



Kaspersky Industrial  
Cybersecurity  
Conference 2024

# Cybersecurity Policies and Regulations for Operational Technology (OT) in Thailand



kaspersky



Kaspersky Industrial  
Cybersecurity  
Conference 2024

# Chalermchai Wonggate

Director of Critical Information Infrastructure  
Management Office  
Thailand National Cyber Security Agency

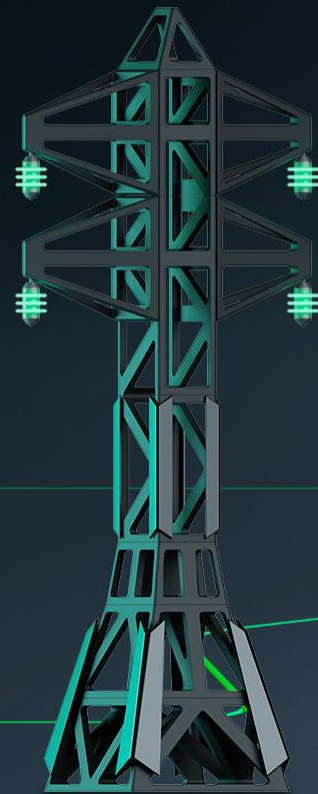
kaspersky

# Operational Technology does matter

We work with OT every day, but we never realize that it has started to change.



OT is indispensable to the functioning of critical infrastructure systems that support the daily operations of industries vital to the economy and society



# Three key aspects

of Operational Technology  
in Thailand

Cybersecurity Policies and Laws  
in Thailand

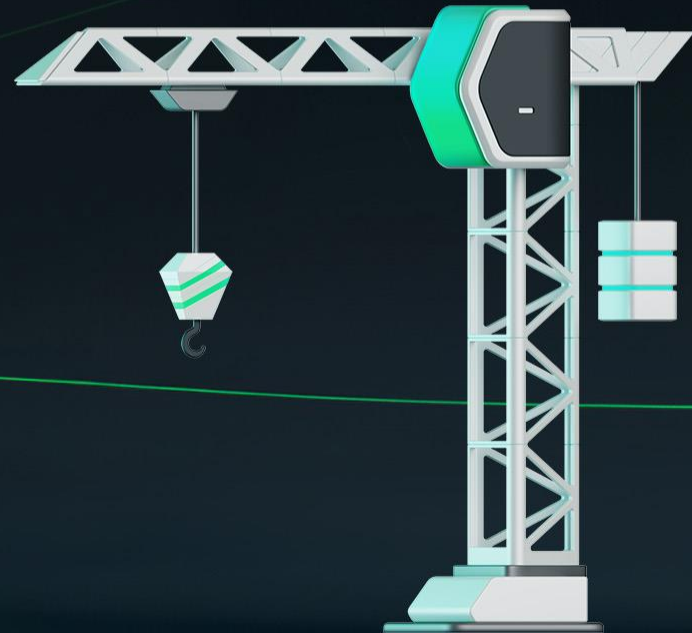
Impact of Policies and Laws on  
Operational Technology

Recommendations for Thai  
Government Agencies operating  
in Operational Technology



Thailand has seen an increased reliance on OT in critical sectors to enhance operational efficiency

improve safety, and ensure the continuity of services. However, this also brings challenges, particularly in terms of cybersecurity





(Unofficial Translation)

No. 136 Chapter 69 Kor Government Gazette 27 May 2019

[Official Emblem of Royal Command]

Cybersecurity Act,  
B.E. 2562 (2019)

His Majesty King Phra Poramenthra Ramathibodi Sisin Maha Vajiralongkorn  
Phra Vajira Klao Chao Yu Hua

Given on the 24<sup>th</sup> Day of May B.E. 2562:  
Being the 4<sup>th</sup> Year of the Present Reign.

His Majesty King Phra Poramenthra Ramathibodi Sisin Maha Vajiralongkorn Phra Vajira  
Klao Chao Yu Hua is graciously pleased to proclaim that:  
Whereas it is expedient to have an enabling act on the law concerning cybersecurity.



## Cyber Security Policy and Action Plan 2022 - 2027



Notification of the Cybersecurity Regulating Committee  
Re: Codes of Practice and Standard Frameworks  
for Government Agencies and Organizations of Critical Information Infrastructure  
B.E. 2564 (2021)

Whereas it is deemed appropriate to establish Codes of Practice and Cybersecurity  
Standard Frameworks as minimum cybersecurity requirements for Government Agencies and

หน้า ๕  
เล่ม ๑๔๑ ตอนพิเศษ ๑๘ ง ราชกิจจานุเบกษา ๑๘ มกราคม ๒๕๖๗

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ  
เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์  
ให้แก่ข้อมูลหรือระบบสารสนเทศ  
พ.ศ. ๒๕๖๖

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้  
คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีหน้าที่และอำนาจสร้างมาตรฐานเกี่ยวกับ  
การรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์

หน้า ๙  
เล่ม ๑๔๑ ตอนพิเศษ ๑๘ ง ราชกิจจานุเบกษา ๑๘ มกราคม ๒๕๖๗

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ  
เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ  
พ.ศ. ๒๕๖๖

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการ  
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีหน้าที่และอำนาจสร้างมาตรฐานเกี่ยวกับการรักษา  
ความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์  
หรือโปรแกรมคอมพิวเตอร์ จึงสมควรกำหนดมาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ เพื่อให้  
การปฏิบัติงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ



Cyber Security Policy and Action Plan 2022 - 2027

Cybersecurity Management Policy for Government Agency and Critical Information Infrastructure Organization.

Nonetheless, if the information technology risk regulatory structure is combined with companies in the same business group or related companies, roles and responsibilities of the regulatory structure are consistent with the Three Lines of Defense.

1. Good Governance in Cybersecurity

1.1 Organizational structure of the cybersecurity management should have checked and balanced with clear authorities, roles, and responsibilities in line with effective Three Lines of Defense (control, regulate, and audit) with independent regulator and auditor who can perform effectively. Therefore, roles and responsibilities must be clearly identified, both agencies, or those who create risks and control risks at the first level (Business Unit or First Line of Defense). They shall tend and operate according to guidelines with appropriate internal control and risk management. Internal agency or regulator (Second Line of Defense) i.e., risk management, compliance, and internal audit (Third Line of Defense) to promote appropriate audit and check and balance mechanisms. The Government Agency and Organization of Critical Information Infrastructure shall practice and be in line with current related laws and regulations including related guidelines issued by Supervising and Regulating Organization subsequently and will become effective for Government Agency and Organization of Critical Information Infrastructure.

guidelines, Cyber Threats handling as well as monitoring to ensure the practice accordingly.

2) There are security specifications and IT security architecture.

3) Risk management for information technology security and Cyber Threats according to the organizational risks and submit to the committee as regular agenda.

4) Manage the agency to be prepared for handling Cyber Threats.

5) Manage to provide knowledge and awareness of information technology security and Cyber Threats to organizational personnel.

3) Risk management for information technology security and Cyber Threats according to the organizational risks and submit to the committee as regular agenda.





21.3 Vulnerability Assessment and Penetration Testing  
21.3.1 Vulnerability assessment for Critical Services of Government Agencies and

Organizational  
risk management

21.3 Vulnerability Assessment and Penetration Testing  
21.3.1 Vulnerability assessment for Critical Services of Government Agencies and Organizations of Critical Information Infrastructure shall be undertaken in accordance with their risk management principles. The assessment aims to identify vulnerabilities in cybersecurity and control of all Critical Services of Government Agencies and Organizations of Critical Information Infrastructure which includes:

- (a) Information Technology (IT) system;
- (b) Industrial Control System (ICS).

and control  
Information

shall ensure

Organizational  
vulnerabilities in cybersecurity before testing any new systems that will be connected to the  
Critical Services, or before implementing any changes of systems that are vital to the Critical  
Services. The changes include the addition of new application modules, system updates, and  
technological modifications.



หน้า ๕  
เล่ม ๑๔๑ ตอนพิเศษ ๑๘ ง ราชกิจจานุเบกษา ๑๘ มกราคม ๒๕๖๗

## ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์  
ให้แก่ข้อมูลหรือระบบสารสนเทศ  
พ.ศ. ๒๕๖๖

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีหน้าที่และอำนาจสร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือโปรแกรมคอมพิวเตอร์ จึงสมควรมีมาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ เพื่อประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นแก่ข้อมูลหรือระบบสารสนเทศอันจะนำไปสู่การเลือกมาตรการในการควบคุมความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม เพื่อให้การดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๙ (๕) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในคราวการประชุมครั้งที่ ๔/๒๕๖๖ เมื่อวันที่ ๒๘ พฤศจิกายน ๒๕๖๖ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ ดังต่อไปนี้

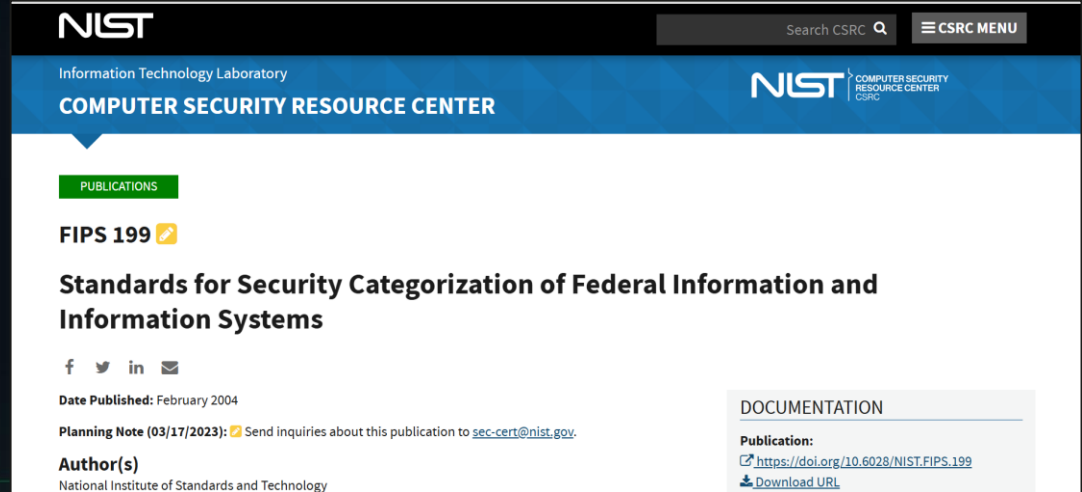
ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“ประเภทข้อมูล” หมายความว่า หมวดข้อมูลที่ถูกกำหนดขึ้นโดยหน่วยงานตามแนวทางที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติประกาศกำหนด

“ระบบสารสนเทศ” หมายความว่า ระบบหรือชุดทรัพยากรด้านสารสนเทศที่ถูกใช้สำหรับการเก็บรวบรวม การประมวลผล การบำรุงรักษา การให้ การเผยแพร่ หรือการทำลายข้อมูล



NIST  
Information Technology Laboratory  
COMPUTER SECURITY RESOURCE CENTER

Search CSRC CSRC MENU

NIST COMPUTER SECURITY RESOURCE CENTER CSRC


PUBLICATIONS

### FIPS 199

## Standards for Security Categorization of Federal Information and Information Systems

[f](#) [t](#) [in](#) [e](#)

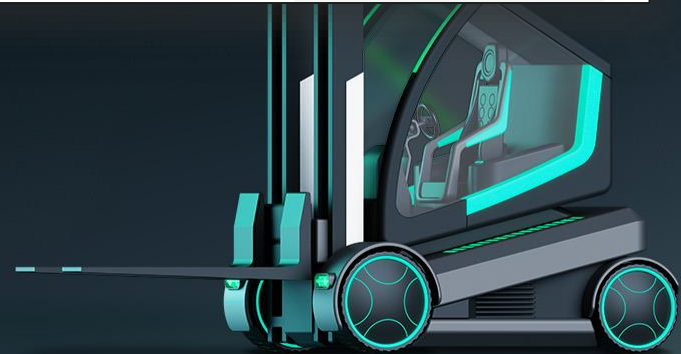
Date Published: February 2004

Planning Note (03/17/2023):  Send inquiries about this publication to [sec-cent@nist.gov](mailto:sec-cent@nist.gov).

Author(s)  
National Institute of Standards and Technology

DOCUMENTATION

Publication:  
<https://doi.org/10.6028/NIST.FIPS.199>  
[Download URL](#)



หน้า ๔  
เล่ม ๑๔๑ ตอนพิเศษ ๑๘ ง ราชกิจจานุเบกษา ๑๘ มกราคม ๒๕๖๒

## ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีหน้าที่และอำนาจสร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือโปรแกรมคอมพิวเตอร์ จึงสมควรกำหนดมาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ เพื่อให้การปฏิบัติงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๔ (๔) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในคราวการประชุมครั้งที่ ๔/๒๕๖๖ เมื่อวันที่ ๒๘ พฤศจิกายน ๒๕๖๖ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“หน่วยงาน” หมายความว่า หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

“มาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการที่กำหนดขึ้นเพื่อดำเนินการรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) สำหรับข้อมูลหรือระบบสารสนเทศ

“ประกาศประมวลแนวทางปฏิบัติและกรอบมาตรฐาน” หมายความว่า ประกาศคณะกรรมการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ข้อ ๔ ภายหลังจากหน่วยงานได้กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูล

NIST Information Technology Laboratory  
COMPUTER SECURITY RESOURCE CENTER

Search CSRC Q CSRC MENU

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

PUBLICATIONS

## FIPS 200

### Minimum Security Requirements for Federal Information and Information Systems

f t in e

Date Published: March 2006

Supersedes: [SP 800-26 \(11/01/2001\)](#)

Planning Note (03/17/2023): [Send inquiries about this publication to sec-cert@nist.gov.](#)

DOCUMENTATION

Publication:  
<https://doi.org/10.6028/NIST.FIPS.200>  
[Download URL](#)



## FIPS PUB 200

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

### Minimum Security Requirements for Federal Information and Information Systems

Computer Security Division  
Information Technology Laboratory  
National Institute of Standards and Technology  
Gaithersburg, MD 20899-8930

March 2006



U.S. DEPARTMENT OF COMMERCE  
Carlos M. Gutierrez, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY  
William Jeffrey, Director

## 4 SECURITY CONTROL SELECTION

Organizations must meet the minimum security requirements in this standard by selecting the appropriate security controls and assurance requirements as described in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*.<sup>5</sup> The process of selecting the appropriate security controls and assurance requirements for organizational information systems to achieve *adequate security*<sup>6</sup> is a multifaceted, risk-based activity involving management and operational personnel within the organization. Security categorization of federal information and information systems, as required by FIPS Publication 199, is the first step in the risk management process.<sup>7</sup> Subsequent to the security categorization process, organizations must select an appropriate set of security controls for their information systems that satisfy the minimum security requirements set forth in this standard. The selected set of security controls must include one of three, appropriately tailored<sup>8</sup> security control baselines from NIST Special Publication 800-53 that are associated with the designated impact levels of the organizational information systems as determined during the security categorization process.

- For *low-impact* information systems, organizations must, as a minimum, employ appropriately tailored security controls from the low baseline of security controls defined in NIST Special Publication 800-53 and must ensure that the minimum assurance requirements associated with the low baseline are satisfied.
- For *moderate-impact* information systems, organizations must, as a minimum, employ appropriately tailored security controls from the moderate baseline of security controls defined in NIST Special Publication 800-53 and must ensure that the minimum assurance requirements associated with the moderate baseline are satisfied.
- For *high-impact* information systems, organizations must, as a minimum, employ appropriately tailored security controls from the high baseline of security controls defined in NIST Special Publication 800-53 and must ensure that the minimum assurance requirements associated with the high baseline are satisfied.

Organizations must employ all security controls in the respective security control baselines unless specific exceptions are allowed based on the tailoring guidance provided in NIST Special Publication 800-53.





## 4 SECURITY CONTROL SELECTION

Organizations must meet the minimum security requirements in this standard by selecting the appropriate security controls and assurance requirements as described in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*.<sup>5</sup> The process of selecting the appropriate security controls and assurance requirements for organizational information systems to achieve *adequate security*<sup>6</sup> is a multifaceted, risk-based activity involving management and operational personnel within the organization. Security categorization of federal information and information systems, as required by FIPS Publication 199, is the first step in the risk management process.<sup>7</sup> Subsequent to the security categorization process, organizations must select an appropriate set of security controls for their information systems that satisfy the minimum security requirements set forth in this standard. The selected set of security controls must include one of three, appropriately tailored<sup>8</sup> security control baselines from NIST Special Publication 800-53 that are associated with the designated impact levels of the organizational information systems as determined during the security categorization process.

- For *low-impact* information systems, organizations must, as a minimum, employ appropriately tailored security controls from the low baseline of security controls defined in NIST Special Publication 800-53 and must ensure that the minimum assurance requirements associated with the low baseline are satisfied.
- For *moderate-impact* information systems, organizations must, as a minimum, employ appropriately tailored security controls from the moderate baseline of security controls defined in NIST Special Publication 800-53 and must ensure that the minimum assurance requirements associated with the moderate baseline are satisfied.
- For *high-impact* information systems, organizations must, as a minimum, employ appropriately tailored security controls from the high baseline of security controls defined in NIST Special Publication 800-53 and must ensure that the minimum assurance requirements associated with the high baseline are satisfied.

Organizations must employ all security controls in the respective security control baselines unless specific exceptions are allowed based on the tailoring guidance provided in NIST Special Publication 800-53.

หัวข้อในการกำหนด มาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ สำหรับข้อมูลหรือระบบสารสนเทศ	ระดับคุณลักษณะ ความมั่นคงปลอดภัยไซเบอร์ ของข้อมูลหรือระบบสารสนเทศ		
	ต่ำ	กลาง	สูง
<b>ประมวลแนวทางปฏิบัติ</b>			
องค์ประกอบที่ ๑ แผนการตรวจสอบด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ (Cybersecurity Audit Plan)		•	
องค์ประกอบที่ ๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment)	•	•	•
องค์ประกอบที่ ๓ แผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)	•	•	•
<b>กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์</b>			
<b>๑. การประเมินความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)</b>			
๑.๑ การจัดการทรัพย์สิน (Asset Management)	•	•	•
๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)	•	•	•
๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)			
๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)			•
<b>๒. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)</b>			
๒.๑ การควบคุมการเข้าถึง (Access Control)	•	•	•
๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)	•	•	•
๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)		•	•
๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)		•	•
๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)	•	•	•
๒.๖ การแบ่งปันข้อมูล (Information Sharing)			
<b>๓. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)</b>			
๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)	•	•	

หัวข้อในการกำหนด มาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ สำหรับข้อมูลหรือระบบสารสนเทศ	ระดับคุณลักษณะ ความมั่นคงปลอดภัยไซเบอร์ ของข้อมูลหรือระบบสารสนเทศ		
	ต่ำ	กลาง	สูง
<b>๔. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)</b>			
๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)	•	•	•
๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)	•	•	•
๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)	•	•	•
<b>๕. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)</b>			
๕.๑ การรักษาระดับความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)			•



- Adopting a risk-based approach
  - Identifying critical assets and vulnerabilities within OT environments
  - Prioritize protection where it matters most
  - Conducting regular risk assessments, threat modeling, and penetration testing
- Implementing Defense in Depth
  - Deploying multiple protective measures across different levels
  - Segmentation of networks to prevent lateral movement, hardening devices with minimal services running
- Continuous Monitoring and Threat Intelligence
  - Building real-time monitoring systems
  - Integrating threat intelligence feeds helps OT operators
- Ensuring that personnel understand the specifics of OT security





- Organizations must embed security requirements directly into their OT operational processes. Aligning daily tasks with legal and regulatory mandates
- Automated tools can be used to track access logs, system configurations, and the enforcement of security controls, helping ensure compliance without the need for frequent audits.
- Organizations should conduct periodic audits to assess their current status against regulatory frameworks, using the findings to refine their strategies and close gaps
- Talk to professional ***Kaspersky***





As OT becomes more interconnected, the vulnerabilities multiply.



Protecting our critical infrastructure requires a collective effort to address the unique challenges of securing OT environments.

Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency (CISA)





Chalermchai Wonggate  
Director of CII Management Office  
[chalermchai.w@nrsa.or.th](mailto:chalermchai.w@nrsa.or.th)

**kaspersky**