิทยาลัย |
| คณะสถาปัตยกรรมศาสตร์ |
| สำนักงานมหาวิทยาลัย |
| สำนักหอสมุด |
| สำนักส่งเสริมศิลปวัฒนธรรม |
| สำนักงานมหาวิทยาลัย |
| สถาบันวิจัยวิทยาศาสตร์และเทคโนโลยี |
| คณะสัตวแพทยศาสตร์ |
| สำนักงานมหาวิทยาลัย |
| วิทยาลัยศิลปะ สื่อ และเทคโนโลยี |
| อุทยานวิทยาศาสตร์และเทคโนโลยี |
| คณะเภสัชศาสตร์ |
| สถาบันวิจัยวิทยาศาสตร์สุขภาพ |
| คณะนิติศาสตร์ |
| วิทยาลัยนานาชาตินวัตกรรมดิจิทัล |
| คณะสาธารณสุขศาสตร์ |
| คณะพยาบาลศาสตร์ |
| คณะการสื่อสารมวลชน |
| คณะอุตสาหกรรมเกษตร |
| คณะเศรษฐศาสตร์ |
| สำนักงานมหาวิทยาลัย |
| คณะมนุษยศาสตร์ |
| สำนักทะเบียนและประมวลผล |
| บัณฑิตวิทยาลัย |
| สำนักงานมหาวิทยาลัย |
| คณะทันตแพทยศาสตร์ |
| คณะแพทยศาสตร์ |
| ศูนย์แก้ไขความพิการบนใบหน้าและกะโหลกศรีษะ มูลนิธิเทคโนโลยีสารสนเทศ ตามพระราชดำริฯ มช. |
| สถาบันภาษา |
| คณะการสื่อสารมวลชน |

| 0 | 0 | 3 | 0 | 32 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

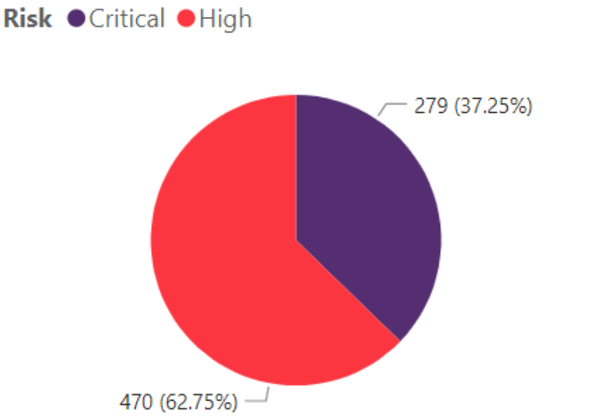
Vulnerabilities Total: 35

| SEVERITY | CVSS V3.0 | PLUGIN | NAME |
|---|---|---|---|
| MEDIUM | 6.5 | 51192 | SSL Certificate Cannot Be Trusted |
| MEDIUM | 6.5 | 157288 | TLS Version 1.1 Protocol Deprecated |
| MEDIUM | N/A | 57582 | SSL Self-Signed Certificate |
| INFO | N/A | 46180 | Additional DNS Hostnames |
| INFO | N/A | 45590 | Common Platform Enumeration (CPE) |
| INFO | N/A | 54615 | Device Type |
| INFO | N/A | 84502 | HSTS Missing From HTTPS Server |
| INFO | N/A | 10107 | HTTP Server Type and Version |
| INFO | N/A | 24260 | HyperText Transfer Protocol (HTTP) Information |
| INFO | N/A | 11219 | Nessus SYN scanner |
| INFO | N/A | 19506 | Nessus Scan Information |
| INFO | N/A | 11936 | OS Identification |
| INFO | N/A | 31422 | Reverse NAT/Intercepting Proxy Detection |
| INFO | N/A | 56984 | SSL / TLS Versions Supported |
| INFO | N/A | 83298 | SSL Certificate Chain Contains Certificates Expiring Soon |
| INFO | N/A | 56472 | SSL Certificate Chain Contains Unnecessary Certificates |
| INFO | N/A | 56471 | SSL Certificate Chain Not Sorted |
| INFO | N/A | 42981 | SSL Certificate Expiry - Future Expiry |

# วิเคราะห์แนวโน้มความเสี่ยงของระบบภาพรวมทั้งมหาวิทยาลัย

## Vulnerability

### Count of Risk by Risk

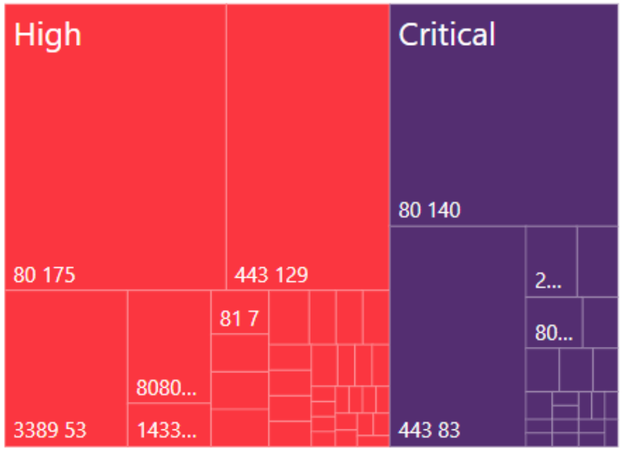



### Count of Risk

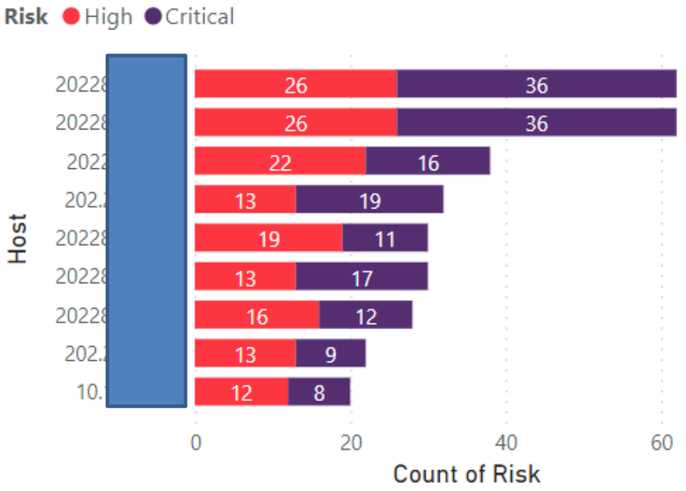

### Risk Ratio by Faculty


### Risk Ratio by Server


### Count of Risk by Risk and Port




### Count of Risk by Host and Risk




| Host | Risk | Port | Name | OrgName |
|---|---|---|---|---|
| 202 | Critical | 25 | SSL Version 2 and 3 Protocol Detection | |
| 202 | High | 25 | SSL Medium Strength Cipher Suites Supported (SWEET32) | |
| 202 | High | 443 | SSL Medium Strength Cipher Suites Supported (SWEET32) | |
| 202 | Critical | 444 | VMware ESX / ESXi Unsupported Version Detection | |
| 202 | High | 0 | ESXi 6.0 < Build 5485776 Multiple Vulnerabilities (VMSA-2017-0015) (remote check) | |
| 202 | High | 0 | ESXi 6.0 U1 < Build 5251621 / 6.0 U2 < Build 5251623 / 6.0 U3 < Build 5224934 Multiple Vulnerabilities (VMSA-2017-0006) (remote check) | |
| 202 | High | 444 | ESXi 5.5 / 6.0 / 6.5 / Multiple Vulnerabilities | |

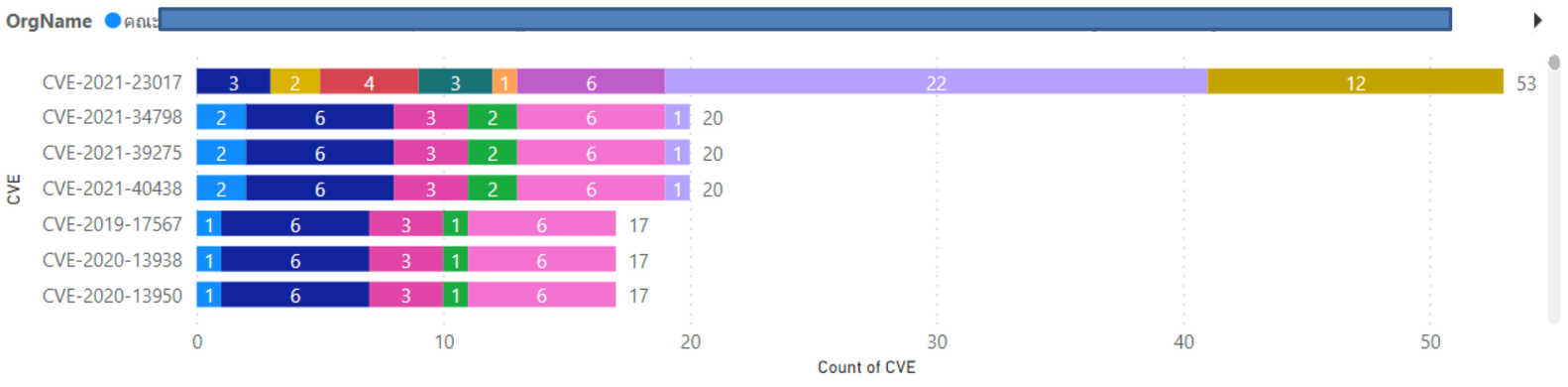
Total

# จัดเรียงตามปริมาณระบบที่ได้รับผลกระทบในความเสี่ยงสูงสุด

## CVE

Name

Search




| CVE | Count of CVE | Risk | Host | OrgName | Name |
|---|---|---|---|---|---|
| CVE-2022-23943 | 1 | Critical | 202282 | | Apache 2.4.x < 2.4.53 Multiple Vulnerabilities |
| CVE-2022-23943 | 1 | Critical | 202282 | | Apache 2.4.x < 2.4.53 Multiple Vulnerabilities |
| CVE-2022-22721 | 1 | Critical | 202282 | | Apache 2.4.x < 2.4.53 Multiple Vulnerabilities |
| CVE-2022-22721 | 1 | Critical | 202282 | | Apache 2.4.x < 2.4.53 Multiple Vulnerabilities |
| CVE-2022-22720 | 1 | Critical | 202282 | | Apache 2.4.x < 2.4.53 Multiple Vulnerabilities |
| CVE-2022-22720 | 1 | Critical | 202282 | | Apache 2.4.x < 2.4.53 Multiple Vulnerabilities |
| CVE-2022-22719 | 1 | Critical | 202282 | | Apache 2.4.x < 2.4.53 Multiple Vulnerabilities |
| CVE-2022-22719 | 1 | Critical | 202282 | | Apache 2.4.x < 2.4.53 Multiple Vulnerabilities |
| CVE-2021-44790 | 1 | Critical | 202.28. | | Apache 2.4.x < 2.4.52 Multiple Vulnerabilities |
| CVE-2021-44790 | 1 | Critical | 202282 | | Apache 2.4.x < 2.4.52 Multiple Vulnerabilities |
| CVE-2021-44790 | 2 | Critical | 202282 | | Apache 2.4.x < 2.4.52 Multiple Vulnerabilities |
| **Total** | **639** | | | | |

# Cyber-Security is much more than a matter of IT

*Stephane Nappo*

# Thank You