

PROACTIVE PROTECTION **X** TOTAL DEFENSE:

THAILAND'S CYBERSECURITY

The National Cyber Security Agency

ANNUAL REPORT

2024



รายงานประจำปี 2567
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ



PROACTIVE PROTECTION  TOTAL DEFENSE:

THAILAND'S CYBERSECURITY



The National Cyber Security Agency
ANNUAL REPORT 2024
รายงานประจำปี 2567
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ



ผลงานเด่นประจำปี 2567 ของ สกมช.



กิจกรรมเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว เนื่องในโอกาสมหามงคลเฉลิมพระชนมพรรษา 6 รอบ 28 กรกฎาคม 2567 Cybersecurity Activities in Honor of His Majesty the King's 72nd Birthday Anniversary on July 28, 2024

สกมช. ร่วมเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว เนื่องในโอกาสมหามงคลเฉลิมพระชนมพรรษา 6 รอบ 28 กรกฎาคม 2567 จัดโครงการและกิจกรรมเฉลิมพระเกียรติฯ ตลอดปี 2567 โดยคำนึงถึงความจำเป็นและประโยชน์ที่มีต่อสังคมโดยรวม เพื่อถวายเป็นพระราชกุศล

The NCSA organized events throughout 2024 to honor His Majesty King Maha Vajiralongkorn on his 72nd birthday anniversary. These initiatives aim to provide societal benefits while paying tribute to His Majesty.



พิธีรับมอบตราสัญลักษณ์ งานเฉลิมพระเกียรติฯ

สกมช. เข้าร่วมพิธีรับมอบตราสัญลักษณ์งานเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว เนื่องในโอกาสพระราชพิธีมหามงคลเฉลิมพระชนมพรรษา 6 รอบ 28 กรกฎาคม 2567 โดยมี ศาสตราจารย์พิเศษวิศิษฐ์ วัชรสินธุ รองอธิบดีกรมส่งเสริมการค้าระหว่างประเทศ เป็นประธาน

Ceremony for Receiving the Royal Emblem

NCSA participated in the emblem presentation ceremony for activities commemorating His Majesty the King's 72nd birthday anniversary. Adjunct Professor Wisit Wisitsora-At, Permanent Secretary of the Ministry of Digital Economy and Society (MDES), presided over the event.



การประชุมเตรียมความพร้อมจัดกิจกรรมฯ

ผู้บริหาร พนักงาน และเจ้าหน้าที่ สกมช. ประชุมเพื่อเตรียมความพร้อมการจัดกิจกรรมเฉลิมพระเกียรติฯ ซึ่งที่ประชุมฯ ได้รับทราบเรื่องการขออนุญาตใช้ตราสัญลักษณ์งานเฉลิมพระเกียรติฯ รวมไปถึงโครงการและกิจกรรมเฉลิมพระเกียรติฯ ที่ สกมช. จะดำเนินการตลอดปี 2567

Preparatory Meeting for Commemorative Activities

NCSA executives and staff convened to discuss preparations for the year-long activities. The meeting acknowledged the use of the royal emblem and outlined planned projects, ensuring alignment with the commemorative purpose.



2024 NCSA HIGHLIGHTS



ด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความรู้ประชาชน และเด็กนักเรียนในพื้นที่ใกล้เคียงศูนย์ฯ 29,543 คน ผ่านศูนย์อินเทอร์เน็ตสาธารณะหรือว่าศูนย์ USO Net จำนวน 1,805 แห่งทั่วประเทศ ทั้งนี้ ได้ดำเนินงานผ่าน ศูนย์ USO Net 6 จังหวัด ประกอบด้วย พิษณุโลก เชียงใหม่ ร้อยเอ็ด ชุมพร นครพนม และระยอง

“Know, Be Aware, and Prevent Cyber Threats” Project

In collaboration with the NBTC, NCSA launched a project to enhance cybersecurity skills among the public, particularly vulnerable groups in remote and underserved areas. The initiative includes training via the **NCSA MOOC platform**, educating over 29,543 individuals through 1,805 USO Net public internet centers across Thailand, with core centers in six provinces: Phitsanulok, Chiang Mai, Roi Et, Chumphon, Nakhon Phanom, and Rayong.

โครงการ “รู้เท่า รู้ทัน รู้ป้องกันภัยไซเบอร์ เพื่อเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว เนื่องในโอกาส มหามงคลเฉลิมพระชนมพรรษา 6 รอบ 28 กรกฎาคม 2567”

สทท. ร่วมกับ สำนักงาน กสทช. ร่วมเสริมสร้างทักษะป้องกันภัยไซเบอร์ ที่เข้าใจง่ายให้ประชาชนและเด็กนักเรียน โดยเฉพาะในกลุ่มผู้เปราะบาง ประชาชนในพื้นที่ชายขอบและพื้นที่ห่างไกล ให้มีความรู้ความเข้าใจและรับมือกับภัยคุกคามทางไซเบอร์ เพื่อสังคมดิจิทัลที่ปลอดภัยสำหรับทุกคน และยังมีการจัดกิจกรรมอบรมแพลตฟอร์ม “NCSA MOOC” ซึ่งเป็นแพลตฟอร์มเพื่อการเรียนรู้



กิจกรรม CSR จัดอาสาเฉลิมพระเกียรติฯ เสริมภูมิเด็กไทย รู้เท่าทันภัยไซเบอร์

CSR Activities: Building Cyber Awareness Empowering Thai Youth

สทท. จัดกิจกรรม CSR เสริมภูมิคุ้มกันผู้สังคมยุคใหม่ รู้เท่าทันภัยไซเบอร์ ณ **มูลนิธิบ้านพระพร** ภายใต้ชื่อกิจกรรม “สทท. เสริมภูมิคุ้มกันผู้สังคมยุคใหม่ รู้เท่าทันภัยไซเบอร์” ซึ่งเป็นส่วนหนึ่งในกิจกรรมจิตอาสาเฉลิมพระเกียรติฯ เพื่อสร้างความตระหนักถึงความสำคัญของภัยคุกคามทางไซเบอร์ไปพร้อม ๆ กับการพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงมอบของบริจาคจากตู้ปันสุขและทุนสนับสนุนโครงการกิจกรรมของมูลนิธิฯ พร้อมเลี้ยงอาหารกลางวัน

NCSA organized a CSR program titled “Empowering the New Era: Cyber Threat Awareness” at the **Baan Phraphon Foundation** to raise awareness about cybersecurity threats. The program included donating supplies, supporting the foundation's projects, and hosting a lunch for attendees.



สทท. ตัดอาวูรทางปัญญา ผ่านกิจกรรม CSR เด็กไทยฉลาดรู้ฉลาดคิด ใช้ชีวิตในโลกไซเบอร์ พร้อมสนับสนุนทุนการศึกษา ซึ่งเป็นส่วนหนึ่งในกิจกรรมจิตอาสาเฉลิมพระเกียรติฯ ณ **โรงเรียนวัดรังสิต จังหวัดปทุมธานี**

As part of its CSR initiatives, NCSA provided scholarships and promoted responsible cyber practices among Thai students at **Wat Rang Sit School, Pathum Thani**.



สทท. นำทีมสร้างภูมิคุ้มกันเด็กรุ่นใหม่ปลอดภัยไซเบอร์ ผ่านกิจกรรม CSR จิตอาสาเฉลิมพระเกียรติฯ ณ **โรงเรียนเทพมงคลรังษี จังหวัดกาญจนบุรี** ซึ่งเป็นส่วนหนึ่งในกิจกรรมจิตอาสาเฉลิมพระเกียรติฯ พร้อมมอบทุนการศึกษาและเลี้ยงอาหารกลางวัน โดยมีอาจารย์และนักเรียนเข้าร่วมกว่า 120 คน NCSA conducted a CSR activity focusing on building cybersecurity awareness for over 120 students, including teachers, providing scholarships, and hosting a lunch at **Thepmongkonrangsri School, Kanchanaburi**.

ผลงานเด่นประจำปี 2567 ของ สกมช.

RANKINGS & ASSESSMENTS



7th
GLOBAL



GCI | Global
Cybersecurity
Index

**ผลการประเมิน 2024
Global Cybersecurity Index (GCI)**

อันดับที่ **7** จาก **194** ประเทศทั่วโลก

ได้คะแนน **99.22/100** อยู่ในกลุ่ม T1-Role Modelling

Ranked 7th out of 194 countries worldwide

Scored 99.22/100, classified in T1-Role Modelling

**การประเมินสถานะของหน่วยงานภาครัฐ
ในการเป็นระบบราชการ 4.0 (PMQA 4.0)**

ประจำปี 2567 ได้คะแนน **473.71** คะแนน เพิ่มขึ้น **16.18** คะแนน **(+3.45%)**

The Public Sector Management Quality Award (PMQA 4.0) in 2024 received a score of 473.71 points, marking an increase of 16.18 points (+3.45%) compared to the previous year

PMQA 4.0



**การประเมินคุณธรรมและความโปร่งใสในการดำเนินงาน
ของหน่วยงานภาครัฐ ประจำปี 2567** อยู่ในระดับผ่าน ด้วยคะแนน **87.56**

Integrity & Transparency Assessment (ITA) 2024: Scored 87.56, falls within the "Pass" range

AWARDS AND INNOVATIONS

**รางวัลเลิศรัฐ ประจำปี 2567
สาขาบริการภาครัฐ
ประเภทนวัตกรรมบริการ**

กับผลงาน Proactive Protection X
Total Defense by NCSA

The NCSA's Proactive Protection X Total Defense project was honored with the Public Sector Excellence Award for Public Service Innovation in 2024



**ISC2[®] GLOBAL
Achievement Awards**

**2024 ISC2 Mid-Career
Professional Award
Recipient**



AVM Jadet Khuhakongkit
CISSP, CGRC, CC

Asia-Pacific Region

**รางวัล 2024 ISC2 Mid-Career
Professional Award:**

พลอากาศตรี จเด็จ กูทะก้องกิจ
ผู้ช่วยเลขาธิการ สกมช.

2024 ISC2 Mid-Career Professional Award:
Awarded to AVM Jadet Khuhakongkit,
Assistant Secretary-General of NCSA

2024 NCSA HIGHLIGHTS

LAWS AND STANDARDS

ประกาศใช้กฎหมายลำดับรองในราชกิจจานุเบกษา รวมทั้งสิ้นจำนวน 6 ฉบับ (The publication of six subordinate legislations) ได้แก่

- 1 ประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566
Notification of the NCSC on Cybersecurity Standards for Information or Information Systems, B.E. 2566 (2023)
- 2 ประกาศ กมช. เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566
Notification of the NCSC on Minimum Standards for Information or Information Systems, B.E. 2566 (2023)
- 3 ประกาศ กมช. เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566
Notification of the NCSC on Standards and Guidelines for Promoting and Developing Cybersecurity Service Systems, B.E. 2566 (2023)
- 4 ประกาศ กกม. เรื่อง หน้าที่ยของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานควบคุมหรือกำกับดูแล พ.ศ. 2567
Notification of the CRC on Obligations for Critical Information Infrastructure Organizations and Regulatory Agencies, B.E. 2567 (2024)
- 5 ประกาศ กมช. เรื่อง มาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2567
Notification of the NCSC on Measures and Guidelines for Enhancing Knowledge, Skills, and Expertise in Cybersecurity, B.E. 2567 (2024)
- 6 ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567
Notification of the NCSC on Cybersecurity Standards for Cloud Systems, B.E. 2567 (2024)



INITIATIVES AND PUBLIC AWARENESS

**การพิจารณาสั่งการกรณี
กลุ่มมิจฉาชีพหลอกลวงประชาชน
โดยใช้แอปดูดเงิน เป็นภัยคุกคาม
ทางไซเบอร์ในระดับร้ายแรง**
ของคณะกรรมการรับมือภัยคุกคาม
ทางไซเบอร์ในระดับร้ายแรง (คสร.)
Elevated Mobile Banking Trojans as an
'Incident at a Critical Level'



ศูนย์ปฏิบัติการพิเศษกรณีกลุ่มมิจฉาชีพ หลอกลวงประชาชนโดยใช้แอปพลิเคชันดูดเงิน

ตรวจจับเหตุการณ์ได้ 206 เหตุการณ์
ป้องกันความเสียหาย 15,091,953 บาท

The Special Operations Center for Mobile Banking Trojans detected 206 incidents of fraudulent activities targeting the public through mobile banking trojan applications, successfully preventing damages totaling 15,091,953 THB.

ผลงานเด่นประจำปี 2567 ของ สกมช.

PUBLIC AWARENESS AND EDUCATION



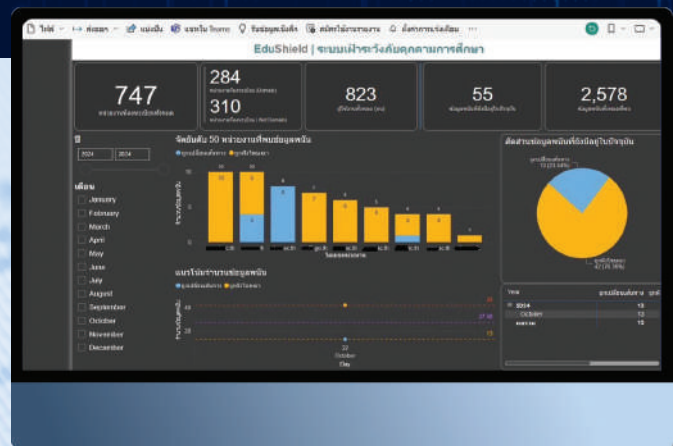
โครงการ "A Good Digital Citizen"

ขยายความรู้สู่ **529** อำเภอ
ผู้เข้าร่วม **35,219** คน
"A Good Digital Citizen"
Project: Extended digital
knowledge to 529 districts,
involving 35,219 participants



โครงการ "เว็บไซต์การศึกษา ปลอดภัยออนไลน์"

เจ้าหน้าที่สนใจ **3,706** คน
ผู้สมัครใช้งาน **1,002** คน
"Secure Education's Website to
Prevent Online Gambling Hijacking"
attracted 3,706 staff members, 1,002
of whom registered as users.



2024 NCSA HIGHLIGHTS

INTERNATIONAL COLLABORATION



การเข้าร่วมเป็นสมาชิก FIRST (Forum of Incident Response and Security Teams) (22 ก.พ. 2567)

และเชื่อมต่อระบบ MISP (Malware
Information Sharing Platform)
เพิ่มข้อมูลการบ่งชี้การโจมตี

On February 22, 2024, NCSA joined FIRST
and connected to FIRST's MISP, extend
source of Indicator of Compromise (IOC).

Project for Enhancing ASEAN - Japan Capacity Building Programme for Cybersecurity and Trusted Digital Services

ภายใต้ AJCCBC (ASEAN-Japan Cybersecurity
Capacity Building Centre) ร่วมกับ JICA (Japan
International Cooperation Agency) ให้แก่ประเทศ
สมาชิกอาเซียนทั้ง 10 ประเทศ มีผู้ผ่านการอบรม 271 คน
และในรูปแบบออนไลน์มีผู้ผ่านการอบรม 384 คน

“Project for Enhancing ASEAN - Japan Capacity Building
Programme for Cybersecurity and Trusted Digital
Services”, provided training to all 10 ASEAN member
countries total of 655 individuals trained.



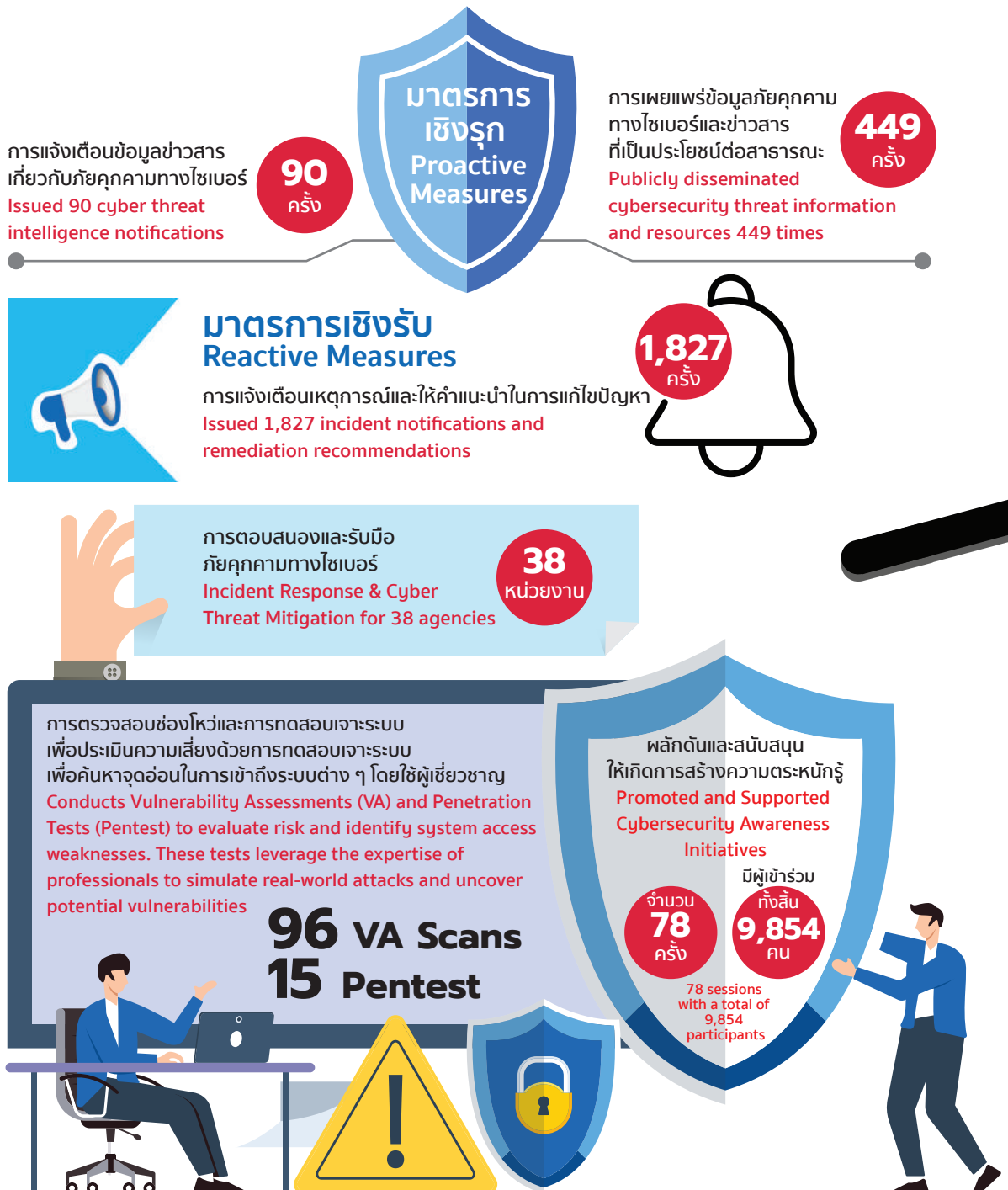
เจ้าภาพจัดการประชุมคณะทำงาน อาเซียน-ญี่ปุ่น ว่าด้วยการรักษาความมั่นคง ปลอดภัยไซเบอร์ ครั้งที่ 1 ประจำปี 2567 (The 1st ASEAN - Japan Cybersecurity Working Group Meeting 2024)

มีผู้แทนเข้าร่วมจากกลุ่มประเทศ
อาเซียน 10 ประเทศ สำนักงานเลขาธิการอาเซียน และ The
National Center of Incident Readiness and Strategy for
Cybersecurity (NISC) เข้าร่วมประมาณ 50 คน
Hosting the 1st ASEAN-Japan Cybersecurity Working
Group Meeting (2024) Representatives from 10 ASEAN
countries and NISC, totaling 50 participants

ผลงานเด่นประจำปี 2567 ของ สกมช.

ผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่มีผลกระทบอย่างมีนัยสำคัญ

Key Achievements in Cybersecurity Operations



2024 NCSA HIGHLIGHTS

สรุปสถานการณ์ภัยคุกคามทางไซเบอร์

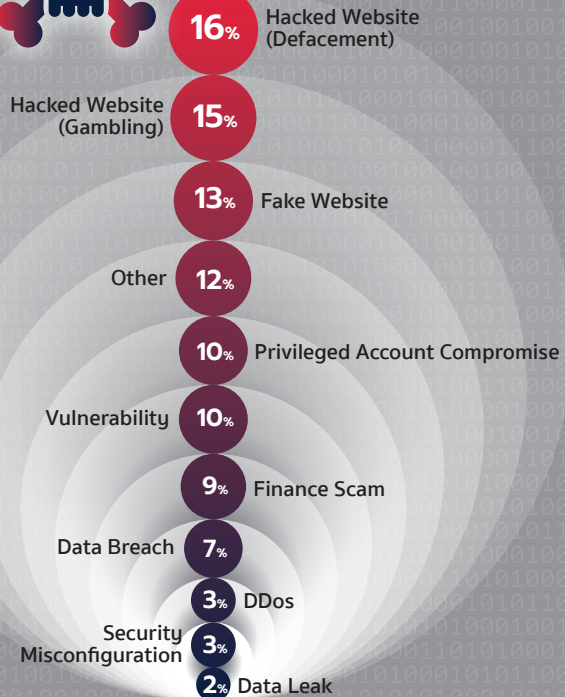
ต.ค. 66 - ก.ย. 67

ที่มา: ThaiCERT

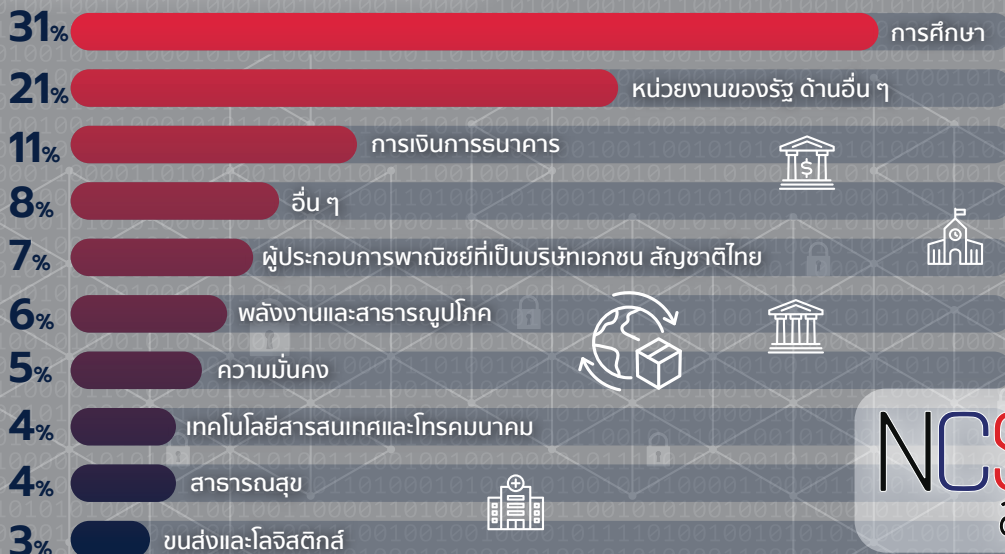
รวมทั้งสิ้น
1,827
ครั้ง



รูปแบบภัยคุกคาม



ประเภทภารกิจหน่วยงาน



สารนายกรัฐมนตรี

MESSAGE FROM THE PRIME MINISTER



ปัญหาอาชญากรรมออนไลน์เป็นสาเหตุสำคัญที่สร้างความเดือดร้อนให้แก่พี่น้องประชาชน และส่งผลกระทบต่อการพัฒนาประเทศ ซึ่งรัฐบาลไม่ได้มีเจตนาที่จะเร่งแก้ไขปัญหาต่าง ๆ เหล่านี้ โดยบูรณาการหน่วยงานที่เกี่ยวข้องเพื่อเพิ่มประสิทธิภาพในการเสริมสร้างป้องกันปราบปราม และแก้ไขปัญหามาในทุกระดับ ทั้งในระดับประเทศ และระดับนานาชาติ รวมถึงการพัฒนาโครงสร้างพื้นฐานทางไซเบอร์ให้สามารถตอบสนองต่อการป้องกันภัยคุกคามรูปแบบใหม่และแก้ไขปัญหอาชญากรรมออนไลน์ทุกรูปแบบ เพื่อปกป้องทรัพย์สินและชีวิตของพี่น้องประชาชน รวมถึงผลประโยชน์ของชาติ

ตลอดระยะเวลาที่ผ่านมาการดำเนินงานของ**สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ** มีส่วนสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์ และเป็นกำลังสำคัญที่ช่วยเสริมสร้างความปลอดภัย และแก้ไขปัญหาคาการกระทำผิดทางไซเบอร์ทุกประเภทให้แก่ประเทศในภาพรวม ดิฉันขอเป็นกำลังใจให้ผู้ปฏิบัติงานทุกคนที่มีส่วนสำคัญในการขับเคลื่อนภารกิจการสร้าง ความมั่นคงปลอดภัยทางไซเบอร์ของชาติให้เกิดประสิทธิผล และสร้างความปลอดภัยทางไซเบอร์แก่พี่น้องประชาชนตลอดมา

ดิฉันหวังว่ารายงานผลการดำเนินงานประจำปีงบประมาณ **พ.ศ. 2567** จะเป็นประโยชน์แก่หน่วยงานที่เกี่ยวข้องและผู้มีส่วนได้ส่วนเสียที่จะได้รับทราบถึงผลการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รวมทั้งทำให้ประชาชนเข้าใจถึงผลกระทบที่เกิดขึ้นจากปัญหาอาชญากรรมและอาชญากรรมออนไลน์ และรู้จักป้องกันความเสี่ยงที่อาจจะเกิดขึ้นจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพต่อไป



Online crime is a major concern, causing significant hardship for the public and impeding national development. The government remains committed to addressing these challenges by integrating efforts from all relevant agencies to enhance the effectiveness of prevention, suppression, and resolution across all dimensions, both domestically and internationally. This includes the development of cybersecurity infrastructure capable of responding to new threats and resolving all forms of online crime, safeguarding the lives and assets of the people, and protecting the nation's interests.

Over the years, the **National Cyber Security Agency (NCSA)** has played a pivotal role in maintaining cybersecurity. It has been a key force in enhancing safety and addressing cybercrimes at all levels. I extend my heartfelt encouragement to all personnel who contribute significantly to effectively driving the nation's cybersecurity mission and ensuring the safety of the public.

I hope that the **NCSA Annual Report 2024** will serve as a valuable resource for all relevant agencies and stakeholders, providing insights into the NCSA's accomplishments. Moreover, I hope it fosters greater public understanding of the impacts of crime and online crime, empowering citizens to mitigate risks posed by cyber threats effectively in the future.



(นางสาวอุฬราร ชินวัตร)
นายกรัฐมนตรี

สารรองนายกรัฐมนตรี

และรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) และ

ประธานกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)



MESSAGE FROM THE DEPUTY PRIME MINISTER

& THE MINISTER OF DIGITAL ECONOMY AND SOCIETY

Chairman of the National Cyber Security Committee (NCSC)

Chairman of the Cybersecurity Regulating Committee (CRC)

Chairman of the Committee Managing the National Cyber Security Agency (CMSA)



ปัจจุบันเทคโนโลยีมีความก้าวหน้าอย่างก้าวกระโดด ก่อให้เกิดภัยคุกคามหลายรูปแบบโดยเฉพาะก่อให้เกิดอาชญากรรมทางไซเบอร์ที่มีความซับซ้อนและหลากหลายมากขึ้น ซึ่งสร้างความเสียหายเพิ่มขึ้นต่อการดำเนินชีวิตของพี่น้องประชาชน และเกิดผลกระทบต่อความมั่นคงของประเทศ ทั้งในด้านเศรษฐกิจและสังคม การรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยให้มีประสิทธิภาพสูงสุด จึงต้องบูรณาการความร่วมมือจากทุกภาคส่วนเป็นสำคัญ

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ในปีที่ผ่านมาได้ขับเคลื่อน ติดตาม ประเมินผลอย่างต่อเนื่องและมีประสิทธิภาพ ส่งผลให้การประเมินดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ของโลก จากการจัดอันดับ

Global Cybersecurity Index 2024 (GCI) ในปี พ.ศ. 2567 ประเทศไทยก้าวขึ้นสู่อันดับที่ 7 ของโลก โดยมีการประเมินทั้งด้านกฎหมาย ด้านเทคนิค ด้านหน่วยงาน ด้านการพัฒนาศักยภาพและด้านความร่วมมือ แสดงให้เห็นถึงการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุมทุกมิติ อีกทั้งยังได้มีการประกาศ เรื่อง **มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567** ซึ่งสะท้อนให้เห็นถึงการกำกับดูแลและการบริหารจัดการความเสี่ยงที่มีประสิทธิภาพทันสมัยเท่าทันต่อเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว

คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) ยังเป็นอีกบทบาทหนึ่งที่มีความสำคัญต่อการส่งเสริมและพัฒนาศักยภาพในการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ของประเทศเป็นอย่างมาก เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์สามารถปฏิบัติภารกิจได้อย่างรวดเร็ว มีประสิทธิภาพ ทั้งในการรับมือกับภัยคุกคามทางไซเบอร์และอาชญากรรมทางไซเบอร์ทุกรูปแบบโดยเฉพาะอย่างยิ่งในเรื่องของการประกาศยกระดับภัยคุกคามจากการหลอกลวงติดตั้ง**แอปพลิเคชันเพื่อขโมยเงิน (Mobile Banking Trojan)** ซึ่งเป็นปัญหาที่สร้างมูลค่าความเสียหายให้แก่ประชาชนและประเทศชาติอย่างมหาศาล ถือเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง นอกจากนี้ยังมีการกำหนดให้หน่วยงานของทุกภาคส่วนที่เกี่ยวข้องบูรณาการความร่วมมือในการปฏิบัติการเชิงรุก เพื่อช่วยป้องกันและแก้ไขปัญหาภัยคุกคามจากการจารกรรมทางไซเบอร์ เพื่อสร้างความปลอดภัยให้แก่ประชาชน รวมทั้งเกิดความเชื่อมั่นต่อการใช้บริการทางการเงินออนไลน์ อีกทั้งยังมีการเปิดตัว**สถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ** เพื่อถ่ายทอดความรู้และความตระหนักรู้แก่ประชาชนและหน่วยงานต่าง ๆ ภายในประเทศ ตลอดจนมีการติดตามกำกับ**การฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ระดับประเทศ (Thailand's National Cyber Exercise 2024)** เพื่อสร้างมาตรฐานความมั่นคงปลอดภัยไซเบอร์ที่แข็งแกร่งตั้งแต่ระดับโครงสร้างพื้นฐานสำคัญของประเทศแก่ทุกภาคส่วนทั้งหน่วยงานภาครัฐ ภาคเอกชน จนไปสู่ระดับประชาชน

การดำเนินการที่สำคญนี้ จะสามารถบรรลุผลสำเร็จที่มีประสิทธิภาพได้อย่างมั่นคงและยั่งยืนก็ด้วยการกำกับดูแลการบริหารจัดการที่ดีภายในองค์กร เกิดจากบทบาทของ **คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)** ที่มีส่วนสำคัญยิ่งในการกำกับ ดูแลปฏิบัติภารกิจทุกคน ตั้งแต่ระดับผู้บริหาร พนักงานและลูกจ้าง ให้มีความร่วมมือกันและผลักดันจนนำไปสู่การดำเนินงานของหน่วยงานที่ก้าวหน้าขึ้นไปอีกระดับ โดยสิ่งที่บ่งชี้เห็นได้ชัดเจนคือ **ผลการประเมินองค์กรจากบุคคลภายนอกในปี พ.ศ. 2567 อยู่ในระดับคะแนน 98.60 คะแนน** จัดอยู่ในระดับดีมากและการได้รับรางวัลเลิศรัฐ สาขารางวัล **บริการภาครัฐ** ประเภทนวัตกรรมบริการ ด้วยผลงาน Proactive Protection X Total Defense by NCSA ซึ่งถือเป็นความสำเร็จที่เป็นรูปธรรม ผลักดันให้การยกระดับการทำงานในการรักษาความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของประเทศมีประสิทธิภาพอย่างต่อเนื่อง

ในนามประธานคณะกรรมการทั้ง 3 คณะ ผมมีความยินดีและรู้สึกภูมิใจที่ได้กำกับดูแลความมั่นคงปลอดภัยไซเบอร์ในทุกระดับ ร่วมกับคณะกรรมการจากหน่วยงานภาครัฐ ภาคเอกชน และผู้เชี่ยวชาญ เพื่อขับเคลื่อนงานในการกิจด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยให้เกิดประโยชน์สูงสุดและสร้างความมั่นคงให้แก่มกประเทศ ตอบสนองต่อนโยบายของรัฐบาลที่มุ่งเน้นการผลักดันให้มีการลงทุนต่อโครงสร้างพื้นฐานสำคัญทางดิจิทัลเพื่อส่งเสริมให้ประเทศไทยมีความมั่นคงทางเศรษฐกิจ ประชาชนมีความเป็นอยู่ที่ดียิ่งขึ้น ในโอกาสนี้ ผมขอให้กำลังใจผู้บริหาร ข้าราชการ และเจ้าหน้าที่สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติทุกคนที่ได้มุ่งมั่น และตั้งใจปฏิบัติหน้าที่ร่วมกันมาอย่างเข้มแข็ง โดยมีเป้าหมายป้องกัน รับมือและลดความเสี่ยง จากภัยคุกคามทางไซเบอร์ รวมทั้งป้องกันมิให้อาชญากรรมทางไซเบอร์ทุกรูปแบบเกิดขึ้น ซึ่งจะส่งเสริมให้ประเทศไทยให้ก้าวสู่ความเป็นผู้นำในด้านความมั่นคงปลอดภัยไซเบอร์ในระดับภูมิภาคต่อไป

Rapid advancements in technology have led to increasingly diverse and complex cyber threats. These threats can cause significant damage, disrupting citizens' lives and impacting the nation's security, economy, and society. To ensure maximum cybersecurity efficiency for Thailand, collaboration across all sectors is imperative.

The **National Cyber Security Committee (NCSC)** has made substantial progress over the past year by driving, monitoring, and evaluating cybersecurity initiatives. As a result, Thailand advanced to **7th place in the Global Cybersecurity Index (GCI) 2024**, achieving a score of 99.22 out of 100. This evaluation encompasses legal, technical, organizational, capacity-building, and cooperative dimensions, reflecting comprehensive cybersecurity coverage. Moreover, the Committee

issued the **Cloud Cybersecurity Standards B.E. 2567**, demonstrating effective and modern risk management aligned with rapidly evolving technologies.

The **Cybersecurity Regulating Committee (CRC)** also played a crucial role in strengthening the nation's cyber defenses, ensuring rapid and effective responses to cyber threats and crimes. This includes elevating **Mobile Banking Trojans** to the 'Incident at a Critical Level', an issue causing extensive financial losses. Proactive measures have been introduced to integrate operations across relevant agencies, ensuring public safety and building trust in online financial services. Additionally, the **Thailand National Cyber Academy** was established to raise awareness and impart knowledge to citizens and organizations. The **Thailand National Cyber Exercise 2024** was conducted to strengthen cybersecurity standards across critical infrastructure, public and private sectors, and down to individual citizens.

These vital initiatives were achieved through effective organizational governance, led by the **Committee Managing the National Cyber Security Agency (CMSA)**. The committee has overseen personnel at all levels, fostering collaboration that resulted in external evaluations rating the agency at **98.60 points**, categorized as "Excellent." The agency also received the prestigious **Public Sector Excellence Award** for its innovative work, Proactive Protection X Total Defense by NCSA, a testament to its impactful contributions to national cybersecurity.

As Chairman of these three committees, I am honored and proud to have overseen cybersecurity at all levels alongside experts from public and private sectors. Together, we have advanced Thailand's cybersecurity mission, supporting government policies that encourage investment in critical digital infrastructure to bolster economic stability and improve citizens' quality of life. I extend my deepest gratitude to the executives, officials, and staff of the National Cyber Security Agency for their unwavering commitment to protecting the nation from cyber threats and crimes. With our collective efforts, I am confident that Thailand will emerge as a regional leader in cybersecurity, ensuring a safer and more secure future for all.


(นายประเสริฐ จันทรรวงทอง)
รองนายกรัฐมนตรีและรัฐมนตรีว่าการกระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

สารเลขาธิการคณะกรรมการ

การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

กรรมการและเลขานุการ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

(กมช.) คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) และ

คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)



MESSAGE FROM SECRETARY-GENERAL

OF THE NATIONAL CYBER SECURITY COMMITTEE

Committee and Secretary of National Cyber Security Committee (NCSC),
Cybersecurity Regulating Committee (CRC), and
Committee Managing the National Cyber Security Agency (CMSA)



การเติบโตทางเทคโนโลยีอย่างรวดเร็ว เป็นสิ่งกระตุ้นให้หน่วยงานทุกภาคส่วนในประเทศไทย ทั้งภาครัฐและภาคเอกชน รวมทั้งประชาชน จำเป็นต้องใช้เทคโนโลยีเพื่อการทำงานและการดำรงชีวิตที่เพิ่มมากขึ้น ไม่ว่าจะเป็นการบริการภาครัฐที่สำคัญ การเงินการธนาคาร เทคโนโลยีสารสนเทศและโทรคมนาคม การขนส่งและโลจิสติกส์ พลังงาน และสาธารณสุข สาธารณสุข ตลอดจนไปถึงกิจกรรมที่เกี่ยวข้องในด้านความมั่นคงของรัฐ ด้วยเหตุนี้ จึงเป็นเรื่องที่ทำให้ต้องเผชิญกับภัยคุกคามทางไซเบอร์อย่างหลีกเลี่ยงไม่ได้ จากการสำรวจความเสี่ยงระดับโลกของ WORLD ECONOMIC FORUM ประจำปี 2023-2024 พบว่า ในระยะสั้น

2 ปีข้างหน้าหรือปี ค.ศ. 2026 ความไม่มั่นคงปลอดภัยทางไซเบอร์ (CYBER INSECURITY) จัดอยู่ในอันดับที่ 4 จาก 10 อันดับ ความเสี่ยงที่รุนแรงระดับโลก และในระยะยาว 10 ปีข้างหน้าหรือปี ค.ศ. 2034 ยังคงอยู่ในอันดับที่ 8 ของโลก นอกจากนี้ ยังมีเรื่องของภัยคุกคามทางไซเบอร์ที่มาจากปัญญาประดิษฐ์ (ARTIFICIAL INTELLIGENCE: AI) ที่มีความซับซ้อนและมีแนวโน้มทวีความรุนแรงเพิ่มมากขึ้น สิ่งเหล่านี้แสดงให้เห็นว่า ภัยคุกคามทางไซเบอร์ยังคงเป็นปัญหาท้าทายสำหรับประเทศไทยที่ต้องเผชิญ และปรับตัวให้มีความพร้อม ในการรับมือ ป้องกัน และลดความเสี่ยงอย่างมีประสิทธิภาพ

ปี พ.ศ. 2567 นี้เป็นปีที่ 2 ของระดมในบทบาทเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งได้เน้นย้ำอย่างต่อเนื่องในเรื่องของ PROACTIVE PROTECTION (การป้องกันเชิงรุก) และ TOTAL DEFENSE (การผนึกกำลังในการป้องกัน) เพื่อให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สภามช.) สามารถบูรณาการขับเคลื่อนร่วมกับหน่วยงานต่าง ๆ ที่เกี่ยวข้องทั้งภายในประเทศและต่างประเทศ เสริมสร้างให้การรักษาความมั่นคงปลอดภัยไซเบอร์ในภาพรวมมีประสิทธิภาพ เป็นไปตามมาตรฐานสากล และมีความเข้มแข็งอย่างยั่งยืน

และจากการที่ประเทศไทยได้รับการประเมินดัชนีความมั่นคงปลอดภัยไซเบอร์ของโลก (GLOBAL CYBERSECURITY INDEX : GCI) ประจำปี พ.ศ. 2567 ครั้งล่าสุด มีคะแนนประเมินรวม 99.22 จาก 100 คะแนน ได้รับการประเมินจัดอยู่ในกลุ่ม T1-ROLE MODELLING และจัดอยู่ในอันดับที่ 7 จาก 194 ประเทศและรัฐทั่วโลก จึงเป็นเครื่องบ่งชี้ได้อย่างชัดเจนว่าความสำเร็จดังกล่าวได้รับความร่วมมือจากทุกภาคส่วน เป็นจุดเริ่มต้นของการพัฒนาและดำรงสถานภาพความมั่นคงปลอดภัยไซเบอร์ให้ยั่งยืนอย่างแท้จริง

ในนามของ สกมช. กระผมขอขอบคุณอย่างยิ่งสำหรับความร่วมมือจากหน่วยงานทุกภาคส่วน ทั้งหน่วยงานควบคุมหรือกำกับดูแล (REGULATOR) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (หน่วยงาน CII) หน่วยงานของรัฐ หน่วยงานภาคเอกชน และภาคประชาสังคม ตลอดจนบุคลากรของ สกมช. ที่มุ่งมั่นปฏิบัติหน้าที่ของตนเองอย่างเต็มที่และต่อเนื่อง และในปี พ.ศ. 2568 เราจะดำรงความมุ่งมั่นหมายการบูรณาการการรักษาความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของประเทศให้ตรงกับคำสำคัญที่กระผมได้กำหนดไว้คือ **TEAM THAILAND FOR CYBERSECURITY** เพื่อตอบสนองนโยบายรัฐบาลที่มุ่งผลประโยชน์ต่อประชาชนและประเทศชาติอย่างแท้จริง

The rapid pace of technological advancement has necessitated increased reliance on technology across all sectors in Thailand. Government agencies, private businesses, and individual citizens increasingly rely on technology for work, daily life, and accessing essential public services, finance, communication, transportation, energy, public health, and even national security. However, this dependency has also made Thailand increasingly vulnerable to cyber threats.

According to the World Economic Forum's 2023-2024 Global Risks Report, cybersecurity ranks as the fourth most severe global risk in the short term (by 2026). It remains in the eighth position globally in the long term (by 2034). The rising complexity and intensity of cyber threats, including those driven by Artificial Intelligence (AI), underscore the urgent need for Thailand to enhance its preparedness to mitigate these risks effectively and proactively.

In 2024, my second year as Secretary-General of the National Cyber Security Committee, I have continued to emphasize Proactive Protection and Total Defense as key strategies. These approaches aim to integrate efforts with domestic and international partners, ensuring Thailand's cybersecurity framework meets global standards and achieves long-term sustainability.

Thailand's success in achieving a score of **99.22 out of 100** in the **2024 Global Cybersecurity Index (GCI)**, securing **7th place globally** and recognition in the **Tier 1 - Role Modelling**, is a testament to our collective commitment. This achievement is a milestone and a foundation for further development to sustain and enhance national cybersecurity.

On behalf of the NCSA, I extend my deepest gratitude to all stakeholders, including regulators, organizations of critical information infrastructure, government agencies, private enterprises, civil society, and the dedicated personnel of the NCSA. Your unwavering efforts have been instrumental in our progress. As we move forward into 2025, we remain steadfast in our mission to strengthen national cybersecurity under the guiding principle of **"Team Thailand for Cybersecurity."** This reflects our commitment to aligning with government policies to benefit the people and the nation.

พลอากาศตรี

(อมร ชมเชย)

เลขาธิการคณะกรรมการ

การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

กรรมการและเลขานุการ

CONTENTS

สารบัญ

- 2 ผลงานเด่นประจำปี 2567
- 10 สารนายกรัฐมนตรี
- 12 สารรองนายกรัฐมนตรีและประธาน กมช.
- 14 สาร ลร.กมช.

01

ORGANIZATIONAL STRUCTURE OVERVIEW

- 17 เกี่ยวกับองค์กร
- 18 ประวัติความเป็นมา
- 20 การยกระดับความมั่นคงปลอดภัยไซเบอร์
- 22 วิสัยทัศน์
- 23 การขับเคลื่อนองค์กร
- 24 รายงาน กมช.
- 26 รายงาน กกม.
- 28 รายงาน กบส.
- 30 การเข้าร่วมประชุมของ กบส.
- 32 คณะกรรมการและคณะอนุกรรมการ ที่ กบส. แต่งตั้ง
 - 32 คณะกรรมการตรวจสอบภายใน
 - 32 คณะอนุกรรมการด้านกฎหมาย
 - 32 คณะอนุกรรมการด้านการบริหารงานบุคคล
 - 33 คณะอนุกรรมการด้านยุทธศาสตร์
 - 33 คณะอนุกรรมการประเมินผลการปฏิบัติงานของเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
- 34 คณะผู้บริหาร NCSA
- 38 โครงสร้างองค์กร

02

OPERATIONAL PERFORMANCE HIGHLIGHTS

- 40 ผลการดำเนินงาน
- 41 ยุทธศาสตร์ที่ 1 CAPACITY
- 66 ยุทธศาสตร์ที่ 2 PARTNERSHIP
- 82 ยุทธศาสตร์ที่ 3 RESILIENCE
- 94 ยุทธศาสตร์ที่ 4 STANDARD
- 124 ผลงานอื่น ๆ

03

FINANCIAL REPORT

128 รายงานทางการเงิน

04

PERFORMANCE EVALUATION

134 การประเมินผลการดำเนินงาน

05

ISSUES, CHALLENGES, AND RECOMMENDATIONS & 2025 OPERATIONAL PLAN

136 ปัญหา อุปสรรค และข้อเสนอแนะ &
แผนการดำเนินงานปี 2568

06

APPENDIX

142 ภาคผนวก



เกี่ยวกับองค์กร

ORGANIZATIONAL STRUCTURE OVERVIEW

ประวัติความเป็นมา HISTORY

จุดเริ่มต้น สกมช.

ภัยคุกคามทางไซเบอร์ทวีความรุนแรงขึ้นทั่วโลกในช่วงทศวรรษที่ผ่านมา เหตุการณ์โจมตีระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศเกิดขึ้นบ่อยครั้ง สร้างความเสียหายต่อความมั่นคงของรัฐและประชาชนอย่างกว้างขวาง ตอกย้ำถึงความสำคัญเร่งด่วนของการรักษาความมั่นคงปลอดภัยไซเบอร์ และการพัฒนาขีดความสามารถในการรับมือภัยคุกคามทั้งในปัจจุบันและอนาคต

บทเรียนจากภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงของประเทศ

- ▶ **เอสโตเนีย** กรณีการโจมตี ด้วย DDOS ที่ใหญ่ที่สุดใน พ.ศ. 2550 ส่งผลกระทบต่อระบบคอมพิวเตอร์ของประเทศทุกระบบ ทั้งเว็บไซต์ และการให้บริการทางการเงินหยุดชะงัก ไม่สามารถให้บริการได้หลายสัปดาห์
- ▶ **WANNACRY** เป็นการโจมตีทางไซเบอร์ที่ส่งผลกระทบในวงกว้างทั่วโลกและเป็นกรณีศึกษาที่สำคัญในปี 2017 โดยเป็นมัลแวร์แบบ RANSOMWARE ที่มีการเข้ารหัสข้อมูลสำคัญบนเครื่องที่ถูกโจมตี และเรียกค่าไถ่จากผู้เสียหาย มีการแพร่กระจายบนระบบปฏิบัติการวินโดวส์โดยใช้ ETERNALBLUE ซึ่งเป็นโปรแกรมที่ใช้ช่องโหว่ความมั่นคงปลอดภัยเข้าถึงระบบโดยไม่ได้รับอนุญาต ส่งผลกระทบต่อองค์กรต่าง ๆ ใน 150 ประเทศ เช่น NHS ในสหราชอาณาจักร และบริษัทโทรคมนาคมในสเปน เหตุการณ์นี้ชี้ให้เห็นถึงความสำคัญของการอัปเดตระบบเพื่อปิดช่องโหว่ความมั่นคงปลอดภัย การสำรองข้อมูล และการเฝ้าระวังความปลอดภัยอย่างต่อเนื่อง
- ▶ **STUXNET** เป็นมัลแวร์แบบ WORM ซึ่งพุ่งเป้าโจมตีไปที่ระบบ SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) ผู้เชี่ยวชาญเชื่อว่า STUXNET เป็นต้นเหตุที่สร้างความเสียหายให้กับโครงการนิวเคลียร์ของอิหร่าน STUXNET มีการใช้ประโยชน์จากช่องโหว่ที่ยังไม่ได้รับการค้นพบและเปิดเผย (ZERO-DAY) เพื่อโจมตี PROGRAMMABLE LOGIC CONTROLLER (PLC) และทำให้เครื่องหมุนเหวี่ยงแยกวัตถุ (FAST-SPINNING CENTRIFUGE) ทำงานผิดพลาดและเกิดความเสียหายเป็นจำนวนมาก ทำให้โครงการนิวเคลียร์ของอิหร่านล่าช้าไป นับเป็นอาวุธดิจิทัลที่ทั่วโลกให้ความสนใจและสร้างความตื่นตัวให้เห็นถึงความสำคัญของการปกป้องรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานที่สำคัญของประเทศ

KEY MILESTONES IN THE CYBERSECURITY ACT ENACTMENT PROCESS



- ▶ **ประเทศไทย** เหตุการณ์โจมตีระบบการให้บริการที่สำคัญต่าง ๆ ภายในประเทศไทย ที่ส่งผลให้เกิดการรั่วไหลของข้อมูลส่วนบุคคล และเป็นต้นตอของอาชญากรรมทางไซเบอร์ การหลอกลวงผ่านสื่อสังคมออนไลน์

สิ่งเหล่านี้แสดงให้เห็นถึงผลกระทบทางเศรษฐกิจและสังคมที่ประชาชนได้รับ ซึ่งมีแนวโน้มทวีความรุนแรงเพิ่มมากขึ้น ด้วยความจำเป็นเร่งด่วนในการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างเป็นรูปธรรม ประเทศไทยจึงได้ตรา **พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562** และมีผลบังคับใช้ เมื่อวันที่ 28 พฤษภาคม พ.ศ. 2562 เป็นต้นไป

Cyber threats have become a critical issue, impacting national security globally. Several incidents highlight the urgency of robust cybersecurity measures:

- ▶ **Estonia's DDoS attack in 2007** disrupted all computer systems, including websites and financial services, leaving them inoperable for weeks.

- ▶ **WannaCry** was a major global cyberattack in 2017, utilizing ransomware to encrypt critical data and demand ransom. It exploited the EternalBlue vulnerability in Windows systems, spreading rapidly and impacting organizations in 150 countries, including the UK's NHS and telecom firms in Spain. This incident underscored the importance of system updates, data backups, and continuous security monitoring.

- ▶ **Stuxnet**, a worm targeting SCADA systems, disrupted Iran's nuclear program by exploiting zero-day vulnerabilities to attack Programmable Logic Controllers (PLCs). It caused significant damage to centrifuges, delaying the program. As the first digital weapon, Stuxnet highlighted the critical need for robust cybersecurity to protect national infrastructure.

- ▶ **Thailand's cyber incidents** led to significant personal data leaks and cybercrimes, such as online scams, disrupting critical services.

To address this, Thailand enacted the **Cybersecurity Act B.E. 2562 (2019), effective May 28, 2019**, to enhance national cybersecurity, protect critical infrastructure, and mitigate risks.



การยกระดับ ความมั่นคงปลอดภัย ไซเบอร์

CYBERSECURITY ADVANCEMENTS

ปี
2562

2019

- ▶ ตรากฎหมายพระราชบัญญัติ
การรักษาความมั่นคงปลอดภัย
ไซเบอร์ พ.ศ. 2562
Enactment of the
Cybersecurity Act B.E.
2562 (2019)



ปี
2564

2021

- ▶ การจัดตั้ง สกมช.
Establishment of the NCSA
- ▶ การจัดตั้ง National CERT
และมีการโอนสิทธิ์ ThaiCERT
จาก ETDA มาให้ สกมช.
ในปี 2566
Establishment of the National
CERT and transfer of
ThaiCERT from ETDA to
NCSA in 2023
- ▶ การกำหนด Regulator และ
หน่วยงาน Critical Information
Infrastructure (CII)
Designation of Regulators
and Organizations of Critical
Information Infrastructure

ปี
2565

2022

- ▶ การฝึก National
Cybersecurity Exercise 2022
เป็นครั้งแรกของประเทศไทย
First National Cybersecurity
Exercise 2022 conducted
in Thailand
- ▶ การจัดตั้งกลุ่ม Thailand CERTs
Community
Establishment of the Thailand
CERTs Community



ปี
2566

ปี
2567

2023

- ▶ การจัดตั้ง Center of Excellence ด้านวิชาการความมั่นคงปลอดภัยไซเบอร์
Establishment of the Center of Excellence in Cybersecurity
- ▶ การฝึก National Cybersecurity Exercise วงรอบ 3 ปี
Conducting the National Cybersecurity Exercise (3-Year Cycle)
- ▶ การแต่งตั้ง คสร. และการฝึกซ้อมเตรียมรับมือภัยคุกคามทางไซเบอร์ระดับประเทศ
Establishment of the CIRC and preparation for managing severe and critical national cyber threats

2024

- ▶ ประเทศไทยได้รับการจัดอันดับที่ 7 ในดัชนีความมั่นคงปลอดภัยไซเบอร์ระดับโลก จากทั้งหมด 194 ประเทศ ด้วยคะแนน 99.22 จาก 100 คะแนน
Thailand ranked 7th in the Global Cybersecurity Index (GCI) out of 194 countries, scoring 99.22/100
- ▶ ยกระดับภัยคุกคามจากแอปดูดเงิน เป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง
Elevated Mobile Banking Trojans as an 'Incident at a Critical Level'
- ▶ ThaiCERT ได้รับการยอมรับเป็นสมาชิกของ FIRST และ AP-CERT
ThaiCERT is recognized as a member of FIRST and AP-CERT

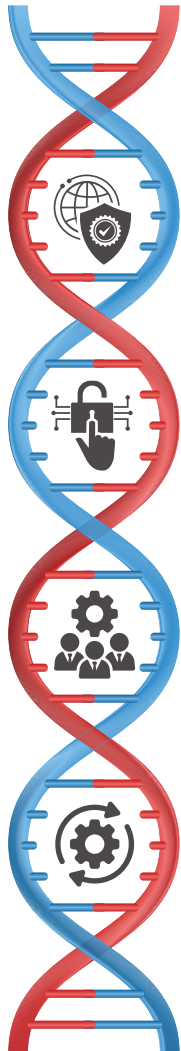
VISION

วิสัยทัศน์และการขับเคลื่อนองค์กร

วิสัยทัศน์ VISION

เป็นผู้นำในการขับเคลื่อนในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยที่มีประสิทธิภาพ พร้อมตอบสนองต่อภัยคุกคามไซเบอร์ทุกมิติ

To be a leader in driving forward effective cybersecurity management in Thailand and always ready to respond to all dimensions of cyber threats



N

NATIONAL :

เป็นองค์กรระดับชาติมีหน้าที่ขับเคลื่อนและสร้างความมั่นคงปลอดภัยไซเบอร์ของประเทศและเป็นศูนย์กลางความร่วมมือหน่วยงานภาครัฐและเอกชนทั้งภายในและต่างประเทศ

Acting as a national-level organization which is responsible for advancing cybersecurity in the country and serving as a central hub for domestic and international collaboration between government and private agencies.

C

COMPETENCY/CUSTOMER CENTRIC :

ต้องมุ่งพัฒนาให้เป็นองค์กรสมรรถนะสูง ในระดับหน่วยงานและระดับบุคคล มุ่งเน้นการบริการให้ประเทศ ประชาชน Regulator และ CII เกิดความประทับใจเกินคาดหวัง

Focusing on developing NCSA into a high-performance organization at both the organizational and individual levels. Focusing on serving the country, people, Regulators, and CIs to impress and exceed expectations.

S

STRONG/SYNERGY :

ต้องเข้มแข็งด้วยความสามัคคี ผนึกกำลังในการปฏิบัติหน้าที่

Showing strength and synergy to fulfill responsibilities.

A

AGILITY :

ต้องมีความคล่องตัวพร้อมรับมือทุกความเปลี่ยนแปลงและทุกความท้าทาย

Operating with agility, adapting to changes and challenges.

พันธกิจ MISSION



1

เสนอแนะและขับเคลื่อนนโยบายแผนยุทธศาสตร์และปรับปรุงกฎหมาย ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งศึกษาวิจัยกำหนดแนวทางมาตรฐาน มาตรการที่เกี่ยวข้องให้สอดคล้องกับสถานการณ์ทั้งในปัจจุบันและอนาคต
Recommend and implement policies, plans, strategies, and improve laws on cybersecurity, including research, establishing guidelines, standards, and relevant measures in line with current and future situations



2

กำกับ ดูแล เฝ้าระวัง ติดตาม วิเคราะห์ ประมวลผล แจ้งเตือน และปฏิบัติการ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์
Regulate, monitor, analyze, process, notify, and also prevent, respond to, and mitigate the risk of cyber threats.



3

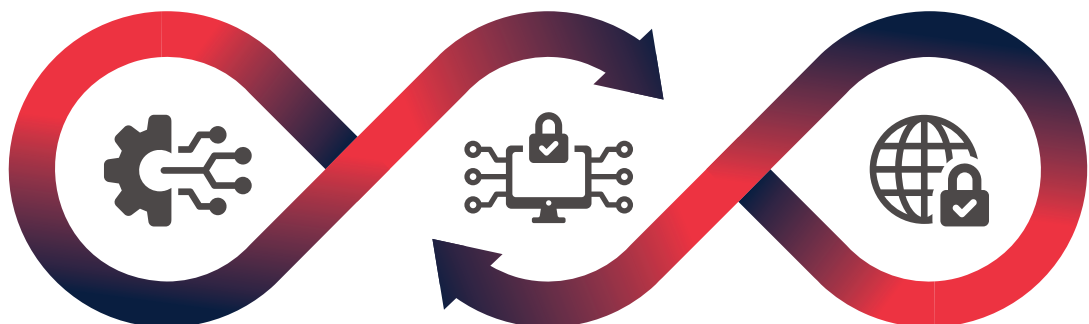
เป็นศูนย์กลางในการประสานความร่วมมือรวมทั้งส่งเสริม สนับสนุนและช่วยเหลือหน่วยงานภาครัฐและเอกชน ทั้งในประเทศและต่างประเทศ เพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์
Act as the central hub for collaboration, as well as promoting, supporting, and assisting national and international public and private agencies for cybersecurity.



4

เผยแพร่ความรู้ความเข้าใจและสนับสนุนการพัฒนาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
Disseminate knowledge, foster understanding, and support the development of cybersecurity personnel.

การขับเคลื่อนองค์กร ORGANIZATIONAL MANAGEMENT



TIER 1

- การสร้างความร่วมมือ
- การจัดทำมาตรฐาน แนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์
- Building cooperation
- Setting standards and guidelines on cybersecurity

TIER 2

- การขับเคลื่อนนโยบาย แผน มาตรฐานและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์
- การส่งเสริมงานวิจัยด้านความมั่นคงปลอดภัยไซเบอร์
- การพัฒนาขีดความสามารถหน่วยงานกลุ่มเป้าหมาย
- การยกระดับ ThaiCERT
- การสร้างการรับรู้และการตระหนักรู้ให้กับประชาชน
- การพัฒนาองค์กรสู่สมรรถนะสูง
- Driving forward cybersecurity policies, plans, standards, and practices
- Promoting cybersecurity research
- Developing the capabilities of the targeted organizations
- Elevating ThaiCERT
- Building public awareness and education
- Developing the organization to be high performance

TIER 3

- การพัฒนาและยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศตามมาตรฐานสากล
- Developing and elevating Thailand's cybersecurity capabilities to meet international standards

ประธานกรรมการ
Chairman



นายประเสริฐ จันทรรวงทอง
รองนายกรัฐมนตรี
และรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
Mr. Prasert Jantararungtong
Deputy Prime Minister
& Minister of Digital Economy and Society

กรรมการโดยตำแหน่ง
Committees by Position

นายภูมิธรรม เวชยชัย
รัฐมนตรีว่าการกระทรวงกลาโหม
Mr. Phumtham Wechayachai
Minister of Defence



นางพงษ์สวาท นีละโยธิน
ปลัดกระทรวงยุติธรรม
Mrs. Pongsawat Neelayothin
Permanent Secretary,
Ministry of Justice



นายประเสริฐ จันทรรวงทอง
รัฐมนตรีว่าการกระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม
Mr. Prasert Jantararungtong
Minister of Digital Economy
and Society



พลตำรวจเอก ต่อศักดิ์ สุขวิมล
ผู้บัญชาการตำรวจแห่งชาติ
Police General Torsak Sukvimol
Commissioner General, Royal Thai Police



นายลวรณ แสงสนิท
ปลัดกระทรวงการคลัง
Mr. Lavaron Sangsnit
Permanent Secretary,
Ministry of Finance



พลตำรวจเอก รอย อินทไพโรจน์
เลขาธิการสภาความมั่นคงแห่งชาติ
Police General Roy Inkapairoj
Secretary-General,
National Security Council



คณะกรรมการ การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) NATIONAL CYBER SECURITY COMMITTEE (NCSC)

กรรมการผู้ทรงคุณวุฒิ Honorary Committees

ดร.ปริญญ์ หอมเอนก

ด้านการรักษาความมั่นคง
ปลอดภัยไซเบอร์

Dr. Prinya Hom-anek

Expert Committee on Cyber Security



นายวิเชษฐ์ ตันติวานิช

ด้านการเงิน

Mr. Vichate Tantiwanich

Expert Committee on Finance

พลเอก มโน นุชเกษม

ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

General Mano Nuchkasem

Expert Committee on Information
Technology and Communications



นายแพทย์ดิเรก ทรัพย์สมบูรณ์

ด้านสาธารณสุข

Dr. Bordin Sapsomboon

Expert Committee on Public Health

พันตำรวจเอก ญาณพล ยั่งยืน

ด้านวิศวกรรมศาสตร์

Police Colonel Yanpol Yungyuen

Expert Committee on Engineering



รองศาสตราจารย์

ดร.ปณิธาน วัฒนายากร

ด้านความสัมพันธ์ระหว่างประเทศ

Associate Professor

Dr. Panitan Wattanayagorn

Expert Committee on
International Relations

ดร.ไพบุณย์ อมรภิญโญเกียรติ

ด้านกฎหมาย

Dr. Paiboon Aamonpingyokeat

Expert Committee on Legal Affairs



กรรมการและเลขาธิการ Committee member and Secretary



พลอากาศตรี ออม ชมเชย

เลขาธิการคณะกรรมการ

การรักษาความมั่นคงปลอดภัย

ไซเบอร์แห่งชาติ

AVM Amorn Chomchoey

Secretary-General,

National Cyber Security Committee

ประธานกรรมการ Chairman



นายประเสริฐ จันทรวงทอง
รองนายกรัฐมนตรี
และรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
Mr. Prasert Jantarauangtong
Deputy Prime Minister
& Minister of Digital Economy and Society

กรรมการโดยตำแหน่ง Committees by Position

นางเอกสิริ ปิณฑะรุจิ
ปลัดกระทรวงการต่างประเทศ
Mrs. Eksiri Pintaruchi
Permanent Secretary,
Ministry of Foreign Affairs



นายแพทย์โอภาส การย์กวินพงศ์
ปลัดกระทรวงสาธารณสุข
Dr. Opat Karnkawinpong
Permanent Secretary,
Ministry of Public Health



นายชัยธรรม พรหมศร
ปลัดกระทรวงคมนาคม
Mr. Chayatan Phromsorn
Permanent Secretary, Ministry of Transport



พลตำรวจเอก ต่อศักดิ์ สุขวิมล
ผู้บัญชาการตำรวจแห่งชาติ
Police General Torsak Sukvimol
Commissioner General, Royal Thai Police



ศาสตราจารย์พิเศษ
วิศิษฐ์ วิศิษฐ์สรอรรถ
ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
**Adjunct Professor
Wisit Wisitsora-At**
Permanent Secretary, Ministry of Digital
Economy and Society



พลเอก ทรงวิทย์ หุ่นภักดี
ผู้บัญชาการทหารสูงสุด
General Songwit Nunpakdee
Commander-in-Chief of the Armed Forces



ดร.ประเสริฐ สีนุขประเสริฐ
ปลัดกระทรวงพลังงาน
Dr. Prasert Sinsukprasert
Permanent Secretary, Ministry of Energy



พลตำรวจเอก รอย อังคไพโรจน์
เลขาธิการสภาความมั่นคงแห่งชาติ
Police General Roy Inkapairoj
Secretary-General,
National Security Council



นายสุภกริพงษ์ จุลเจริญ
ปลัดกระทรวงมหาดไทย
Mr. Suttipong Juljarern
Permanent Secretary, Ministry of Interior



นายฐนัต สุวรรณานนท์
ผู้อำนวยการสำนักข่าวกรองแห่งชาติ
Mr. Thanut Suvarnananda
The Director of National Intelligence Agency



คณะกรรมการ กำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กคม.) CYBERSECURITY REGULATING COMMITTEE (CRC)

กรรมการผู้ทรงคุณวุฒิ Honorary Committees

พลตำรวจตรี มนต์ชัย พันธุ์อัม
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
Police Major General Montien Pun-im
Expert Committee on Cyber Security



รองศาสตราจารย์ ดร.อติวงศ์ สุชาโต
ด้านวิศวกรรมศาสตร์
Assoc. Prof. Dr. Atiwong Suchato
Expert Committee on Engineering



**รองศาสตราจารย์
ดร.ยศชนัน วงศ์สวัสดิ์**
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
**Assoc. Prof.
Dr. Yodchanan Wongsawat**
Expert Committee on Information
Technology and Communications



นายปภาสิต เหลืองทอง
ด้านกฎหมาย
Mr. Pakasit Luangthong
Expert Committee on Legal Affairs



ดร.เศรษฐพุฒิ สุทธิวาทนฤพุฒิ
ผู้ว่าการธนาคารแห่งประเทศไทย
Dr. Sethaput Suthiwartnarueput
Governor of the Bank of Thailand



กรรมการและเลขานุการ Committee member and Secretary

**รองศาสตราจารย์
ดร.พรอนงค์ บุษราตระกูล**
เลขาธิการคณะกรรมการกำกับหลักทรัพย์
และตลาดหลักทรัพย์
**Assoc. Prof.
Dr. Pornanong Budsaratragoon**
Secretary-General, Office of the Securities
and Exchange Commission



นายไทรรัตน์ วิริยะศิริกุล
รองเลขาธิการ กสทช. รักษาการแทนเลขาธิการ
คณะกรรมการกิจการกระจายเสียงกิจการ
โทรทัศน์และกิจการโทรคมนาคมแห่งชาติ
Mr. Trairat Viriyasirikul
Deputy Secretary General,
Acting Secretary General,
The Office of the National Broadcasting and
Telecommunications Commission of Thailand



พลอากาศตรี อมร ชมเชย
เลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัย
ไซเบอร์แห่งชาติ
AVM Amorn Chomchoey
Secretary-General,
National Cyber Security Committee



ประธานกรรมการ Chairman



นายประเสริฐ จันทรรวงทอง
รองนายกรัฐมนตรี
และรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
Mr. Prasert Jantararungtong
Deputy Prime Minister
& Minister of Digital Economy and Society

กรรมการโดยตำแหน่ง Committees by Position

ศาสตราจารย์พิเศษ
วิศิษฐ์ วิศิษฐ์สรอรรถ
ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจ
และสังคม

**Adjunct Professor
Wisit Wisitsora-At**
Permanent Secretary, Ministry of
Digital Economy and Society



ดร.ปิยวัฒน์ ศิวรักษ์
เลขาธิการคณะกรรมการ
ข้าราชการพลเรือน
Dr. Piyawat Sivaraks
Secretary General,
Office of the Civil Service Commission

นางสาวกุลยา ตันติเตมิท
อธิบดีกรมบัญชีกลาง

Ms. Kulaya Tantitemit
Comptroller - General,
The Comptroller General's Department



นางสาวอ่อนฟ้า เวชชาชีวะ
เลขาธิการคณะกรรมการ
พัฒนาระบบราชการ
Ms. Onfa Vejajiva
Secretary-General,
Office of the Public Sector
Development Commission

กรรมการและเลขานุการ Committee member and Secretary

พลอากาศตรี อมร ชมชย
เลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัย
ไซเบอร์แห่งชาติ

AVM Amorn Chomchoey
Secretary-General,
National Cyber Security Committee



คณะกรรมการ บริหารสำนักงานคณะกรรมการ การรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.) COMMITTEE MANAGING THE NATIONAL CYBER SECURITY AGENCY (CMSA)

กรรมการผู้ทรงคุณวุฒิ Honorary Committees

ดร.ชัยชนะ มิตรพันธ์

ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

Dr. Chaichana Mitrpant

Expert Committee on Cyber Security



พลเอก กุชพงศ์ พงษ์ศิริ

ด้านสังคมศาสตร์

General Pushpong Pongsiri

Expert Committee on Social Sciences



รองศาสตราจารย์

สุรศักดิ์ สงวนพงษ์

ด้านเทคโนโลยีสารสนเทศ

และการสื่อสาร

Assoc. Prof.

Surasak Sanguanpong

Expert Committee on Information
Technology and Communications



นางแก้วใจ นาคสกุล

ด้านการบริหารจัดการองค์กร

Mrs. Kaewjai Nacsakul

Expert Committee on Organizational
Administration



รองศาสตราจารย์

ดร.เสาวณีย์ ไทยรุ่งโรจน์

ด้านเศรษฐศาสตร์

Assoc. Prof.

Dr. Sauwanee Thairungroj

Expert Committee on Economics



นายกฤษฎา บุญยมิต

ด้านกฎหมาย

Mr. Krisda Punyasmita

Expert Committee on Legal Affairs



การเข้าร่วมประชุมของ กบส.

PARTICIPATION IN THE MEETINGS OF THE CMSA

ครั้งที่ Meeting No.	ผู้เข้าร่วม Participants	ผู้ไม่เข้าร่วม Absentees	ร้อยละผู้เข้าร่วม Participation Rate (%)
5/2566	12	0	100
6/2566	12	0	100
1/2567	12	0	100
2/2567	12	0	100
3/2567	8	3	75
4/2567	12	0	100
5/2567	11	1	90
6/2567	10	2	80

ครั้งที่
MEETING 5
2566
2023

พิจารณาเรื่องการประเมินองค์กร และรายงานสรุป
ผลการดำเนินงานของการรักษาความมั่นคง
ปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญหรือแนวทางการพัฒนา
มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์
Focused on the evaluation of the organization and
a summary report on the significant impacts
of cybersecurity operations, along with strategies
for developing cybersecurity standards.



ครั้งที่
MEETING 6
2566
2023

พิจารณาเรื่องงบประมาณรายจ่ายประจำปีงบประมาณ
พ.ศ. 2567 ให้สอดคล้องกับแผนการปฏิบัติงาน
ประจำปีงบประมาณ พ.ศ. 2567 เพื่อขับเคลื่อนการดำเนินงานของ สกมช.
Focused on the FY2024 budget allocation to align with the
FY2024 operational plan, ensuring effective
implementation of the NCSA's initiatives.



ครั้งที่ 1
MEETING
2567
2024

พิจารณารายงานผลการดำเนินงานประจำปีของ สกมช. และรับทราบรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์ และผลการดำเนินงานด้านความร่วมมือเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์กับหน่วยงานด้านการต่างประเทศ

Reviewed the NCSA's annual performance report and acknowledged the report on cybersecurity incidents and the outcomes of international collaboration efforts to enhance cybersecurity.



ครั้งที่ 3
MEETING
2567
2024

พิจารณารายงานผลการดำเนินงานของ สกมช. เกี่ยวกับเป้าหมาย พร้อมทั้งสรุปปัญหา อุปสรรคและแนวทางการแก้ไข ระหว่าง 1 มีนาคม - 20 พฤษภาคม 2567 และรายงานผลการดำเนินงานตามยุทธศาสตร์และแผนปฏิบัติการ รอบ 6 เดือน

Reviewed the NCSA's performance report against set targets, including a summary of challenges, obstacles, and proposed solutions from March 1 to May 20, 2024. The meeting also examined the six-month performance report under the strategic and operational plans.



ครั้งที่ 5
MEETING
2567
2024

พิจารณาวาระแผนการปฏิบัติงานและแผนการใช้จ่ายงบประมาณ ประจำปีงบประมาณ พ.ศ. 2568 เพื่อขับเคลื่อนการดำเนินงานของ สกมช. ในการป้องกัน รับมือ และลดความเสี่ยงด้านไซเบอร์ ให้เป็นไปอย่างต่อเนื่องและมีประสิทธิภาพ

Focused on the FY2025 operational and budget expenditure plans to drive the NCSA's initiatives in preventing, responding to, and mitigating cyber risks effectively and consistently.



ครั้งที่ 2
MEETING
2567
2024

พิจารณาแผนการปฏิบัติงานและแผนการใช้จ่ายเงินงบประมาณ ประจำปีงบประมาณ พ.ศ. 2567 และ (ร่าง) แผนกลยุทธ์การบริหารและพัฒนาทรัพยากรบุคคลของ สกมช. ระยะ 4 ปี

Focused on reviewing the FY2024 operational and budget expenditure plans and the draft 4-year strategic plan for NCSA's human resource management and development.



ครั้งที่ 4
MEETING
2567
2024

พิจารณาแผนการบริหารจัดการ สกมช. ประจำปีงบประมาณ พ.ศ. 2568 และรับทราบผลการดำเนินงานที่สำคัญ เช่น การพัฒนานวัตกรรมในเชิงผลิตภัณฑ์และบริการของ สกมช. ประจำปีงบประมาณ พ.ศ. 2567 "Proactive Protection X Total Defense"

Reviewed the NCSA's management plan for FY2025 and acknowledged key achievements, including developing innovative products and services under the FY2024 initiative, "Proactive Protection X Total Defense."



ครั้งที่ 6
MEETING
2567
2024

พิจารณาทบทวนแผนบริหารสำนักงานตามนโยบายรัฐบาล แผนปฏิบัติการ ประจำปีงบประมาณ พ.ศ. 2568 พร้อมทั้งรับทราบรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์และการดำเนินการของ สกมช.

Reviewed the agency management plan in alignment with government policies and the FY2025 operational plan. The meeting also acknowledged the report on cybersecurity incidents and the actions taken by the NCSA.



คณะกรรมการและคณะอนุกรรมการ ที่ กบส. แต่งตั้ง

COMMITTEES AND SUBCOMMITTEES APPOINTED BY THE CMSA



คณะกรรมการตรวจสอบภายใน

- | | |
|---|---------------|
| 1. รองศาสตราจารย์ ดร. เสาวณีย์ ไทยรุ่งโรจน์ | ประธานกรรมการ |
| 2. พลเอก ภูษพงศ์ พงษ์ศิริ | กรรมการ |
| 3. นางพิลาสลักษณ์ ยุคเกษมวงศ์ | กรรมการ |
| 4. นางสาววศินี ธรรมศิริ | กรรมการ |
| 5. นางสาวณิชา ธนภัทรโชติศิริ | เลขานุการ |
- เจ้าหน้าที่กลุ่มปฏิบัติงานทั่วไปด้านตรวจสอบภายใน
รักษาการผู้อำนวยการฝ่ายตรวจสอบภายใน สกมช.



คณะอนุกรรมการด้านกฎหมาย

- | | |
|---------------------------------------|-------------------------------|
| 1. นายกฤษฎา บุญยสมบัติ | ประธานอนุกรรมการ |
| 2. นายพิชโรดม ลิ้มปิยะเชียร | อนุกรรมการ |
| ผู้แทนสำนักงานคณะกรรมการกฤษฎีกา | |
| 3. นายดามพ์ สุกนธทรัพย์ | อนุกรรมการ |
| 4. นายวรรณวิทย์ อาบูบุตร | อนุกรรมการ |
| 5. นางสาวกอบสิริ เอี่ยมสุรีย์ | อนุกรรมการ |
| 6. นางสาวดรุณี พิฤลทอง | อนุกรรมการและเลขานุการ |
| ผู้อำนวยการสำนักกฎหมาย สกมช. | |
| 7. นายสิริโชค ศิริโสภณ | อนุกรรมการและผู้ช่วยเลขานุการ |
| ผู้อำนวยการฝ่ายนิติกรรมและสัญญา สกมช. | |



คณะอนุกรรมการด้านการบริหารงานบุคคล

- | | |
|-------------------------------|-------------------------------|
| 1. นางแก้วใจ นาคสกุล | ประธานอนุกรรมการ |
| 2. นางนิธินุช จรุงเกียรติ | อนุกรรมการ |
| ผู้แทนสำนักงาน ก.พ.ร. | |
| 3. นางสาววิภาดา สิวะเฉลิมวงศ์ | อนุกรรมการ |
| 4. นายบวรนันท์ ทองกัลยา | อนุกรรมการ |
| 5. นางบุกิตา เลิศลักษณะพร | อนุกรรมการ |
| 6. พันตำรวจเอก ปัญญา สิงห์ไชย | อนุกรรมการและเลขานุการ |
| 7. นายสุกฤษฎีวัฒน์ โตสมบุญ | อนุกรรมการและผู้ช่วยเลขานุการ |



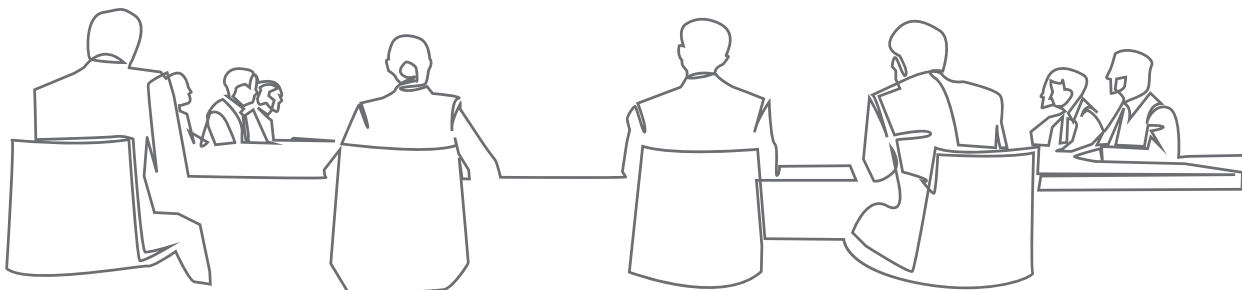
คณะอนุกรรมการด้านยุทธศาสตร์

- | | |
|---|-------------------------------|
| 1. ศาสตราจารย์พิเศษวิชาญ วิชาญสรอรรถ
ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม | ประธานอนุกรรมการ |
| 2. รองศาสตราจารย์สุรศักดิ์ สงวนพงษ์ | อนุกรรมการ |
| 3. ผู้แทนกรมบัญชีกลาง | อนุกรรมการ |
| 4. ดร.ชัยชนะ มีตรพันธ์ | อนุกรรมการ |
| 5. ผู้แทนสำนักงบประมาณ | อนุกรรมการ |
| 6. นายกำพล ศรณะรัตน์ | อนุกรรมการ |
| 7. พลอากาศตรี อมร ชมเชย สร.กมช. | อนุกรรมการ |
| 8. นางมัตติกา จงพิริยะอนันต์
ผู้อำนวยการสำนักการเงินและกลยุทธ์องค์กร สกมช. | อนุกรรมการและเลขานุการ |
| 9. นายปรเมศวร์ กุมารบุญ | อนุกรรมการและผู้ช่วยเลขานุการ |



คณะอนุกรรมการประเมินผลการปฏิบัติงานของเลขาธิการคณะกรรมการ การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

- | | |
|--------------------------------------|------------------|
| 1. ศาสตราจารย์พิเศษวิชาญ วิชาญสรอรรถ | ประธานอนุกรรมการ |
| 2. ดร.ชัยชนะ มีตรพันธ์ | อนุกรรมการ |
| 3. นางสาววิริยา เนตรน้อย | อนุกรรมการ |
| 4. พลอากาศตรี วุฒิกักร จันทรสาร | เลขานุการ |
| 5. นางสาวกมลพรรณ คงไข | ผู้ช่วยเลขานุการ |



คณะผู้บริหาร NCSA EXECUTIVES



พลอากาศตรี อมร ชมเชย

เลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัย
ไซเบอร์แห่งชาติ

AVM Amorn Chomchoey

Secretary-General
of the National Cyber Security Committee



พลตรี ธีรวุฒิ วิทยากรณ์

รองเลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัย
ไซเบอร์แห่งชาติ 4 และผู้อำนวยการ ThaiCERT

Maj. Gen. Teerawut Wittayakorn

Deputy Secretary-General 4 and
Director of ThaiCERT



① **พลเอก สุชาติ วงษ์มาก**
ผู้เชี่ยวชาญด้านการจัดการองค์กร
Gen. Suchart Wongmark
Expert on Organizational Administration

② **ผู้ช่วยศาสตราจารย์ ดร.วราภรณ์ พรหมวิกร**
ผู้ช่วยเลขาธิการ 1
Asst. Prof. Dr. Waraporn Promwikorn
Assistant Secretary-General 1

③ **นางกิงนภา บางชวด**
ผู้ช่วยเลขาธิการ 2
Mrs. Kingnapa Bangchaud
Assistant Secretary-General 2

④ **พลอากาศตรี จเด็จ กูทะก้องกิจ**
ผู้ช่วยเลขาธิการ 3
AVM Jadet Khuhakongkit
Assistant Secretary-General 3

⑤ **พลตรี ศทาวัตร ขจรกิตติยุทธ**
ผู้ทรงคุณวุฒิพิเศษ 1
Maj. Gen. Katavout Kajohonkittiyout
Senior Advisor 1

⑥ **นาวาเอกหญิง ศิริเนตร รักษ์วงศ์**
ผู้ทรงคุณวุฒิพิเศษ 2
Capt. Sirinate Rugvong WRTN
Senior Advisor 2

ผู้อำนวยการสำนัก NCSA DIRECTORS



① พันตำรวจเอก ปัญญา สิงห์ไชย

ผู้อำนวยการสำนักบริหารกลาง

Pol.Col. Panya Singchai

Director of Central
Administration Office

② นายภาณุพงษ์ ธนุกอง

รักษาการผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

Mr. Panupong Thanutong

Acting Director of Information Technology Office

③ นางชไมพร พงศ์พยุหะ

รักษาการผู้อำนวยการศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์

Mrs. Chamaiporn Pongpayuha

Acting Director of Cyber Security Research Center

④ พลอากาศตรี ดร.วุฒิบัทร จันทรสาร

ผู้อำนวยการสำนักนโยบายยุทธศาสตร์
การรักษาความมั่นคงปลอดภัยไซเบอร์

AVM Dr. Vuthibhatra Chansarn

Director of Cyber Security Strategy
and Policy Office

⑤ นางมัตติกา จงพิริยะอนันต์

ผู้อำนวยการสำนักการเงินและกลยุทธ์องค์กร

Mrs. Mattika Jongpiriyaanant

Director of Finance and Strategy Office



⑥ นางสาวดรุณี พิกุลทอง
ผู้อำนวยการสำนักกฎหมาย
Ms. Darunee Phikulthong
Director of Legal Office

⑦ พลอากาศตรี เฉลิมชัย วงษ์กฤต
ผู้อำนวยการสำนักบริหาร
โครงสร้างพื้นฐานสำคัญทางสารสนเทศ
AVM Chalerchai Wonggate
Director of Critical Information
Infrastructure Management Office

⑧ พันตรี ปวิช บุรพาชลทิต
รักษาการผู้อำนวยการสำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
Maj. Pawich Burapachonlatid
Acting Director of National Cyber Security Academy Office

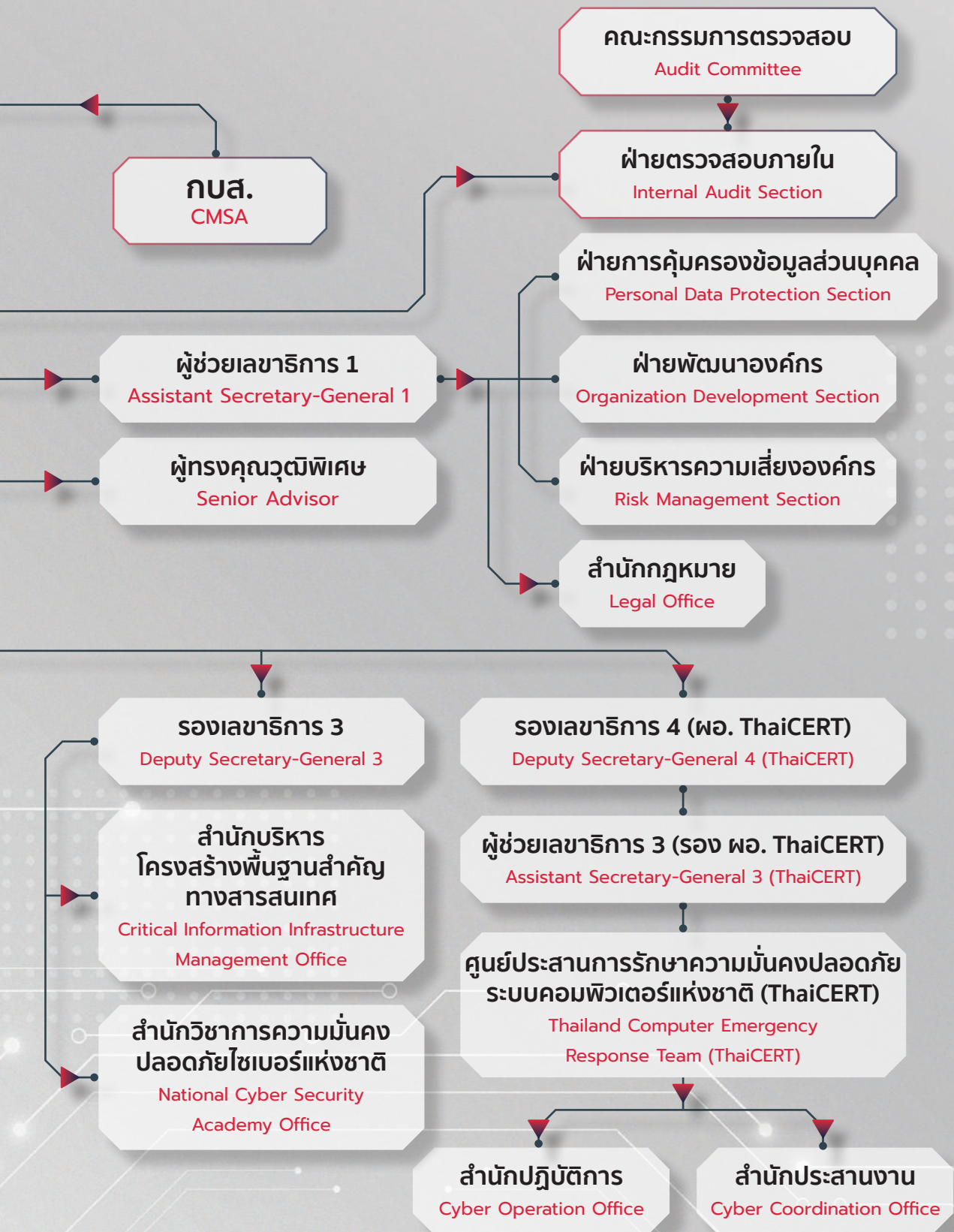
⑨ นางสาวสายชล แซ่ลี
ผู้อำนวยการสำนักประสานงาน
Ms. Salchon Saelee
Director of Cyber Coordination Office

⑩ พันตำรวจเอก ฌักกฤษ พรหมจันทร์
ผู้อำนวยการสำนักปฏิบัติการ
Pol. Col. Naughtakid Phromchan
Director of Cyber Operation Office

โครงสร้างองค์กร

CHART OF ORGANIZATION







ผลการดำเนินงาน OPERATIONAL PERFORMANCE HIGHLIGHTS

(รายงานตามนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. 2565 – 2570)

ยุทธศาสตร์ที่ 1



สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ ของประเทศ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Capacity)

Strategy 1: Building the Nation's Cybersecurity Capabilities
(Workforce, Knowledge, and Technology) (Capacity)

พัฒนาบุคลากรและสร้างความตระหนักรู้ด้านไซเบอร์
เสริมศักยภาพการป้องกันภัยคุกคามในทุกภาคส่วน
สนับสนุนการวิจัยและนวัตกรรมเพื่อลดการพึ่งพา
เทคโนโลยีต่างประเทศ พร้อมจัดฝึกซ้อมระดับประเทศ
เพื่อประเมินความพร้อม เสริมความมั่นคงปลอดภัยไซเบอร์
ในโครงสร้างพื้นฐานสำคัญของประเทศ

Develop cybersecurity workforce and raise public
awareness, enhance threat prevention capabilities
across all sectors, support research and innovation to
reduce reliance on foreign technologies, and conduct
national exercises to assess readiness, strengthening
cybersecurity in the country's critical infrastructure.



กลยุทธ์ที่ 1.1 : เพิ่มบุคลากรที่มีความสามารถ ด้านความมั่นคงปลอดภัยไซเบอร์

Strategy 1.1 : Increasing Skilled Cybersecurity Workforce

พัฒนาหลักสูตรความมั่นคงปลอดภัยไซเบอร์ ทั้งทฤษฎี และปฏิบัติ รองรับความต้องการภาคอุตสาหกรรม พร้อมพัฒนากักขะและฝึกอบรมบุคลากร ทั้งระดับผู้บริหาร และผู้ปฏิบัติงาน เพื่อเสริมศักยภาพด้านความมั่นคง ปลอดภัยไซเบอร์ของประเทศ

Develop specialized cybersecurity curricula, integrating theory and practice to meet industry needs. Enhance skills and provide training for cybersecurity personnel, including executives and operational staff, to strengthen capabilities in safeguarding national security.

กิจกรรมการส่งเสริมการจัดทำหลักสูตร และมาตรฐานวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ในระดับต่าง ๆ Promoting the Development of Cybersecurity Education and Professional Standards

ความสำเร็จในการพัฒนาหลักสูตรและส่งเสริมการศึกษา ด้านความมั่นคงปลอดภัยไซเบอร์ร่วมกับสถานศึกษา ภายในประเทศ 3 สถาบัน ได้แก่



หลักสูตรวิทยาศาสตรบัณฑิต
สาขาวิชาวิทยาการคอมพิวเตอร์
มหาวิทยาลัยกรุงเทพ



หลักสูตรวิทยาศาสตรบัณฑิต
สาขาวิชาการรักษาความมั่นคง
ปลอดภัยไซเบอร์
สถาบันการจัดการปัญญาภิวัฒน์



หลักสูตรวิทยาศาสตรบัณฑิต
สาขาวิชาความมั่นคงปลอดภัยไซเบอร์
มหาวิทยาลัยสวนดุสิต

Achievements include the development and promotion of cybersecurity education in collaboration with three academic institutions in Thailand:

- ▶ Bachelor of Science in Computer Science, Bangkok University
- ▶ Bachelor of Science in Cybersecurity, Panyapiwat Institute of Management
- ▶ Bachelor of Science in Cyber Security, Suankulabdee Rajavidyalaya



คณะวิทยาศาสตร์และเทคโนโลยี
มหาวิทยาลัยสวนดุสิต

หลักสูตรวิทยาศาสตรบัณฑิต
สาขาความมั่นคงปลอดภัยไซเบอร์

ปริญญาของหลักสูตร

หลักสูตรใหม่ พ.ศ. 2568

ผลิตบัณฑิตที่มีความรู้ ทักษะด้านความมั่นคงปลอดภัยไซเบอร์ มีคุณลักษณะที่ 5 ด้านตามกรอบมาตรฐาน
ซึ่งมีความสำคัญสูง เช่น การใช้การโจมตีทางไซเบอร์

จุดเด่นของหลักสูตร

- 1) ผู้มีความรู้ความเข้าใจด้านความมั่นคงปลอดภัยไซเบอร์
- 2) มีทักษะการปฏิบัติงานด้าน Security Operation Center (SOC)
- 3) มีความรู้เกี่ยวกับระบบสารสนเทศด้านความมั่นคงปลอดภัยไซเบอร์
- 4) มีความรู้ด้านกฎหมาย
- 5) มีความรู้เกี่ยวกับระบบสารสนเทศด้านความมั่นคงปลอดภัยไซเบอร์

วัตถุประสงค์ของหลักสูตร

- 1) มีความรู้ด้านความมั่นคงปลอดภัยไซเบอร์และหลักการการดำเนินงาน
- 2) มีทักษะการปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์
- 3) มีทักษะการปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์
- 4) มีความรู้เกี่ยวกับระบบสารสนเทศด้านความมั่นคงปลอดภัยไซเบอร์
- 5) มีความรู้เกี่ยวกับระบบสารสนเทศด้านความมั่นคงปลอดภัยไซเบอร์

อาชีพที่สามารถประกอบได้หลังสำเร็จการศึกษา

- 1) นักวิเคราะห์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operation Center Analyst)
- 2) นักวิเคราะห์ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Analyst)
- 3) นักปฏิบัติการทางไซเบอร์ (Cyber Incident Responder)
- 4) นักทดสอบความมั่นคงปลอดภัย (Penetration Tester)
- 5) นักตรวจสอบความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Auditor)

จำนวนหน่วยกิต 120 หน่วยกิต
สามารถจบได้ภายใน 3 ปีครึ่ง

095-897-4525, 086-362-8373 หรือ 02-244-5692 ถึง 4
https://cybersecurity.dusit.ac.th
หลักสูตรความมั่นคงปลอดภัยไซเบอร์ น.สวนดุสิต
cyber_security_sdu

กิจกรรมการเพิ่มขีดความสามารถบุคลากร สกมช. Enhancing NCSA Personnel Competencies

สกมช. ได้จัดกิจกรรมเพื่อปิดช่องว่างด้านทักษะ (Competency Gap) ของบุคลากร โดยมุ่งเน้นการพัฒนาความรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์และการใช้ภาษาอังกฤษอย่างมีประสิทธิภาพ ผ่านหลักสูตรฝึกอบรมและการทดสอบความสามารถต่างๆ ซึ่งมีการวัดผลโดยเฉลี่ยและพิจารณาจากอัตราการผ่านการอบรมในแต่ละหลักสูตร ดังนี้:

The NCSA has implemented activities to close the competency gap among its personnel, focusing on improving skills through three key training programs. The outcomes were evaluated based on the average scores and pass rates of participants in the following courses:



Certified Ethical Hacker (CEH)

หลักสูตรนี้อ้างอิงตามมาตรฐานระดับสากลของ EC-Council CEH โดยเน้นการฝึกอบรมให้บุคลากรมีทักษะในด้านการเจาะระบบอย่างมีจริยธรรม เพื่อทดสอบความปลอดภัยของระบบสารสนเทศและเครือข่าย โดยจำลองการโจมตีทางไซเบอร์เพื่อค้นหาช่องโหว่และป้องกันความเสี่ยงจากการโจมตีจริง

Certified Ethical Hacker (CEH) -

Advanced training in ethical hacking and cybersecurity.



CompTIA Cloud+ Certification

หลักสูตรนี้เน้นการพัฒนาทักษะที่จำเป็นในการใช้งาน ดูแล ปรับปรุง และแก้ไขปัญหาระบบโครงสร้างพื้นฐานที่ใช้คลาวด์ ช่วยให้บุคลากรสามารถจัดการระบบคลาวด์ได้อย่างมีประสิทธิภาพ

CompTIA Cloud+ Certification -

Skills for managing and optimizing cloud-based infrastructures.



TOEIC Simulation

การประเมินทักษะการใช้ภาษาอังกฤษผ่านการทดสอบจำลอง TOEIC โดยมีอัตราผู้ผ่านเกณฑ์เฉลี่ยอยู่ที่ร้อยละ 60 เพื่อเสริมความสามารถในการสื่อสารในบริบทสากล

TOEIC Simulation Test -

Assessment of language proficiency with a pass rate of 60%.



ยกระดับความพร้อมบุคลากรผู้เชี่ยวชาญ

การพัฒนาศักยภาพของบุคลากรที่มีบทบาทสำคัญในด้านความมั่นคงปลอดภัยไซเบอร์ เช่น ผู้เชี่ยวชาญเฉพาะทาง หรือบุคลากรที่มีหน้าที่หลักในการป้องกันและตอบสนองต่อภัยคุกคามไซเบอร์ เป็นอีกบทบาทสำคัญของ สกมช. ที่มีการดำเนินการอย่างต่อเนื่อง

- ▶ **Web 3.0 and Cybersecurity: Are You Prepared for the Internet Paradigm Shift?** วันที่ 25 มีนาคม 2567 สกมช. ร่วมกับสมาคมฟินเทคประเทศไทยและ Hellfire Security จัดเวทีเสวนา ณ SCBX Next Tech สยามพารากอน โดยมีผู้เชี่ยวชาญร่วมอภิปรายถึงโอกาสและความท้าทายของ Web 3.0 มีผู้เข้าร่วมกว่า **50 คน**
- ▶ **การอบรมเชิงปฏิบัติการด้าน Cloud Security** เมื่อวันที่ 24 เมษายน 2567 สกมช. และ Fortinet Thailand จัดการอบรมการออกแบบ Cloud ให้ปลอดภัยตามมาตรฐานสากล ณ The Office at Central World มีผู้เข้าร่วม **29 คน**
- ▶ การอบรมออนไลน์พื้นฐานด้านการเฝ้าระวังภัยไซเบอร์ เมื่อวันที่ 9 พฤษภาคม 2567 สกมช. และ Fortinet จัดการอบรมออนไลน์ผ่าน Zoom Webinar ในหัวข้อ “การตรวจสอบและเฝ้าระวังเหตุการณ์ภัยไซเบอร์ (Tier 1)” มีผู้เข้าร่วมกว่า **347 คน** พร้อมโอกาสเข้าร่วม Workshop เพิ่มเติมสำหรับผู้ผ่านการคัดเลือก
- ▶ **HCIA Security MOOC Course** ตั้งแต่วันที่ 11-25 เมษายน 2567 สกมช. และ Huawei Technologies จัดการอบรมออนไลน์หลักสูตร HCIA Security มีผู้เข้าร่วม **100 คน** และ **HCIA Security Hands-On Lab** ระหว่างวันที่ 9-10 พฤษภาคม 2567 ผู้เข้าร่วม **15 คน** ได้รับการคัดเลือกจาก **100 คน** ร่วมอบรมแบบลงมือปฏิบัติ ณ Huawei Training Center กรุงเทพฯ พร้อมรับ Voucher มูลค่า 200 ดอลลาร์สหรัฐสำหรับการสอบใบรับรอง HCIA Security
- ▶ **Cyber War Game Simulation** เมื่อวันที่ 8 สิงหาคม 2567 สกมช. และสำนักงานรัฐบาลดิจิทัล (DGA) ร่วมกันจัดกิจกรรม Cyber War Game Simulation ณ The Offices at Central World เพื่อเสริมทักษะการตอบสนองต่อภัยคุกคามทางไซเบอร์ มีผู้เข้าร่วมกว่า **30 คน** โดยมีการสนับสนุนระบบจาก Dnative Co., Ltd.



Enhancing the Readiness of Cybersecurity Experts

- ▶ **Web 3.0 and Cybersecurity:** Are You Prepared for the Internet Paradigm Shift? on March 25, 2024, the NCSA, in collaboration with the Thailand Fintech Association and Hellfire Security, hosted a seminar at SCBX Next Tech, Siam Paragon. **Over 50 participants** attended the session, which featured experts discussing the opportunities and challenges of Web 3.0.
- ▶ **Cloud Security Workshop:** On April 24, 2024, the NCSA and Fortinet Thailand organized a workshop on designing secure cloud systems compliant with international standards. **29 participants** attended the session at The Office at Central World.
- ▶ **Online Cyber Threat Monitoring Training:** On May 9, 2024, the NCSA and Fortinet hosted a Zoom Webinar titled **“Tier 1: Cyber Threat Monitoring and Incident Detection.”** The session attracted **over 347 participants**, with selected attendees allowed to join an advanced workshop.
- ▶ **HCIA Security 2024:** From April 11 to 25, 2024, the NCSA and Huawei Technologies offered the HCIA Security online course, with **100 participants** completing the program. From this group, 15 individuals were selected for the HCIA Security Hands-On Lab conducted on May 9–10, 2024, at Huawei Training Center, Bangkok. Participants also received a \$200 voucher for the HCIA Security certification exam.
- ▶ **Cyber War Game Simulation:** On August 8, 2024, the NCSA and the Digital Government Development Agency (DGA) co-hosted the Cyber War Game Simulation at The Offices at Central World. Supported by Dnative Co., Ltd., the event aimed to enhance participants' skills in responding to cyber threats. **Over 30 participants** joined the simulation to understand risk factors, develop response strategies, and improve decision-making in cybersecurity scenarios.



- ▶ **“หลักสูตร Lead Implementer และ Lead Auditor”** ระหว่างเดือนตุลาคมถึงพฤศจิกายน 2566 สกมช. ได้จัดอบรมเชิงปฏิบัติการ 6 รุ่น โดยมี**ผู้เข้าร่วม 321 คน** แบ่งเป็น หลักสูตรผู้นำการปฏิบัติ และ ผู้นำการตรวจสอบ เพื่อเสริมความเข้าใจด้านนโยบายมาตรฐาน และแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐานสากล ผู้เข้าร่วมที่ผ่านเกณฑ์มีโอกาสสอบรับรอง PECB ISMS Lead Implementer และ Lead Auditor



- ▶ อบรมเรื่อง **การป้องกันเว็บไซต์ถูกแฮ็กและการปรับแต่งเว็บไซต์เพื่อเพิ่มอันดับการค้นหา** โดย สกมช.เชิญวิทยากรจาก Google เช่น Gary Illyes ให้คำแนะนำด้านเทคนิคเชิงลึก มี**ผู้เข้าร่วมกว่า 50 คน**

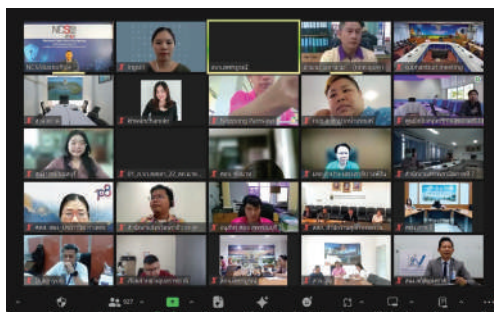


- ▶ **โครงการแลกเปลี่ยนความรู้ด้านไซเบอร์ระดับ Sectoral CERT** ระหว่างวันที่ 13-26 มิถุนายน 2567 สกมช. ร่วมมือกับ Cyberspace Administration of China (CAC) **นำผู้แทน 25 คน เข้าร่วมอบรม** เมืองกุ้ยหยาง ประเทศจีน โดยมุ่งเน้นเรื่อง AI, Big Data, การรักษาความปลอดภัยเครือข่าย และความร่วมมือระหว่างประเทศ รวมถึงศึกษาดูงานบริษัทเทคโนโลยีชั้นนำในจีน



- ▶ **Meta Verified & การป้องกัน Facebook** วันที่ 14 พฤศจิกายน 2567 สกมช. และ Meta จัดสัมมนาออนไลน์ให้หน่วยงาน**กว่า 1,000 คน** มุ่งเน้นการป้องกันบัญชี Facebook ของหน่วยงานจากการถูกแฮ็ก พร้อมแนะนำ Meta Verified เพื่อสร้างความน่าเชื่อถือ

- ▶ **เสริมสร้างความเข้าใจและวางแนวทางเฝ้าระวังภัยคุกคามทางไซเบอร์ในระบบ IT (Information Technology) และระบบ OT (Operational Technology)** กับ การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) ในวันที่ 18 มิถุนายน 2567 โดยมุ่งหวังให้เกิดการประสานสัมพันธ์ และเสริมสร้างความเข้าใจในการกิจที่สำคัญ รวมถึงการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ การสนับสนุนการเฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์ ที่นำมาซึ่งความร่วมมือภารกิจของทั้งสองหน่วยงานให้เป็นไปด้วยความเรียบร้อย

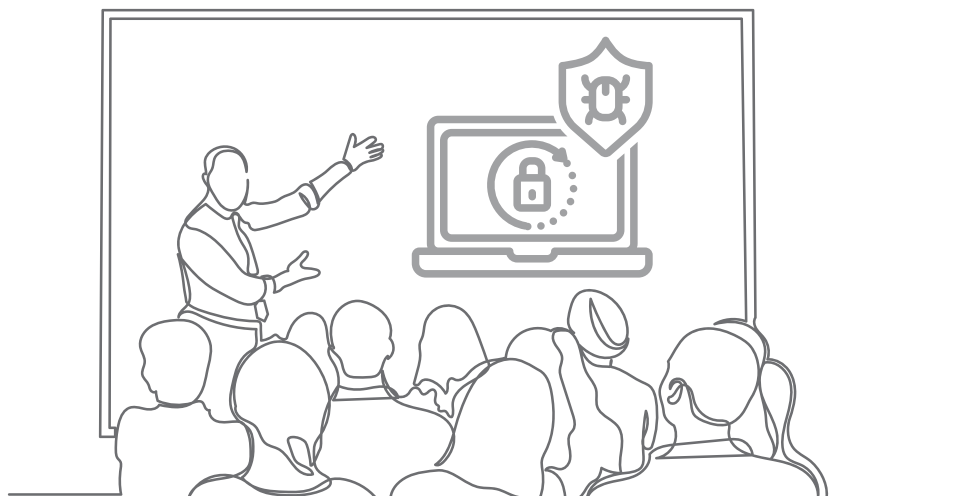


กิจกรรมทั้งหมดสะท้อนความมุ่งมั่นของ สกมช. ในการยกระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศทั้งในภาครัฐและเอกชน



- ▶ **Lead Implementer & Lead Auditor Courses:** From October to November 2023, the NCSA conducted six intensive workshops for regulators and CII personnel. **Three hundred twenty-one participants** completed the Lead Implementer and Lead Auditor courses, gaining insights into cybersecurity policies, standards, and compliance measures. Qualified participants were offered the opportunity to pursue PECB ISMS Lead Implementer and Lead Auditor certifications, further enhancing their expertise.
- ▶ **Cybersecurity and SEO Workshop:** On August 5, 2024, the NCSA organized a training session to combat website hacking and improve search engine rankings for **over 50 participants**. Google experts, including Gary Illyes, shared practical strategies for protecting websites, recovering from cyberattacks, and optimizing SEO.
- ▶ **Sectoral CERT Workshop & Study Tour:** From June 13–26, 2024, the NCSA partnered with China's Cyberspace Administration of China (CAC) to deliver a cybersecurity training program in Guiyang, Guizhou Province. **Twenty-five representatives** from government agencies, CII, and regulators gained hands-on experience in AI governance, cloud security, big data, and network protection.
- ▶ **Meta Verified & Facebook Account Security:** On November 14, 2024, the NCSA collaborated with Meta to host an online seminar attended by **over 1,000 participants** from public and private sectors. The session addressed preventative measures for protecting official Facebook accounts from hacking, emphasizing the importance of verifying for credibility and protection against impersonation.
- ▶ **Government Relations Workshop with EGAT:** On June 18, 2024, the NCSA engaged with the Electricity Generating Authority of Thailand (EGAT) to discuss enhancing cybersecurity for IT and OT systems. The collaboration aimed to align cyber threat monitoring and response strategies, fostering stronger partnerships between key agencies.

These activities underscore the NCSA's commitment to advancing the nation's cybersecurity capabilities across public and private sectors.



การพัฒนาหลักสูตรความมั่นคงปลอดภัยไซเบอร์ รองรับทุกระดับ

สกมช. มุ่งมั่นพัฒนาหลักสูตรความมั่นคงปลอดภัยไซเบอร์ทั้งภาคทฤษฎีและปฏิบัติ เพื่อตอบสนองความต้องการของภาคอุตสาหกรรม และยกระดับขีดความสามารถของบุคลากรในประเทศ โดยมีการดำเนินการที่สำคัญดังนี้:

- 1** **สำรวจและบูรณาการหลักสูตรความมั่นคงปลอดภัยไซเบอร์** เพื่อวางทิศทางการพัฒนาบุคลากรร่วมกับสถาบันการศึกษาและเครือข่ายพันธมิตร พร้อมให้การสนับสนุนทรัพยากรที่จำเป็นสำหรับการผลิตบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรงกับความต้องการของประเทศในอนาคต
- 2** **จัดทำความร่วมมือกับสถาบันคุณวุฒิวิชาชีพเพื่อรับรองหลักสูตรความมั่นคงปลอดภัยไซเบอร์ระดับพื้นฐาน (Cybersecurity Foundation Course)** โดยได้รับการประเมินและประกาศผลเป็นองค์กรที่ทำหน้าที่ให้บริการฝึกอบรม (Training Provider) เมื่อวันที่ 19 มกราคม 2567
- 3** **พัฒนาบุคลากรด้าน Cloud Security First** จัดประชุมร่วมกับสมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ และพันธมิตรจาก FORTINET, GOOGLE, HUAWEI และ EC-Council เมื่อวันที่ 25 ตุลาคม 2566 เพื่อพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ให้พร้อมรับมือกับเทคโนโลยี Cloud Security First ตามมาตรฐานสากล
- 4** **พัฒนาแพลตฟอร์มการเรียนรู้ออนไลน์ MOOC และ NCSA e-Learning** เปิดโอกาสการเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์ผ่านระบบ MOOC และ NCSA e-Learning ให้ผู้สนใจเรียนได้ทุกที่ทุกเวลา ปัจจุบันมีผู้เข้าใช้ระบบแล้วกว่า 10,832 คน ผ่านเว็บไซต์ www.nationalcyberacademy.ncsa.or.th/open-elearning และ www.mooc.ncsa.or.th
- 5** **พัฒนาสื่อการเรียนรู้ดิจิทัล “อุ่นใจไซเบอร์”** ร่วมกับ บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน) พัฒนาหลักสูตรสำหรับครู บุคลากรทางการศึกษา นักเรียน และประชาชนทั่วประเทศ เพื่อเข้าถึงสื่อการเรียนรู้ออนไลน์ผ่านแพลตฟอร์ม LearnDi for Thais (<https://learndiaunjaicyber.ais.co.th/>) ปัจจุบันมีผู้เข้าร่วมอบรมแล้วกว่า 199,747 คน (ข้อมูลเดือนสิงหาคม 2567)



Development of Cybersecurity Curriculum

The NCSA remains committed to developing theoretical and practical cybersecurity training programs to meet the demands of the industrial sector and enhance national workforce capabilities. Key initiatives include:

- 1. Survey and Integration of Cybersecurity Courses:** Conducting surveys to integrate cybersecurity education across institutions and networks to align with the country's future workforce requirements. NCSA also provides support to strengthen the production of skilled cybersecurity professionals.
- 2. Certification and Training Provider Accreditation:** Partnering with the **Thailand Professional Qualification Institute** to certify the **Cybersecurity Foundation Course** and gain recognition as a **Training Provider**.
- 3. Cloud Security First Workforce Development:** On October 25, 2023, NCSA collaborated with the **Cyber Innovation Promotion Association, FORTINET, GOOGLE, HUAWEI, and EC-Council** to enhance cybersecurity skills for professionals, mainly focusing on Cloud Security First initiatives.
- 4. Development of MOOC and NCSA e-Learning Platforms:** NCSA launched online platforms **MOOC** and **NCSA e-Learning**, enabling flexible access to cybersecurity training anytime, anywhere. Over **10,832 participants** have accessed the platforms via www.nationalcyberacademy.ncsa.or.th/open-e-learning and www.mooc.ncsa.or.th.
- 5. Digital Learning Content: Aunjai Cyber** Partnering with **Advanced Info Service (AIS)**, NCSA developed **Aunjai Cyber** program to provide online cybersecurity education for teachers, students, and the general public. As of **August 2024**, over **199,747 participants** have completed the training via the **LearnDi for Thais** platform (<https://learndiaunjaicyber.ais.co.th/>).



กลยุทธ์ที่ 1.2 : สร้างความตระหนักรู้และสร้างทักษะ ด้านความมั่นคงปลอดภัยไซเบอร์ Strategy 1.2 : Building Awareness and Skills in Cybersecurity

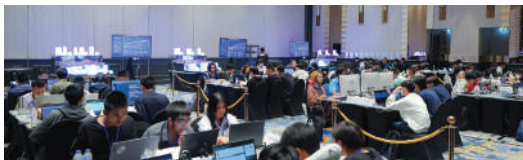
สร้างความตระหนักรู้และความเข้าใจด้านความมั่นคงปลอดภัยไซเบอร์ พร้อมส่งเสริมการบูรณาการหลักสูตรการตระหนักรู้และพัฒนาทักษะด้านความมั่นคงปลอดภัยไซเบอร์ในระบบการศึกษาทุกระดับ

Promote cybersecurity awareness and understanding while encouraging the integration of cybersecurity awareness and skill development curricula into all levels of the education system.

กิจกรรมการสร้างความรู้และพัฒนาศักยภาพเกี่ยวกับภัยคุกคามทางด้านไซเบอร์ (Cyber Top Talent) และแนะแนวอาชีพทางการรักษาความมั่นคงปลอดภัยไซเบอร์

สทศ. จัด **Thailand Cyber Top Talent 2024** รอบคัดเลือก เมื่อวันที่ 28 กันยายน 2567 เพื่อพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์และแนะแนวอาชีพให้กับนักเรียน นิสิต นักศึกษา และประชาชน โดยมีผู้สมัครกว่า **2,400 คน 846 ทีม**

การแข่งขันรอบชิงชนะเลิศจัดขึ้นในวันที่ 12 ตุลาคม 2567 ในรูปแบบ Attack the Virtual World ที่เพิ่มความท้าทายด้วยโจทย์ในส่วนของระบบ IoT และ OT Security โดยทีมชนะเลิศจะเป็นตัวแทนประเทศไทยใน **Cyber SEA Game 2024**



NCSA organized the **Thailand Cyber Top Talent 2024** qualifiers on September 28, 2024, to enhance cybersecurity skills and career pathways for students and the public. Over 2,400 participants in 846 teams.

The final round, held on October 12, 2024, featured the **Attack the Virtual World** challenge, incorporating IoT and OT Security scenarios. The champions will represent Thailand in the **Cyber SEA Game 2024**.



โครงการสัมมนาเชิงปฏิบัติการสำหรับหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ประจำปีงบประมาณ พ.ศ. 2567 (NCSA Cyber Clinic 2024)

การจัดสัมมนาผ่านสื่ออิเล็กทรอนิกส์ **6 ครั้ง** ผู้เข้าร่วม **651 คน** จากหน่วยงาน Regulator (19 หน่วยงาน)
CII (63 หน่วยงาน) หน่วยงานอื่น ๆ (25 หน่วยงาน) และประชาชนทั่วไป ในหัวข้อ



แนวทางการแจ้งเตือนเหตุภัยคุกคาม
และการรายงาน สำหรับหน่วยงาน
ควบคุมหรือกำกับดูแล หน่วยงาน
ของรัฐ และหน่วยงานโครงสร้าง
พื้นฐานสำคัญทางสารสนเทศ



Proactive Protection & Total
Defense ปีชงแค่ไหนก็ไปหวัน
เพราะเราล่อมคอกก่อนวัวหาย



ภาพรวมของกฎหมายลำดับรอง
ทั้งหมดที่เกี่ยวข้องกับการดำเนินงาน
สำหรับหน่วยงานควบคุมหรือ
กำกับดูแล หน่วยงานของรัฐ และ
หน่วยงานโครงสร้างพื้นฐานสำคัญ
ทางสารสนเทศ



CCAPAC Workshop: Cybersecurity
Trends in Policymaking 2024
การประชุมเชิงปฏิบัติการ CCAPAC:
แนวโน้มความปลอดภัยทางไซเบอร์
ในการกำหนดนโยบาย ปี 2024



แนวทางการจัดทำกรอบการบริหาร
ความเสี่ยงด้านความมั่นคงปลอดภัย
ไซเบอร์ของหน่วยงานให้สอดคล้อง
กับนโยบายบริหารจัดการที่เกี่ยวกับ
การรักษาความมั่นคงปลอดภัย
ไซเบอร์สำหรับหน่วยงานของรัฐ และ
หน่วยงานโครงสร้างพื้นฐานสำคัญ
ทางสารสนเทศ ตามประกาศ กมช.
เรื่อง นโยบายและแผนปฏิบัติการ
ว่าด้วยการรักษาความมั่นคงปลอดภัย
ไซเบอร์ (พ.ศ. 2565 - 2570)



มาตรฐานคลาวด์บอกให้ประเมินและ
จัดระดับผลกระทบ สูง กลาง ต่ำ
แล้วหน่วยงานจะอย่างไร



The NCSA Cyber Clinic
2024 conducted six virtual
workshops, engaging
651 participants from 19
Regulators, 63 CII agencies,
25 other organizations,
and the public. Key topics
included Cyber Threat Alerts
and Reporting, Proactive
Protection & Total Defense
Strategies, among others.

โครงการอบรม NCSA Cybersecurity Knowledge Sharing 2567

การสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์แก่ประชาชนทุกช่วงวัยผ่านรูปแบบออนไลน์ เป็นกิจกรรมที่จัดมาต่อเนื่องทุกปี เพื่อเสริมสร้างความรู้เกี่ยวกับภัยไซเบอร์ การป้องกัน และเทคโนโลยีใหม่ ๆ ทำให้ผู้สนใจในหัวข้อต่าง ๆ ที่จัดขึ้นตลอดทั้งปี สามารถเข้าถึงเนื้อหาได้ทุกที่ทุกเวลา ในปีนี้มี**ผู้เข้าร่วม 28,680 คน** โดย**ผู้ผ่านเกณฑ์ร้อยละ 60 มีจำนวน 24,906 คน (คิดเป็นร้อยละ 89.22)** ใน 10 หัวข้อน่าสนใจคือ

- | | | | |
|----------|--|-----------|---|
| 1 | เจาะลึกกลยุทธ์การดำเนินงาน Implementing Zero Trust Architecture (ZTA) และการกำหนดนโยบาย Zero Trust ขององค์กร | 6 | แนะนำ NIST Cybersecurity Framework 2.0 Version ล่าสุด |
| 2 | การสร้างสมดุลระหว่างความมั่นคงปลอดภัยไซเบอร์และความเป็นส่วนตัวของข้อมูล | 7 | Short link สำคัญอย่างไร?...กับความมั่นคงปลอดภัยไซเบอร์ |
| 3 | คู่มือความสำเร็จขององค์กรในการบริหารความเสี่ยงที่เกิดจากปัจจัยภายนอก | 8 | สื่อลามกอนาจารเด็ก (CSAM) ในประเทศไทย และแนวทางป้องกันการล่วงละเมิดทางเพศต่อผู้หญิงและเด็กทางอินเทอร์เน็ต |
| 4 | รอบรู้เรื่อง Digital Forensic พร้อมการรับมือกับ Advanced Threat และ Social Media | 9 | ภัยร้ายที่ไม่ควรมองข้าม!!!...กับพฤติกรรมแฝงเพื่อละเมิดทางเพศเด็ก (Child Grooming) |
| 5 | การออกแบบและใช้งาน Cloud อย่างปลอดภัยตามมาตรฐานสากล | 10 | แอปดูดเงินมหาภัย ผู้สูงวัยใส่ใจไม่ตกเป็นเหยื่อ |



This **NCSA Cybersecurity Knowledge Sharing 2024** online program series enhances cybersecurity awareness for all ages, featuring topics like zero trust architecture, cloud security, and digital forensics. With **28,680 participants**, 89.22% passed the 60% threshold, gaining practical skills to address cyber threats and strengthen security at all levels.



การแข่งขัน Cyber SEA Game 2024

สทศ. ร่วมกับศูนย์ ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) ในนามประเทศไทยเป็นเจ้าภาพจัดการแข่งขัน **Cyber SEA Game 2024** ซึ่งจัดขึ้นระหว่างวันที่ 24 - 25 ตุลาคม 2567 โดยมีทีมจาก **10 ประเทศสมาชิกอาเซียน**เข้าร่วมการแข่งขัน

การแข่งขันนี้มุ่งพัฒนาศักยภาพและประสบการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ให้นักศึกษาจากอาเซียน เพื่อเตรียมความพร้อมสู่การเป็นบุคลากรผู้เชี่ยวชาญในอนาคต ทั้งนี้ ทีมชนะเลิศได้เหรียญทอง จะได้รับโอกาสศึกษาดูงานด้านความมั่นคงปลอดภัยไซเบอร์ที่ญี่ปุ่น

Competition Results:



Gold Medal: Singapore



Silver Medal: Vietnam



Bronze Medal: Indonesia

In collaboration with the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC), NCSA proudly hosted the **Cyber SEA Game 2024** on October 24-25, 2024, welcoming teams from 10 ASEAN member countries.

The competition aimed to enhance cybersecurity skills and provide hands-on experience for ASEAN students, preparing them to become skilled professionals for the future workforce.



กิจกรรมจัดการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ ปี 2567 (Thailand's National Cyber Exercise 2024)

สทท. จัดการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ **Thailand's National Cyber Exercise 2024** เพื่อเสริมสร้างความพร้อมในการป้องกันและรับมือภัยคุกคามไซเบอร์อย่างมีประสิทธิภาพ โดยเริ่มต้นด้วยการฝึกเตรียมการ (Pre-Exercise/Academic) **สอบ Basic** ระหว่างวันที่ 6-7 พฤศจิกายน 2567 ผ่านสื่ออิเล็กทรอนิกส์ โดยมีหน่วยงานเข้าร่วมจำนวน 140 หน่วยงาน มีผู้เข้าร่วมกว่า 600 คน



ผู้ผ่านการคัดเลือกในรอบ Basic ได้เข้าร่วมการฝึก Pre-Exercise **สอบ Advanced** ในวันที่ 25-26 พฤศจิกายน 2567 มีหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมไปถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง เข้าร่วมการอบรมในครั้งนี้รวมทั้งสิ้น **114 คน**

และเข้าสู่ **การฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ (Command Post Exercise: CPX) วันที่ 19-20 ธันวาคม 2567** มีหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงาน Sectoral CERT และ ThaiCERT **เข้าร่วมการฝึก 158 หน่วยงาน โดยมีผู้เข้าร่วมการฝึกกว่า 1,000 คน** ซึ่งนับเป็นการฝึกฯ ครั้งยิ่งใหญ่แห่งปีที่ทุกหน่วยงานจะได้ร่วมฝึกกำลังยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับประเทศต่อไป

กิจกรรมครั้งนี้เน้นย้ำถึงความสำคัญของการร่วมมือกันเพื่อป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ พร้อมผลักดันให้ประเทศไทยมีความมั่นคงทางไซเบอร์ในทุกมิติ





Thailand's National Cyber Exercise 2024

NCSA conducted the **Thailand's National Cyber Exercise 2024** to enhance readiness and effectiveness in preventing and responding to cyber threats. The program commenced with the Pre-Exercise/Academic (Basic Round) held on November 6-7, 2024, through online platform with **over 600 participants from 140 organizations**.

Participants who passed the Basic Round advanced to the Pre-Exercise Advanced Round, held on November 25-26, 2024. This session included **114 participants** from government agencies, regulators, organizations of critical information infrastructure, and other related entities.

The final Thailand's National Cyber Exercise 2024 took place on December 19-20, 2024, **more than 1,000 participants** from **158 organizations**, including government agencies, regulators, organizations of critical information infrastructure, Sectoral CERTs, and ThaiCERT, joined this large-scale training exercise. This significant event of the year symbolizes a collaborative effort among all organizations to strengthen and elevate the cybersecurity posture of the nation.

This initiative was supported by government agencies, regulators, and organizations of critical information infrastructure. It emphasized the importance of collaboration to prevent, mitigate, and respond to cyber threats while strengthening Thailand's cybersecurity resilience across all dimensions.

การยกระดับศักยภาพและความพร้อมของผู้หญิง ด้านความมั่นคงปลอดภัยไซเบอร์และ ICT

ตลอดระยะเวลาที่ผ่านมา สกช. ได้มุ่งมั่นในการส่งเสริมและสนับสนุนผู้หญิงและกลุ่มผู้มีความหลากหลายทางเพศ ให้มีโอกาสพัฒนาทักษะ เพิ่มพูนความรู้ และแสดงศักยภาพในสายงานด้านความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศ ผ่านโครงการและกิจกรรมต่าง ๆ

- 1 การแข่งขัน Women Thailand Cyber Top Talent 2023** สกช. ร่วมกับ บริษัท หัวเว่ย เทคโนโลยี (ประเทศไทย) จำกัด จัดการแข่งขัน Women Thailand Cyber Top Talent 2023 เพื่อค้นหาผู้มีทักษะด้านความมั่นคงปลอดภัยไซเบอร์ในกลุ่มผู้หญิงและเพศสภาพเป็นหญิง การแข่งขันรอบคัดเลือกแบบออนไลน์ มีทีมเข้าร่วมแข่งขันทั้งสิ้น 218 ทีม รวมผู้เข้าแข่งขันกว่า 407 คน แบ่งออกเป็น 3 ระดับ ได้แก่ ระดับนักเรียน (Junior): 92 ทีม ระดับนักศึกษา (Senior): 71 ทีม และระดับประชาชนทั่วไป (Open): 55 ทีม และรอบชิงชนะเลิศ จัดขึ้นเมื่อวันที่ 27 ธันวาคม 2566 ซึ่งเป็นเวทีที่แสดงความสามารถด้านไซเบอร์ของผู้หญิง พร้อมสร้างแรงบันดาลใจให้กับผู้สนใจในสายงานนี้



- 2 งาน Girls in ICT 2024** จัดขึ้นโดย สกช. หัวเว่ย เทคโนโลยี (ประเทศไทย) ร่วมกับ สหภาพโทรคมนาคมระหว่างประเทศ (ITU) เมื่อวันที่ 30 พฤษภาคม 2567 งานนี้เน้นการ ลดความเหลื่อมล้ำ และ ส่งเสริมการมีส่วนร่วมของผู้หญิงในสาขาเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อผลักดันผู้หญิงให้ก้าวสู่บทบาทสำคัญในอุตสาหกรรมเทคโนโลยี



ทั้งสองกิจกรรมแสดงให้เห็นถึงความมุ่งมั่นของ สกช. ในการสร้างความเท่าเทียม พัฒนาทักษะ และเสริมศักยภาพผู้หญิงในด้านความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยี ผ่านการส่งเสริมการเรียนรู้และการสร้างแรงบันดาลใจ กิจกรรมเหล่านี้ถือเป็น ก้าวสำคัญในการลดช่องว่างทางเพศ และสนับสนุนผู้หญิงให้ก้าวสู่ความสำเร็จในยุครัตนโกสินทร์ที่ 250 ปี

Empowering Women in Cybersecurity and ICT

The NCSA remains committed to empowering women and gender-diverse individuals in the cybersecurity and ICT sectors. By fostering confidence, skill development, and learning opportunities, the NCSA aims to unlock women's full potential in these critical fields.

- 1. Women Thailand Cyber Top Talent 2023:** To inspire and empower women in cybersecurity, the NCSA, in collaboration with Huawei Technologies (Thailand), hosted the Women Thailand Cyber Top Talent 2023 competition. This initiative focused on identifying and nurturing cybersecurity talent among women and gender-diverse individuals across the country. The online preliminary round saw participation from **218 teams (over 407 participants)** across three categories: Junior Level: 92 teams (students), Senior Level: 71 teams (university students) & Open Level: 55 teams (public). The final round occurred on December 27, 2023, where top teams showcased their cybersecurity skills. This competition highlighted women's talents in cybersecurity and inspired greater participation and representation in this dynamic and essential field.
- 2. Girls in ICT 2024:** On May 30, 2024, the NCSA, Huawei Technologies (Thailand), and the International Telecommunication Union (ITU) organized an event to inspire young women to develop digital skills and explore opportunities in the ICT sector. Girls in ICT emphasized addressing gender inequality, fostering inclusion, and empowering women to take on leadership roles in the ICT industry. The event created a pathway for women to excel in the digital age by reducing barriers and promoting access to technology.

The NCSA's ongoing commitment to empowering women through initiatives like Women Thailand Cyber Top Talent and Girls in ICT reflects its dedication to fostering equality, skills development, and opportunity for women in cybersecurity and ICT.



กิจกรรมเพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ให้กับกลุ่มเปราะบางและผู้สูงอายุ

สกมช. ได้ดำเนินกิจกรรมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้กับกลุ่มเปราะบางและผู้สูงอายุ โดยจัดการอบรมและบรรยายที่ตอบโจทย์เฉพาะกลุ่ม ได้แก่

- ▶ การอบรมหลักสูตร “ความปลอดภัยทางไซเบอร์ (Cyber Security)” ให้กับกลุ่มเปราะบาง ในสถานพินิจ 10 แห่ง เมื่อวันที่ 17 พฤศจิกายน 2566 โดยมีผู้เข้าร่วม 96 คน
- ▶ การบรรยาย “การสร้างการรับรู้เท่าทันภัยทางดิจิทัล” ร่วมกับ สกสท. และกรมสุขภาพจิต เมื่อวันที่ 20 ธันวาคม 2566 โดยมีกลุ่มเป้าหมายที่เข้ารับฟังการบรรยาย ได้แก่ กลุ่มคนพิการ ผู้สูงอายุ และผู้ด้อยโอกาสที่อยู่ในพื้นที่โครงการจัดให้มีบริการโทรคมนาคมโดยทั่วถึงและในพื้นที่ชายขอบและพื้นที่ห่างไกล โดยมีการ Conference ไปยังศูนย์อินเทอร์เน็ตสาธารณะ ของโครงการฯ มากกว่า 2,184 แห่ง ผ่านการประชุมออนไลน์
- ▶ กิจกรรม “Show and Share: Learning to Live Together” สำหรับเด็กและเยาวชนจากสถานพินิจ 8 แห่ง เมื่อวันที่ 22 มิถุนายน 2567 มีผู้เข้าร่วมกว่า 100 คน
- ▶ โครงการสัมมนาเตรียมตัวก่อนเกษียณบุคคลากร พม. ประจำปี 2567 เพื่อส่งเสริมให้บุคลากรในสังกัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ (พม.) ตระหนักและเตรียมความพร้อมเข้าสู่วัยสูงอายุอย่างมีคุณภาพ และสามารถนำความรู้ที่ได้รับไปปรับใช้เป็นแนวปฏิบัติในการดำเนินชีวิตในอนาคต โดยมีกลุ่มเป้าหมายในสังกัด พม. ที่มีอายุระหว่าง 50-59 ปี และผู้ที่เกษียณอายุราชการในปี 2567 แบ่งเป็น 2 รุ่น โดยรุ่นที่ 1 มีผู้เข้าร่วม 150 คน จัดขึ้นระหว่างวันที่ 14-16 สิงหาคม 2567 และรุ่นที่ 2 มีผู้เข้าร่วม 170 คน จัดขึ้นระหว่างวันที่ 28-30 สิงหาคม 2567
- ▶ การอบรมหัวข้อ “การสร้างความรู้และแนวทางการศึกษาเพื่อพัฒนาอาชีพด้านความมั่นคงปลอดภัยไซเบอร์ ปีที่ 2” ร่วมกับมูลนิธิพระมหาไถ่เพื่อการพัฒนาคนพิการ ให้กับนักเรียนและเครือข่ายคนพิการที่สนใจ จำนวน 200 คน และการอบรม “Training of Thailand Cyber Top Talent 2024” ให้กับนักเรียนเพื่อเข้าแข่งขัน Thailand Cyber Top Talent 2024 ในวันศุกร์ที่ 13 กันยายน 2567

กิจกรรมเหล่านี้เป็นส่วนหนึ่งของความมุ่งมั่นของ สกมช. ในการเสริมสร้างความรู้และความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ในคนทุกกลุ่ม เพื่อให้พวกเขาสามารถปกป้องตนเองจากภัยคุกคามทางไซเบอร์ และใช้เทคโนโลยีอย่างมั่นคงปลอดภัยและมีประสิทธิภาพ



Cybersecurity Awareness Activities for Vulnerable Groups and the Elderly

The NCSA has undertaken initiatives to raise cybersecurity awareness among vulnerable groups and older people through tailored training sessions and lectures, including:

- ▶ **Cybersecurity Training Course:** Conducted for vulnerable groups in 10 juvenile detention centers on November 17, 2023, with **96 participants**.
- ▶ Lecture on **“Digital Threat Awareness”**: Organized in collaboration with the NBTC and the Department of Mental Health on December 20, 2023. The target audience included persons with disabilities, the elderly, and underprivileged individuals residing in remote and underserved areas under the Universal Telecommunications Service project. The event reached **over 2,184 public internet centers** nationwide via online conferencing.
- ▶ **“Show and Share: Learning to Live Together” Event:** **Over 100 participants** attended the event, which was held for children and youths from 8 juvenile detention centers on June 22, 2024.
- ▶ **Pre-Retirement Seminar for M-Society Personnel 2024:** This seminar aimed at promoting awareness and preparedness for quality aging among personnel from the Ministry of Social Development and Human Security (M-Society). It targeted individuals aged 50-59 and those retiring in 2024. Two sessions were held: the first session, with **150 participants**, from August 14-16, 2024, and the second, with **170 participants**, from August 28-30, 2024.
- ▶ Training on **“Cybersecurity Awareness and Career Path Development Year 2”**: Organized in collaboration with the Redemptorist Foundation for People with Disabilities, this session trained **200 students** and disability networks interested in cybersecurity careers. The “Training of Thailand Cyber Top Talent 2024” also prepared students for the Thailand Cyber Top Talent 2024 competition on September 13, 2024.

These activities are part of the NCSA's ongoing commitment to enhancing cybersecurity knowledge and awareness across all groups, empowering individuals to protect themselves from cyber threats and use technology securely and effectively.



กลยุทธ์ที่ 1.3 : ส่งเสริมการวิจัยและพัฒนานวัตกรรม ด้านความมั่นคงปลอดภัยไซเบอร์ Strategy 1.3 : Promoting Cybersecurity Research and Innovation

มุ่งเน้นส่งเสริมการศึกษา วิจัย และพัฒนานวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์ เสริมสร้างความร่วมมือระหว่างหน่วยงานวิจัย ส่งเสริมการลงทุนในเทคโนโลยีความมั่นคงปลอดภัยไซเบอร์ และส่งเสริมการพัฒนาผลิตภัณฑ์ที่สามารถต่อยอดเชิงพาณิชย์ได้อย่างยั่งยืน

Focusing on promoting education, research, and innovation in cybersecurity, strengthening collaboration among research agencies, encouraging investment in cybersecurity technologies, and supporting the development of products that can be sustainably commercialized.

กิจกรรมการจัดทำและปรับปรุงฐานข้อมูลผู้ให้บริการ และผู้ประกอบการภาคอุตสาหกรรมด้านความมั่นคงปลอดภัยไซเบอร์

สทศ. ได้ดำเนินการพัฒนาระบบบริหารและจัดการฐานข้อมูลผู้ให้บริการและผู้ประกอบการภาคอุตสาหกรรมด้านความมั่นคงปลอดภัยไซเบอร์ โดยมีการออกแบบแนวคิดและรายละเอียดระบบงาน พร้อมจัดทำ Mock-up ของระบบทั้งหมด เพื่อให้สอดคล้องกับกรอบคุณลักษณะของฐานข้อมูลที่กำหนดไว้



Development and Improvement of the Cybersecurity Industry Database

Efforts are underway to develop a management system for the cybersecurity industry database, including service providers and operators. The system's design concept and detailed specifications have been completed, along with a full Mock-up of the system, ensuring alignment with the key attributes outlined for the database.



กิจกรรมส่งเสริมและสนับสนุนผู้ประกอบการภาคอุตสาหกรรมด้านความมั่นคงปลอดภัยไซเบอร์ภายในประเทศ เพื่อลดการพึ่งพาเทคโนโลยีจากต่างประเทศ

สททช. โดย ศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์ สนับสนุนและผลักดันให้เกิดผลิตภัณฑ์และการให้บริการในภาคอุตสาหกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีความร่วมมือกับ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) มาอย่างต่อเนื่อง เพื่อส่งเสริมการนำผลงานวิจัยและพัฒนาของไทยไปใช้ในการปฏิบัติงาน

ผลงานที่โดดเด่นในปี 2567 คือการผลักดันให้ผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์อย่าง **Cost-Efficient Open-Source SOC Platform** ซึ่งวิจัยและพัฒนาโดย NECTEC ได้มีการนำไปใช้ใน ศูนย์ประสานงานการรักษาความปลอดภัยไซเบอร์แห่งสาธารณรัฐประชาธิปไตยประชาชนลาว (LaoCERT) และหน่วยงานที่ต่าง ๆ ในสาธารณรัฐประชาธิปไตยประชาชนลาว รวมถึงความร่วมมือในการพัฒนาความรู้และทักษะของบุคลากรในการยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ระหว่างสองประเทศ

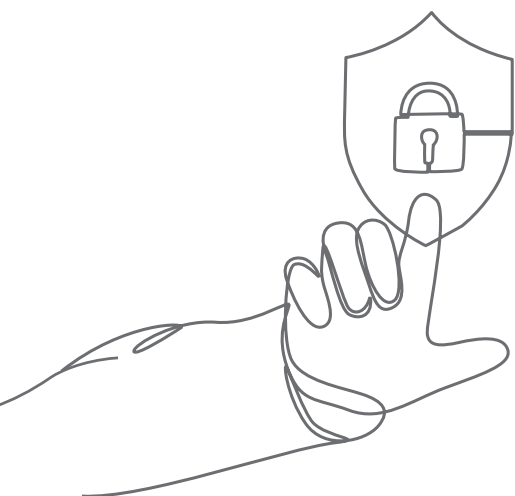


สททช. NECTEC LaoCERT และหน่วยงานใน สปป.ลาว ร่วมประชุม เมื่อวันที่ 19 กันยายน 2567 เพื่อติดตามการนำ Cost-Efficient Open-Source SOC Platform ไปใช้งานใน สปป.ลาว
The NCSA, NECTEC, LaoCERT, and agencies in the Lao PDR held an online meeting on September 19, 2024, to review the implementation of the Cost-Efficient Open-Source SOC Platform in Laos.

Promoting and Supporting Domestic Cybersecurity Entrepreneurs to Reduce Dependence on Foreign Technology

Through its Cybersecurity Research Center, the NCSA has actively supported and driven the development of products and services in the cybersecurity industry. This effort is underpinned by ongoing collaboration with the National Electronics and Computer Technology Center (NECTEC) to promote the practical application of Thai research and development in operational environments.

A key achievement in 2024 was the successful adoption of the **Cost-Efficient Open-Source SOC Platform**, developed by NECTEC, by the **Cybersecurity Coordination Center of the Lao People's Democratic Republic (LaoCERT)** and other agencies within Laos. This initiative also fostered bilateral cooperation to enhance knowledge and skills among cybersecurity personnel, elevating cybersecurity standards between the two countries.



แถลงข่าวการจัดตั้งสถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (THNCA)

เมื่อวันที่ 21 สิงหาคม 2567 สกมช. ได้เปิดตัว **สถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (Thailand National Cyber Academy: THNCA)** โดยมีเป้าหมายเพื่อพัฒนาบุคลากรในทุกระดับ ทั้งภาครัฐ และเอกชน โดยเฉพาะหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ผ่านหลักสูตรอบรมที่ครอบคลุมระดับพื้นฐาน ระดับเชี่ยวชาญ และระดับผู้บริหาร



THNCA คือศูนย์กลางความรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรทุกช่วงวัย ตั้งแต่นักเรียน นักศึกษา ผู้ปฏิบัติงาน ไปจนถึงผู้เชี่ยวชาญและผู้บริหาร รวมถึงประชาชนทั่วไป โดยมุ่งเน้นการสร้างมาตรฐานและการเตรียมความพร้อม ในงานด้านความมั่นคงปลอดภัยไซเบอร์ในยุคดิจิทัลที่เทคโนโลยีเปลี่ยนแปลงอย่างรวดเร็ว พร้อมสนับสนุนการทดสอบและ รับประกาศนียบัตรระดับสากล เพื่อเร่งสร้างผู้เชี่ยวชาญและกำลังคนในภาคส่วนที่เกี่ยวข้อง

Press Conference: Establishment of the Thailand National Cyber Academy (THNCA)

On August 21, 2024, the NCSA officially launched the **Thailand National Cyber Academy (THNCA)**. The initiative aims to develop skilled personnel across all levels-government and private sectors. Especially focusing on the Organization of Critical Information Infrastructure through comprehensive training courses, including essential, advanced, and executive levels.

THNCA serves as a knowledge hub for enhancing cybersecurity skills across all age groups, from students and professionals to experts and executives and the general public. The academy emphasizes setting cybersecurity standards and strengthening readiness in an era of rapidly evolving digital technologies. It also supports participants in achieving internationally recognized certifications and specialized training, accelerating the growth of cybersecurity experts and workforce development in both the public and private sectors.

"คน" คือ หัวใจ ของ CYBERSECURITY

ผลงานประจำปี 2567

สถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เพิ่มทักษะขีดความสามารถแก่บุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

NCSA Cyber Clinic

กลุ่มเป้าหมาย
ผู้แทนหน่วยงานกำกับดูแล
และโครงสร้างพื้นฐานสำคัญ
สารสนเทศ องค์การอิสระ
และผู้สนใจ

จำนวนที่จัด
6 ครั้ง
ยอดผู้เข้าร่วม
1,193 คน

การฝึกอบรม พร้อมประกาศนียบัตรสากล

จำนวนหลักสูตร
9 หลักสูตร
ผู้เข้าฝึกอบรม
6,777 คน

Certificate ที่ได้รับ
1,022 ใบ
300 150 150 C EH 160 C HFI 80
40 50 72 10 10



Lead Implementet, Lead Auditor



จำนวนที่จัด
6 ครั้ง
ยอดผู้เข้าร่วม
321 คน

ลงนาม MOU

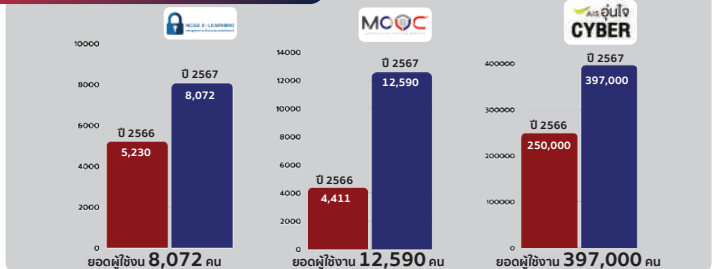
7 หน่วยงาน

NCSA แพลตฟอร์มออนไลน์ ปี 2566-2567

จัดอบรมพิเศษร่วมกับภาคีเครือข่าย



ผู้เข้าอบรม **71,074** คน



สร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ของทุกภาคส่วน

NCSA Cybersecurity Knowledge Sharing

กลุ่มเป้าหมาย

ผู้แทนหน่วยงานกำกับดูแลและโครงสร้างพื้นฐานสารสนเทศ
รัฐวิสาหกิจ องค์การมหาชน องค์กรอิสระ และประชาชนทุกช่วงวัย

จำนวนที่จัด
10 ครั้ง

ยอดผู้เข้าร่วม
28,680 คน



M.TECH
ไซเบอร์ บอร์ดเกม
แจกจ่ายให้หน่วยงานทั่วประเทศ

มากกว่า
500
หน่วยงาน

กิจกรรมสร้างความตระหนักรู้และแนวทางการศึกษา
เพื่อพัฒนาอาชีพด้านความมั่นคงปลอดภัยไซเบอร์ ปีที่ 2
มูลนิธิพระมหาไถ่เพื่อการพัฒนาคนพิการ



ผู้เข้าร่วม **200** คน

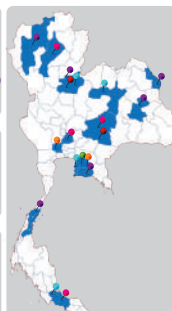


การพัฒนาบุคลากรในระดับประเทศและในภูมิภาคอาเซียน

โครงการ "รู้เท่า รู้ทัน รู้ป้องกันภัยไซเบอร์"
เพื่อเฉลิมพระเกียรติ พระบาทสมเด็จพระเจ้าอยู่หัว
ร่วมกับ สำนักงาน กสทช. ศูนย์บริการอินเทอร์เน็ต
สาธารณะ (USO Net)
ได้แก่ จังหวัดพิษณุโลก เชียงใหม่ ร้อยเอ็ด อุบลราชธานี ระยอง
ผู้เข้าร่วม **30,000** คน

โครงการแข่งขันทักษะทางไซเบอร์ "NCSA Boot
Camp" และ "Thailand Cyber Top Talent 2024"
ได้แก่ จังหวัดนครราชสีมา และ พิษณุโลก
ผู้เข้าร่วม **2,408** คน

กิจกรรมค่ายเยาวชนไซเบอร์
"Cyber Youth Camp"
ได้แก่ จังหวัดนครปฐม และ ชลบุรี
ผู้เข้าร่วม **100** คน

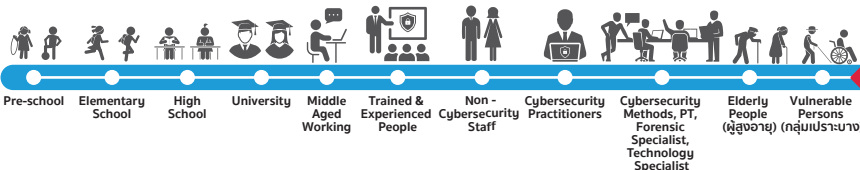
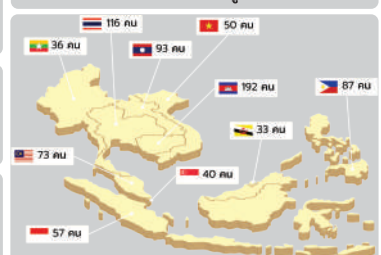


โครงการพัฒนาหลักสูตรและขีดความสามารถ
ผู้ปฏิบัติงานตามมาตรฐานสากล
ได้แก่ จังหวัดพิษณุโลก อุบลราชธานี ชลบุรี สงขลา
ผู้เข้าร่วม **766** คน

โครงการส่งเสริมและสนับสนุนการขับเคลื่อนการพัฒนา
ดิจิทัลในระดับจังหวัดและอำเภอ ภายใต้แนวคิด "A Good
Digital Citizen ก้าวไปสู่ความเป็นพลเมืองดิจิทัล
ที่มีคุณภาพไปด้วยกัน"
ได้แก่ จังหวัดพระนครศรีอยุธยา สงขลา นครราชสีมา ลำปาง
ผู้เข้าร่วม **35,219** คน

กิจกรรม "สร้างความตระหนักรู้และแนวทางการศึกษา
เพื่อพัฒนาอาชีพด้านความมั่นคงปลอดภัยไซเบอร์
ปีที่ 2" (พระมหาไถ่)
ได้แก่ จังหวัดชลบุรี
ผู้เข้าร่วม **200** คน

จัดอบรมร่วมกับศูนย์ AJCCBC
จำนวน **12** ครั้ง ผู้เข้าร่วมรวม **777** คน



รวมทั้งสิ้น

505,513 คน

สรุปผู้เข้าร่วมกิจกรรมตั้งแต่ ปี 2564-2567 มากกว่า **1.5** ล้านคน

กิจกรรมการกำหนดทิศทางและสนับสนุนการวิจัยที่สำคัญเพื่อสร้างองค์ความรู้และเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์

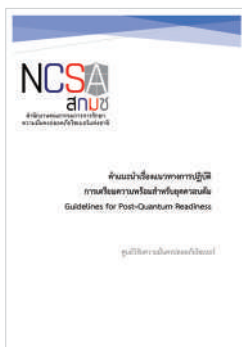
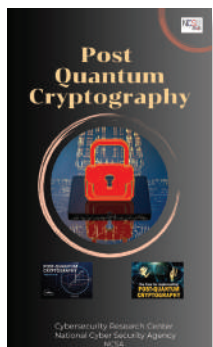
นอกจากการจัดทำ “ฐานข้อมูลผู้ประกอบการภาคอุตสาหกรรมด้านความมั่นคงปลอดภัยไซเบอร์ภายในประเทศ” เพื่อส่งเสริมให้มีผลิตภัณฑ์และการให้บริการ เพิ่มศักยภาพการแข่งขันในภาคอุตสาหกรรมด้านความมั่นคงปลอดภัยไซเบอร์ ยังได้จัดทำบทความและคู่มือ เพื่อให้ทุกภาคส่วนเข้าใจการพัฒนาเทคโนโลยี รวมทั้งพิจารณาถึงผลกระทบต่อความมั่นคงปลอดภัยในโลกไซเบอร์ และเตรียมตัวรับมือได้ทัน

บทความ ประกอบด้วยเรื่อง **Chat GPT, Generative AI** และ **Post Quantum Cryptography** ส่วนคู่มือ ได้แก่ **คำแนะนำเรื่องแนวทางการปฏิบัติการเตรียมความพร้อมสำหรับยุคควอนตัม Guidelines for Post-Quantum Readiness** ซึ่งทั้งหมดสามารถดาวน์โหลดได้ที่ <https://www.ncsa.or.th/article.html>

Directing and Supporting Cybersecurity Research and Technology Development

The NCSA has published articles and guidelines to enhance the understanding of emerging cybersecurity technologies across all sectors, their implications, and proactive preparation for emerging challenges.

The articles cover **Chat GPT, Generative AI, and Post Quantum Cryptography.** The guidelines, including the **Guidelines for Post-Quantum Readiness**, provide actionable recommendations for preparing for the quantum era.



กิจกรรมการจัดหาโครงสร้างพื้นฐานที่จำเป็นสำหรับการวิจัยความมั่นคงปลอดภัยไซเบอร์

สทศ. ได้ผลักดันแผนพัฒนาระบบการดำเนินงานวิจัยด้านความมั่นคงปลอดภัยไซเบอร์ ที่สามารถสนับสนุนการดำเนินการวิจัยด้านความมั่นคงปลอดภัยไซเบอร์ โดยมีการดำเนินงานตามลำดับในปี 2567 นี้คือ

1 ขออนุมัติดำเนินการกิจกรรมการจัดหาโครงสร้างพื้นฐานที่จำเป็นสำหรับการวิจัยความมั่นคงปลอดภัยไซเบอร์

2 จัดทำขอบเขตของงานดำเนินกิจกรรมการจัดหาโครงสร้างพื้นฐานที่จำเป็นสำหรับการวิจัยความมั่นคงปลอดภัยไซเบอร์เพื่อจัดหาระบบและเครื่องมือที่ใช้สำหรับงานสนับสนุนงานด้านงานวิจัย สำหรับการเก็บข้อมูล ผู้ให้บริการ ผู้ประกอบการ และนักวิจัย ด้านความมั่นคงปลอดภัยไซเบอร์ในประเทศ และจัดกิจกรรมเพื่อสนับสนุนงานวิจัย และส่งเสริมอุตสาหกรรมด้านความมั่นคงปลอดภัยไซเบอร์

3 กำหนดแผนการดำเนินงาน แนวทาง และรูปแบบการพัฒนาระบบที่สามารถสนับสนุนการดำเนินการวิจัยความมั่นคงปลอดภัยไซเบอร์จำนวน 1 ระบบ



Infrastructure Development for Cybersecurity Research

The NCSA is driving the development of essential systems to support cybersecurity research through three key initiatives:

1. Securing approval for activities related to acquiring critical infrastructure for research.
2. Defining the scope and procuring tools to collect data on service providers, operators, and researchers while promoting research activities and supporting the cybersecurity industry.
3. Planning and developing a prototype system to effectively facilitate cybersecurity research.

This initiative establishes a solid foundation for advancing innovation and research, enhancing the nation's cybersecurity capabilities.

กิจกรรมการจัดตั้งห้องปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Lab)

ดำเนินการจัดฝึกอบรมเจ้าหน้าที่ในการใช้งานเครื่องมือและอุปกรณ์ในห้องปฏิบัติการ รวมถึงการบำรุงรักษา และการแก้ไขปัญหาเบื้องต้น ให้เป็นไปตามมาตรฐาน ISO 17025

Cybersecurity Laboratory Initiatives (Cyber Security Lab)

Conduct training for staff on using tools and equipment in the laboratory, including maintenance and basic troubleshooting, in compliance with ISO 17025 standards.

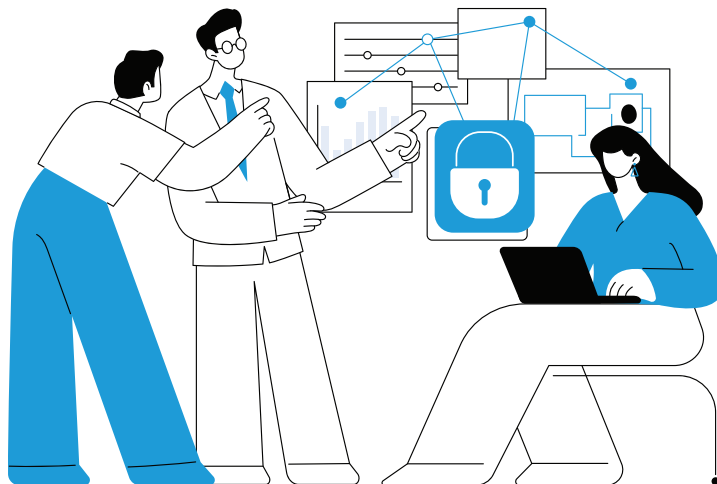
ยุทธศาสตร์ที่ 2

บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)

Strategy 2: Fostering Partnerships for Cyber Incident Response and Resilience

มุ่งเน้นการสร้างความร่วมมือทั้งภายในประเทศและระหว่างประเทศ เพื่อเตรียมความพร้อมรับมือกับภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ และเร่งฟื้นฟูบริการสำคัญให้กลับสู่สภาพปกติได้อย่างรวดเร็ว โดยเน้นการประสานงานระหว่างหน่วยงานภาครัฐ ภาคเอกชน และองค์กรระหว่างประเทศเพื่อความมั่นคงทางไซเบอร์ที่ยั่งยืน

Enhancing collaboration domestically and internationally to effectively address cyber threats and ensure the swift restoration of critical services to normalcy. It emphasizes strong coordination among the public, private, and international organizations to achieve sustainable cybersecurity resilience.





กลยุทธ์ที่ 2.1 : ส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและภาคเอกชน

Strategy 2.1 : Promoting Public-Private Collaboration

มุ่งเน้นความร่วมมือระหว่างหน่วยงานภาครัฐและภาคเอกชน โดยกำหนดโครงสร้างการกำกับดูแลและกลไกการประสานงานที่ชัดเจน เพื่อเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ ควบคู่กับการคุ้มครองข้อมูลส่วนบุคคล นอกจากนี้ ยังสนับสนุนการพัฒนาศักยภาพบุคลากรภาครัฐที่เกี่ยวข้องกับการบังคับใช้กฎหมายด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเพิ่มประสิทธิภาพในการรับมือกับภัยคุกคามที่เปลี่ยนแปลงตลอดเวลา

Fostering collaboration between government agencies and the private sector by establishing clear governance structures and coordination mechanisms. It aims to strengthen cybersecurity while ensuring data privacy protection. Additionally, it supports capacity-building for government personnel enforcing cybersecurity laws, enhancing their ability to address evolving cyber threats effectively.

การป้องกันการรั่วไหลของข้อมูล (Data Leak) จากภัยคุกคามทางไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลไม่ให้ถูกละเมิด (Data Breach)

สทช. ได้บูรณาการร่วมกับ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ปฏิบัติงานร่วมกันเพื่อป้องกันการรั่วไหลของข้อมูล จากภัยคุกคามทางไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลไม่ให้ถูกละเมิด โดยมีการ**ประชุมความร่วมมือในการป้องกันการรั่วไหลของข้อมูล (Data leak) จากภัยคุกคามทางไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลไม่ให้ถูกละเมิด (Data breach)** เพื่อเตรียมการและวางแผนการตรวจหน่วยงานต่อไป

รวมทั้งมีการแต่งตั้งคณะทำงานป้องกันการละเมิดของข้อมูลส่วนบุคคลจากภัยคุกคามทางไซเบอร์ เพื่อบูรณาการและขับเคลื่อนการตรวจประเมินให้มีประสิทธิภาพเพิ่มมากขึ้น และได้ดำเนินการตรวจประเมินด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล สำหรับหน่วยงานที่มีข้อมูลส่วนบุคคลเป็นจำนวนมาก ซึ่งเป็นหน่วยงานภายใต้ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐ ซึ่งต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2566 โดยนำร่องการตรวจ 20 หน่วยงาน ในช่วงเดือนมีนาคม - กรกฎาคม 2567

ทั้งนี้ได้ให้คำแนะนำที่เหมาะสมตามความเร่งด่วนของแต่ละหน่วยงาน เพื่อให้ดำเนินการในด้านดังกล่าวได้อย่างมีประสิทธิภาพ สอดคล้องตามมาตรฐานสากลมากยิ่งขึ้น โดยมีผลการตรวจประเมินฯ ในภาพรวมเป็นไปด้วยความเรียบร้อย





Activities to Prevent Data Leaks from Cyber Threats and Protecting Personal Data from Breaches

The NCSA, in collaboration with the **Office of the Personal Data Protection Committee (PDPC)**, has initiated joint efforts to prevent data leaks caused by cyber threats and ensure the protection of personal data from breaches. A collaborative meeting was held to discuss strategies for preventing data leaks and safeguarding personal data, focusing on preparing and planning for future organizational audits.

A task force was established to address personal data breaches arising from cyber threats, aiming to streamline and enhance the effectiveness of data protection assessments. The task force conducted cybersecurity and data protection evaluations for agencies managing significant volumes of personal data. These assessments are following the **PDPC's Notification on Public Agencies as Data Controllers and Processors**, requiring the appointment of **Data Protection Officers (DPOs)** under the **2023 Notification on Data Protection Responsibilities**. **Between March and July 2024, 20 agencies underwent a pilot assessment**, focusing on evaluating their cybersecurity and data protection measures.

Agencies received tailored recommendations based on the urgency of their needs, ensuring effective implementation of data protection measures in alignment with international standards. The overall assessment process was completed successfully, with positive results indicating enhanced compliance and readiness across all assessed organizations.

บันทึกความเข้าใจว่าด้วยความร่วมมือกับหน่วยงานต่าง ๆ

สทกษ. ได้ดำเนินการจัดทำบันทึกความเข้าใจว่าด้วยความร่วมมือ (MOU) ในปี 2567 ทั้งสิ้น 22 ฉบับ

1. ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กับ กองทุนเงินให้กู้ยืมเพื่อการศึกษา (กยศ.) (17 ม.ค. 67)
2. ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กับ บริษัท โกลิอุค จำกัด (17 ม.ค. 67)
3. ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กับ มหาวิทยาลัยธรรมศาสตร์ (31 ม.ค. 67)
4. ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กับ กรมการขนส่งทางบก (31 ม.ค. 67)
5. ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กับ Fortinet Thailand (31 ม.ค. 67)
6. ด้านการวิจัยและพัฒนา กับ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (1 ก.พ. 67)
7. ด้านวิจัยและวิชาการ กับ สำนักงานสถิติแห่งชาติ (1 ก.พ. 67)
8. ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กับ สำนักงานการบินพลเรือนแห่งประเทศไทย (8 ก.พ. 67)
9. ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กับ กองทัพอากาศ (9 ก.พ. 67)
10. ด้านการส่งเสริมการพัฒนาศักยภาพการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กับ มหาวิทยาลัยอุบลราชธานี (4 มี.ค. 67)
11. ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กับ แคสเปอร์สกี (Kaspersky) (10 เม.ย. 67)
12. ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กับ บริษัท ไมโครซอฟท์ (ประเทศไทย) (11 เม.ย. 67)
13. ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กับ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สทกษ.) (22 เม.ย. 67)
14. ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กับ มหาวิทยาลัยราชภัฏพระนครศรีอยุธยา (10 มิ.ย. 67)
15. ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กับ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (DGA) (10 มิ.ย. 67)
16. ประกาศความร่วมมือในการเสริมความมั่นคงปลอดภัยทางไซเบอร์ในชุมชนท้องถิ่น กับ สมาคมสันนิบาตเทศบาลแห่งประเทศไทย (10 มิ.ย. 67)
17. ด้านวิชาการ กับ สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ (CIPAT) (25 มิ.ย. 67)
18. ด้านวิชาการ กับ มหาวิทยาลัยศรีนครินทรวิโรฒ (12 ก.ค. 67)



บันทึกความร่วมมือ (Memorandum of Understanding: MOU) ของ สกมช. ในปี 2567



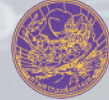
กองทุนเงินให้กู้ยืม
เพื่อการศึกษา (กยศ.)

Gogolook

บริษัทโกโกลูก
(ประเทศไทย) จำกัด



มหาวิทยาลัยธรรมศาสตร์



กรมการขนส่งทางบก

FORTINET

บริษัทฟอร์ทเน็ต
ซีเคียวริตี้ เน็ตเวิร์ค
(ประเทศไทย) จำกัด

สวทช. NSTDA

สำนักงานพัฒนา
วิทยาศาสตร์
และเทคโนโลยีแห่งชาติ



สำนักงานสถิติแห่งชาติ

CAAT

สำนักงานการบินพลเรือน
แห่งประเทศไทย



กองทัพอากาศ



มหาวิทยาลัย
อุบลราชธานี



กสทช.



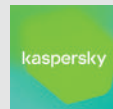
มหาวิทยาลัย
ราชภัฏพระนครศรีอยุธยา

DGA
DIGITAL GOVERNMENT
DEVELOPMENT AGENCY

DGA



สมาคมสันนิบาตเทศบาล
แห่งประเทศไทย



แคสเปอร์สกี
(Kaspersky)

CIPAT

สมาคมส่งเสริมเทคโนโลยีการคอมพิวเตอร์
Cyber Innovation Promotion Association of Technology

สมาคม CIPAT

Microsoft

บริษัทไมโครซอฟท์
(ประเทศไทย)



มหาวิทยาลัย
สกลนคร



ภายใต้โครงการ "Digital Vaccine"
11 หน่วยงาน



สำนักงานการวิจัยแห่งชาติ (วช.)
และสำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล (สคส.)



3 มหาวิทยาลัย
มหาวิทยาลัยราชภัฏร้อยเอ็ด
มหาวิทยาลัยกรุงเทพ
และมหาวิทยาลัยหอการค้าไทย



กรมสนับสนุน
บริการสุขภาพ
กระทรวงสาธารณสุข

19. การจัดทำพร้อมทั้งเผยแพร่สื่อประชาสัมพันธ์ ภายใต้โครงการ “Digital Vaccine” 11 หน่วยงาน ประกอบด้วย 1) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม 2) สำนักงานตำรวจแห่งชาติ 3) กรมสอบสวนคดีพิเศษ 4) กรมประชาสัมพันธ์ 5) ธนาคารแห่งประเทศไทย 6) สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ 7) สำนักงานป้องกันและปราบปรามการฟอกเงิน 8) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ 9) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ 10) สมาคมธนาคารไทย 11) สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (9 ส.ค. 67)
20. ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กับ กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข (21 ส.ค. 67)
21. ด้านการวิจัยและพัฒนาเพื่อเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย กับ สำนักงานการวิจัยแห่งชาติ (วช.) และ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) (27 ส.ค. 67)
22. ด้านการพัฒนาทักษะและองค์ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ กับ มหาวิทยาลัยราชภัฏร้อยเอ็ด มหาวิทยาลัยกรุงเทพ และมหาวิทยาลัยหอการค้าไทย (17 ก.ย. 67)

Memorandums of Understanding (MOUs) in 2024

The NCSA signed a total of **22 MOUs in 2024, focusing on cybersecurity, research, and capacity building:**

1. Cybersecurity: **Student Loan Fund (SLF)** (Jan 17, 2024).
2. Cybersecurity: **Gogolook Co., Ltd.** (Jan 17, 2024).
3. Cybersecurity: **Thammasat University** (Jan 31, 2024).
4. Cybersecurity: **Department of Land Transport** (Jan 31, 2024).
5. Cybersecurity: **Fortinet Thailand** (Jan 31, 2024).
6. Research & Development: **National Science and Technology Development Agency (NSTDA)** (Feb 1, 2024).
7. Research & Academics: **National Statistical Office (NSO)** (Feb 1, 2024).
8. Cybersecurity: **Civil Aviation Authority of Thailand** (Feb 8, 2024).
9. Cybersecurity: **Royal Thai Air Force** (Feb 9, 2024).
10. Capacity Building: **Ubon Ratchathani University** (Mar 4, 2024).
11. Cybersecurity: **Kaspersky** (Apr 10, 2024).
12. Cybersecurity: **Microsoft Thailand** (Apr 11, 2024).
13. Cybersecurity: **National Broadcasting and Telecommunications Commission (NBTC)** (Apr 22, 2024).
14. Cybersecurity: **Pibulsongkram Rajabhat University** (Jun 10, 2024).
15. Cybersecurity: **Digital Government Development Agency (DGA)** (Jun 10, 2024).
16. Cybersecurity in Local Communities: **The National Municipal League of Thailand** (Jun 10, 2024).
17. Academics: **Cybersecurity Innovation Promotion Association of Thailand (CIPAT)** (Jun 25, 2024).
18. Academics: **Srinakharinwirot University** (Jul 12, 2024).
19. Public Awareness Campaign: “Digital Vaccine” initiative with **11 organizations**, including the Ministry of Digital Economy and Society, Royal Thai Police, Department of Special Investigation, and Bank of Thailand (Aug 9, 2024).
20. Cybersecurity: **Department of Health Service Support, Ministry of Public Health** (Aug 21, 2024).
21. Cybersecurity and Data Protection: **National Research Council of Thailand (NRCT)** and the **Office of the Personal Data Protection Committee (PDPC)** (Aug 27, 2024).
22. Academics: **Roi Et Rajabhat University, Bangkok University, and University of the Thai Chamber of Commerce** (Sep 17, 2024).



These collaborations aim to enhance cybersecurity capabilities, promote research and innovation, and foster partnerships across sectors at both national and international levels.

บูรณาการความร่วมมือด้านกฎหมายรับมือภัยคุกคามไซเบอร์

เมื่อวันที่ 24 เมษายน 2567 สกมช. จัดประชุมร่วมกับศาลอาญา ศาลปกครอง สำนักงานอัยการสูงสุด และสำนักงานคณะกรรมการกฤษฎีกา เพื่อหารือแนวทางจัดการภัยคุกคามทางไซเบอร์ ครบคลุมการออกคำสั่ง การยื่นคำร้อง การตีความกฎหมาย และขั้นตอนปฏิบัติงาน การหารือดังกล่าวช่วยเสริมความร่วมมือและบูรณาการการทำงานเพื่อรับมือภัยไซเบอร์อย่างมีประสิทธิภาพและทันทั่วทั้ง

Legal Collaboration for Cyber Incident Response

On April 24, 2024, the NCSA held a meeting with the **Criminal Court, Administrative Court, Office of the Attorney General, and Office of the Council of State** to discuss managing cybersecurity threats. Key topics included administrative orders, court filings, legal interpretation, and procedural steps for handling incidents. This collaboration strengthens interagency coordination for an effective and timely response to cyber threats.



กลยุทธ์ที่ 2.2 : ประสานความร่วมมือระหว่างประเทศ เพื่อรับมือกับภัยคุกคาม

Strategy 2.2 : Coordinating International Cooperation to Response the Threats

ยกระดับความสำคัญของความมั่นคงปลอดภัยไซเบอร์ในระดับนโยบายต่างประเทศ โดยการเข้าร่วมเวทีระหว่างประเทศ สร้างความร่วมมือในทุกมิติ พัฒนายุทธศาสตร์ให้สอดคล้องกับมาตรฐานสากล และพัฒนาทรัพยากรบุคคลเพื่อทำงานร่วมกับนานาชาติได้อย่างมีประสิทธิภาพ

Elevating the importance of cybersecurity in foreign policy by participating in international forums, fostering cooperation in all dimensions, aligning national strategies with global standards, and developing human resources to collaborate effectively with international partners.

CYBERSEC ASIA x Thailand International Cyber Week 2024

CYBERSEC ASIA x Thailand International Cyber Week 2024 โดย สกมช. กิจกรรมสำคัญครั้งใหญ่ประจำปีสำหรับอุตสาหกรรมความมั่นคงปลอดภัยทางไซเบอร์ระดับนานาชาติ จัดขึ้นระหว่างเมื่อวันที่ **31 มกราคม และ 1 กุมภาพันธ์ 2567** มีธุรกิจชั้นนำกว่า 58 ราย จากนานาชาติ และผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์ นักลงทุน ผู้ซื้อรายสำคัญและผู้ที่สนใจ **กว่า 2,200 รายจาก 39 ประเทศ** เข้าร่วมงานในครั้งนี้

กิจกรรมครั้งนี้ได้รวม**วิทยากรผู้ทรงคุณวุฒิ 61 ท่านจากทั่วโลก** ซึ่งมีความรู้และเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์มาร่วมพูดคุยกันผ่านการประชุม การสัมมนา และกิจกรรมเวิร์กช็อปซึ่งเจาะลึกด้านเทคนิคและวิธีการ **กว่า 50 กิจกรรม** ครอบคลุมหัวข้อที่หลากหลายโดยเจาะลึกถึงแนวโน้มของเทรนด์ล่าสุด การรับมือกับความท้าทายใหม่ และนวัตกรรมด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ล้ำสมัย

ผู้เข้าร่วมงานมาจากประเทศต่าง ๆ โดย 5 อันดับแรก ได้แก่ ประเทศไทย สิงคโปร์ มาเลเซีย อินเดีย และสหรัฐอเมริกา ตามลำดับ พร้อมทั้งยังให้การต้อนรับคณะผู้แทนธุรกิจจากอิสราเอล รัสเซีย ลาว เมียนมาร์ ญี่ปุ่น เนปาล จีน และอื่น ๆ อีกมากมาย ด้วยเป้าหมายระยะยาวในการมุ่งยกระดับมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ภายในประเทศไปสู่ระดับนานาชาติ



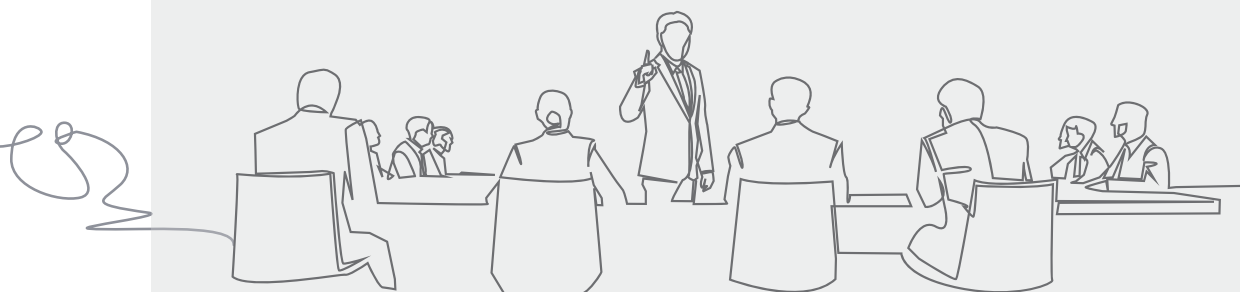


CYBERSEC ASIA x Thailand International Cyber Week 2024

The CYBERSEC ASIA x Thailand International Cyber Week 2024, hosted by NCSA on January 31 and February 1, 2024, marked a pivotal convergence for the global cybersecurity industry in Thailand. Featuring over 58 leading brands from various nations, the event welcomed **over 2,200 attendees from 39 countries**, including cybersecurity experts, investors, key buyers, and enthusiasts.

The event showcased **61 distinguished speakers** from around the world, who shared insights through **over 50 sessions** of conferences, seminars, and technical workshops. Discussions spanned cutting-edge cybersecurity innovations, emerging trends, and strategies to address new challenges.

Top participating countries included Thailand, Singapore, Malaysia, India, and the United States. Delegations from Israel, Russia, Laos, Myanmar, Japan, Nepal, China, and more also attended this event. Reflecting a collective effort to elevate Thailand's cybersecurity standards to the global stage.



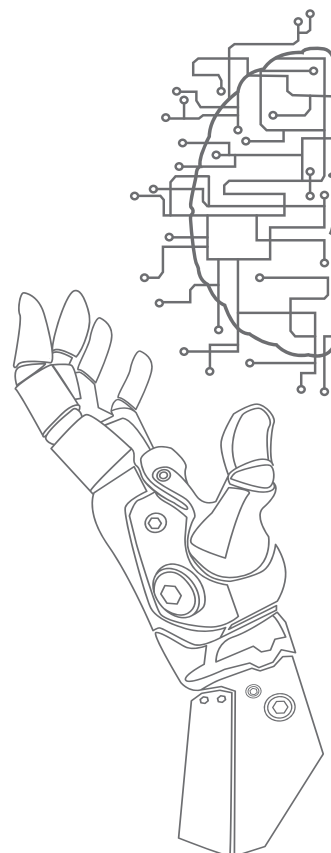
Thailand International Cyber Week 2024 ในงานมหกรรมวิทยาศาสตร์และเทคโนโลยี และมหกรรมงานวิจัยแห่งชาติ 2567

สทศ. ได้ยกระดับกิจกรรม Thailand International Cyber Week 2024 เพื่อให้เข้าถึงกลุ่มเยาวชนและประชาชนอย่างกว้างขวางขึ้น เข้าร่วมสองงานใหญ่ประจำปีของหน่วยงานพันธมิตร ได้แก่

1 มหกรรมวิทยาศาสตร์และเทคโนโลยีแห่งชาติ 2567 (National Science and Technology Fair 2024) ระหว่างวันที่ 16-25 สิงหาคม 2567 จัดโดย องค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ (อพวช.) และ สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (อว.) โดยมีผู้ลงทะเบียนเข้าร่วมงานกว่า 685,226 คน

2 มหกรรมงานวิจัยแห่งชาติ 2567 (Thailand Research Expo 2024) ระหว่างวันที่ 26-30 สิงหาคม 2567 จัดโดย สำนักงานการวิจัยแห่งชาติ (วช.) มีผู้ลงทะเบียนประมาณ 30,000 คน

สทศ. ได้สร้างสรรคณิทรศการและกิจกรรมให้เข้าถึงกลุ่มเป้าหมายหลากหลาย ตั้งแต่เยาวชน นักเรียน นักศึกษา นักวิจัย ไปจนถึงบุคคลทั่วไป ด้วยเครื่องมือการเรียนรู้ใหม่ เช่น โซนบอร์ดเกม และแพลตฟอร์มเสริมความรู้ด้านไซเบอร์ เพื่อกระตุ้นความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ พร้อมมอบองค์ความรู้ในการปกป้องตัวเองและผู้อื่นจากภัยไซเบอร์ในโลกดิจิทัลที่เปลี่ยนแปลงอย่างรวดเร็ว



Thailand International Cyber Week 2024 at the National Science and Technology Fair & Thailand Research Expo 2024

Broadening the Thailand International Cyber Week 2024 exhibition and activities to be showcased at two major annual events of NCSA's Alliances:

1. **National Science and Technology Fair 2024**, held from August 16-25, 2024, by the **National Science Museum (NSM)** and **MHESI**, attracting **685,226 attendees**.
2. **Thailand Research Expo 2024**, held by **NRCT** from August 26-30, 2024, with **approximately 30,000 participants**.

NCSA introduced innovative exhibits and activities to engage diverse audiences, including youth, students, researchers, and the general public, such as cyber board games and educational cybersecurity platforms. These initiatives aimed to raise awareness about cyber threats and equip attendees with knowledge on protecting themselves and others in the rapidly evolving digital era.



Joint Coordinating Committee (JCC)

การประชุมส่งเสริม ASEAN-Japan Cybersecurity Capacity Building Centre: ก้าวสำคัญสู่การพัฒนา Cybersecurity ในอาเซียน “Joint Coordinating Committee (JCC) Meeting” เพื่อหารือและติดตามความคืบหน้าในการดำเนินงานของ ASEAN-Japan Cybersecurity Capacity Building Centre ที่ผ่านมา นอกจากนี้ยังมีการหารือถึงแผนงานที่จะขับเคลื่อนต่อไป ด้วยเป้าหมายการเพิ่มจำนวนผู้เข้าร่วมอบรมของชาติอาเซียนให้มากขึ้นกว่าเดิม และมุ่งมั่นที่จะสร้างเครือข่ายระดับสากลผ่านการดำเนินงานของกิจกรรมต่าง ๆ

การดำเนินงานของ ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) ภายใต้ความร่วมมือของประเทศไทย ญี่ปุ่น และประเทศสมาชิกอาเซียน ได้ประกาศความสำเร็จในการจัดกิจกรรมเพื่อส่งเสริมและพัฒนาศักยภาพด้าน Cybersecurity ให้แก่บุคลากรในภูมิภาคอาเซียน แสดงให้เห็นถึงความมุ่งมั่นในการสร้างความรู้และทักษะใหม่ๆ ในยุคดิจิทัล ผลงานที่สำคัญของ AJCCBC ในช่วงเวลาที่ผ่านมา ไม่ว่าจะเป็นการจัดสัมมนา การอบรมเชิงปฏิบัติการ และโครงการที่เน้นการสร้างศักยภาพด้าน Cybersecurity ให้แก่ผู้เข้าร่วม โดยมีเป้าหมายเพื่อเพิ่มความเข้าใจและเตรียมความพร้อมให้กับประชาชนในการรับมือกับภัยคุกคามในโลกไซเบอร์ที่เพิ่มขึ้น

การประชุม JCC ครั้งที่ 1 จัดขึ้นเมื่อวันที่ 20 ตุลาคม 2566 ครั้งที่ 2 วันพุธที่ 27 มีนาคม 2567 และครั้งที่ 3 วันพุธที่ 4 กันยายน 2567 หน่วยงานเข้าร่วมประชุมประกอบด้วย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กรมความร่วมมือระหว่างประเทศ และกรมอาเซียน กระทรวงการต่างประเทศ หน่วยงานต่างประเทศ ซึ่งเป็นส่วนหนึ่งของคณะประชุม Joint Coordinating Committee (JCC) เข้าร่วมการประชุม ประกอบด้วย Ministry of Internal Affairs and Communications (MIC) of Japan, Ministry of Foreign Affairs (MOFA) of Japan, สำนักเลขาธิการอาเซียน (ASEAN Secretariat) และ Japan International Cooperation Agency (JICA)



Joint Coordinating Committee (JCC) Meeting: Advancing Cybersecurity Capacity in ASEAN

The **Joint Coordinating Committee (JCC) Meeting** is a significant milestone in advancing the **ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC)** development. The meeting focuses on reviewing the progress made thus far and discussing future initiatives to expand the center's activities. Key objectives include increasing the participation of ASEAN member states in training programs and fostering an international network through various collaborative initiatives.

Under the partnership between Thailand, Japan, and ASEAN member countries, the AJCCBC has demonstrated remarkable achievements in promoting and enhancing cybersecurity capabilities across the ASEAN region. Notable accomplishments include seminars, hands-on workshops, and capacity-building projects designed to equip participants with essential knowledge and skills in cybersecurity. These initiatives aim to strengthen the readiness of ASEAN professionals and citizens to address the increasing challenges of cyber threats in the digital age.

The JCC Meetings have occurred as follows: the first Meeting was on October 20, 2023; the second Meeting was on March 27, 2024; and the third Meeting was on September 4, 2024.

Representatives from **Thailand's Ministry of Digital Economy and Society (MDES)**, the **Department of International Cooperation**, the **Department of ASEAN Affairs**, and the **Ministry of Foreign Affairs** are the participants. International participants include the **Ministry of Internal Affairs and Communications (MIC)** of Japan, the **Ministry of Foreign Affairs (MOFA)** of Japan, the **ASEAN Secretariat**, and the **Japan International Cooperation Agency (JICA)**.

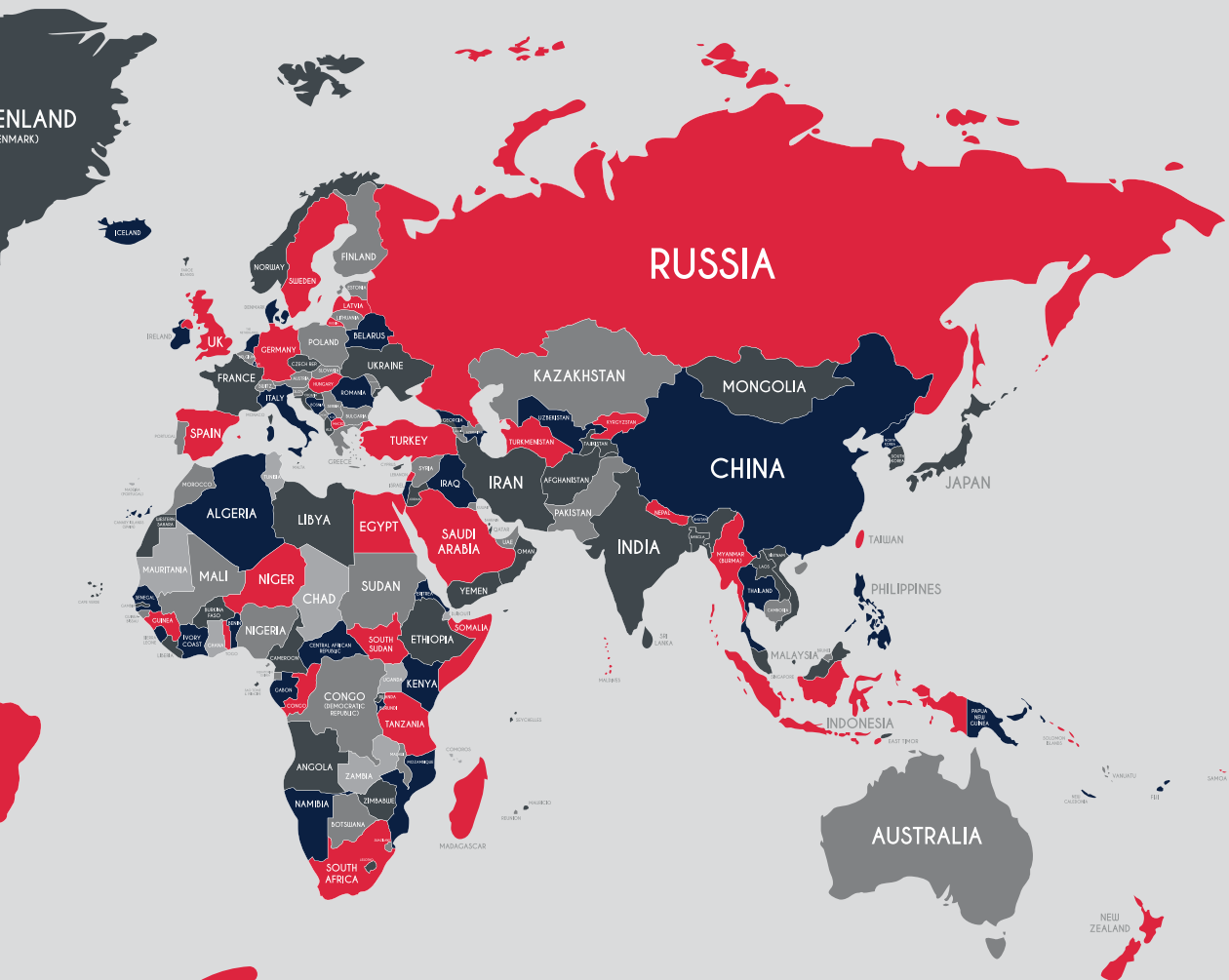
The continued collaboration through the JCC highlights a shared commitment to strengthening cybersecurity across the ASEAN region, fostering innovation, and building a resilient digital ecosystem capable of addressing evolving cyber threats.



สถิติการดำเนินงาน ด้านความร่วมมือระหว่างประเทศ INTERNATIONAL COOPERATION STATISTICS FOR FISCAL YEAR 2024



	Bilateral	Multilateral
ประสานงาน/ร่วมมือกับต่างประเทศ (Coordination/International Engagements)	199	228
ประชุม/อบรม/สัมมนา (Meetings/Training/Seminars)	122	173
พิจารณา/ให้ความเห็น/สนับสนุนข้อมูล (Evaluations/Recommendations/Information Support)	30	47
รวม (Total)	351	448



ยุทธศาสตร์ความร่วมมือทวิภาคี (Bilateral Cooperation Strategy)

Countries: Australia, Bangladesh, Bahrain, Belgium, Canada, China, Czech, India, Indonesia, Israel, Japan, Korea, Malaysia, Netherlands, New Zealand, Russia, Singapore, UAE, UK, USA



ยุทธศาสตร์ความร่วมมือพหุภาคี (Multilateral Cooperation Strategy)

Organizations: AALCO, ASEAN, APEC, BIMSTEC, ESIWA, EU, ICANN, ITU, UN
Digital Trade/E-Commerce Platforms: APT, ACAFTA, CEPA, FTA, EFTA, IPEF, SECA, WTO



การลงนามในบันทึกความเข้าใจ (Memorandum of Understanding :MOU)

- ▶ NCSA signed Memorandum of Understandings (MOUs) with China และ Israel
- ▶ NCSA signed Record of Discussions with JICA for AJCCBC
- ▶ MOU with India is in process

ยุทธศาสตร์ที่ 3

สร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์ และฟื้นคืนสู่สภาพปกติได้ (Resilience)

Strategy 3: Enhancing Cybersecurity Resilience for Public Services and Critical Information Infrastructure

มุ่งเน้นการกำหนดกรอบการกำกับดูแลและมาตรการที่ชัดเจนสำหรับหน่วยงานภาครัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยมีเป้าหมายเพื่อสร้างความมั่นคงปลอดภัยไซเบอร์ในระดับพื้นฐาน ส่งเสริมการปกป้องระบบข้อมูลและเครือข่าย รวมถึงการพัฒนาความสามารถในการฟื้นคืนบริการที่สำคัญในกรณีที่เกิดภัยคุกคามหรือเหตุการณ์ไม่คาดฝัน ยุทธศาสตร์นี้เป็นรากฐานสำคัญในการยกระดับความมั่นคงปลอดภัยไซเบอร์ของประเทศให้เทียบเท่ามาตรฐานสากล

Establishing clear governance frameworks and baseline security measures for government agencies and critical information infrastructure. This strategy aims to ensure robust cybersecurity protections, safeguard information systems and networks, and strengthen the capacity to restore essential services during cyber threats or unexpected incidents. It is a foundational pillar to elevate the nation's cybersecurity standards to align with international best practices.





กลยุทธ์ที่ 3.1 : กำหนดมาตรการการรักษาความมั่นคงปลอดภัย ขั้นต่ำสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศ (Critical Information Infrastructure : CII)

Strategy 3.1 : Establishing Minimum Cybersecurity Measures for Organization of Critical Information Infrastructure

ระบุประเภทของโครงสร้างพื้นฐานที่สำคัญและวางแผนก
มาตรฐานความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ เพื่อช่วย
ลดความเสี่ยงจากภัยคุกคาม ส่งเสริมการออกแบบระบบ
ที่คำนึงถึงความปลอดภัยตั้งแต่เริ่มต้น (Security by
Design) และสร้างความตระหนักรู้ให้บุคลากรทุกระดับ
เกี่ยวกับบทบาทสำคัญในการรักษาความมั่นคงปลอดภัย
ไซเบอร์ เพื่อให้ระบบสารสนเทศที่สำคัญของประเทศมั่นคง
ปลอดภัยและพร้อมรับมือภัยคุกคาม

Identifying critical infrastructure types and setting
minimum cybersecurity standards to mitigate risks.
The strategy also promotes the principle of Security
by Design, ensuring secure system architecture from
the outset. It emphasizes raising awareness across all
personnel levels regarding their role in maintaining
cybersecurity. These initiatives aim to safeguard
critical information systems and ensure they are
prepared to counter evolving cyber threats in the
digital era.

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

กรอบมาตรฐานเพื่อยกระดับความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานภาครัฐ หน่วยงานควบคุมหรือกำกับดูแล
และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยมุ่งเน้นการจัดลำดับผลกระทบจากภัยคุกคามในระดับต่ำ
กลาง และสูง พร้อมระบุมาตรการควบคุมขั้นต่ำเพื่อรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูล
หรือระบบสารสนเทศในทุกกระบวนอย่างมีประสิทธิภาพ ซึ่งมาตรฐานดังกล่าวจะมีผลบังคับใช้ตั้งแต่วันที่ 18 มกราคม 2568
เพื่อสร้างความเชื่อมั่นในระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศและเสริมความพร้อมของประเทศในการเผชิญหน้า
กับภัยไซเบอร์ในอนาคต

Notification of the National Cyber Security Committee on the Minimum Standards for Information or Information Systems (2023)

Establishes a robust framework to enhance cybersecurity for government agencies, regulators,
and organizations of critical information infrastructure. This standard, effective from January
18, 2025, aims to build confidence in critical information infrastructure and strengthen the
nation's readiness against future cyber threats.

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566
 (ฐานอำนาจตามมาตรา 9 (4) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)



ประกาศในราชกิจจานุเบกษา
 18 มกราคม 2567

มีผลใช้บังคับ
18 มกราคม 2568



มีผลบังคับใช้กับ
GOV REG และ CII



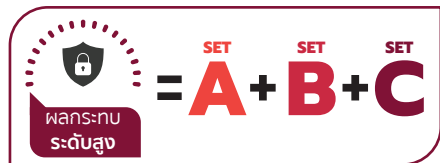
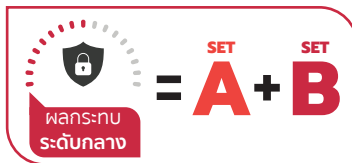
Security Baselines



เพื่อให้ **GOV REG** และ **CII** สามารถกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขึ้นได้อย่างเหมาะสม
 คำนึงถึง ลดมาตรการควบคุมและค่าใช้จ่ายที่เกินความจำเป็น ช่วยประหยัดงบประมาณแผ่นดินของประเทศ



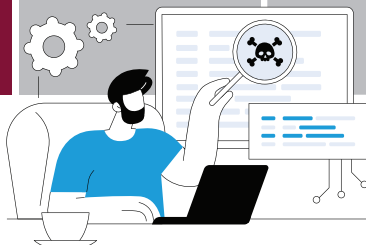
ภายหลังจากหน่วยงานได้กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์
 และได้ระดับผลกระทบที่อาจเกิดขึ้นแก่ข้อมูลหรือระบบสารสนเทศแล้ว
ให้กำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ
 สำหรับข้อมูลหรือระบบสารสนเทศในแต่ละระดับ ดังนี้



ประมวลแนวทางปฏิบัติ

กรอบมาตรฐานด้าน Cybersecurity

SET A	การประเมินความเสี่ยง ด้าน Cybersecurity แผนการรับมือ ภัยคุกคามทางไซเบอร์	การระบุความเสี่ยง (Identify) การจัดการทรัพย์สิน การประเมินความเสี่ยงและกลยุทธ์ มาตรการตรวจสอบและเฝ้าระวัง (Detect) การตรวจสอบและเฝ้าระวัง	มาตรการป้องกัน (Protect) การควบคุมการเข้าถึง การทำให้ระบบมีความแข็งแกร่ง การสร้างความตระหนักรู้ มาตรการเผชิญเหตุ (Respond) แผนการรับมือ แผนการสื่อสารในภาวะวิกฤต การฝึกซ้อม
SET B	แผนการตรวจสอบ ด้าน Cybersecurity	มาตรการป้องกัน (Protect) การเชื่อมต่อระยะไกล สื่อเก็บข้อมูลแบบถอดได้	
SET C		การระบุความเสี่ยง (Identify) การประเมินช่องโหว่และ การทดสอบเจาะระบบ การจัดการผู้ให้บริการภายนอก	มาตรการป้องกัน (Protect) การแบ่งปันข้อมูล มาตรการรักษาและฟื้นฟูความเสียหาย (Recover) การรักษาและฟื้นฟู ความเสียหายที่เกิด



ประกาศ กมช.
 เรื่อง มาตรฐานขั้นต่ำ

กลยุทธ์ที่ 3.2 : กำหนดโครงสร้างการกำกับดูแล และกรอบกฎหมายสำหรับหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

Strategy 3.2 : Establishing Governance Structures and Legal Frameworks for Organization of Critical Information Infrastructure

มุ่งเน้นการวางโครงสร้างการกำกับดูแลและกรอบกฎหมายที่ทันสมัยสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) โดยเน้นการบริหารจัดการความเสี่ยงเพื่อปกป้องโครงสร้างสำคัญจากภัยคุกคามไซเบอร์ พร้อมทั้งพัฒนากลไกการกำกับดูแลที่ชัดเจนและครอบคลุม รวมถึงพิจารณาให้ข้อมูลและบริการคลาวด์เป็นส่วนหนึ่งของโครงสร้างพื้นฐานสำคัญที่ต้องอยู่ภายใต้การกำกับดูแล นอกจากนี้ ยังมุ่งพัฒนากฎหมายและกฎระเบียบที่เกี่ยวข้องให้สอดคล้องกับสถานการณ์และภัยคุกคามที่เปลี่ยนแปลงไปอย่างรวดเร็ว เพื่อเพิ่มประสิทธิภาพการป้องกันและตอบสนองต่อความเสี่ยงในระดับประเทศอย่างยั่งยืน

Establishing a robust governance framework and modern legal standards for Organization of Critical Information Infrastructure. The strategy emphasizes risk management to protect vital infrastructures from cyber threats while developing comprehensive and clear oversight mechanisms. The strategy also includes plans to incorporate Data and Cloud Computing as part of CII under future regulatory oversight. Additionally, it prioritizes updating cybersecurity laws and regulations to align with evolving threats and technological advancements, enhancing the nation's capacity to prevent and respond to cyber risks effectively and sustainably.

กิจกรรมส่งเสริมการบังคับใช้กฎหมายในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

สทท. แสดงให้เห็นถึงบทบาทสำคัญในความพยายามป้องกันภัยคุกคามทางไซเบอร์ ผ่านการสร้างความร่วมมือระดับโลก พัฒนากฎหมายภายในประเทศ และแลกเปลี่ยนองค์ความรู้ในระดับภูมิภาค โดยมุ่งเน้นทั้งการป้องกันและลดผลกระทบที่อาจเกิดขึ้นกับประชาชนและองค์กร ผ่านกิจกรรมต่าง ๆ

1 การสร้างความร่วมมือระดับโลกในงาน Security Analysis Summit (SAS) ในวันที่ 25-27 ตุลาคม 2566 ที่จัดโดย Kaspersky โดยในงานได้รวมวิทยากรผู้ที่มีวิสัยทัศน์ทั้งในโลกดิจิทัล Cyber Security และหน่วยงานบังคับใช้กฎหมายระดับโลก ร่วมเสวนาในหัวข้อ “Securing Supply Chains in the Open-Source Era” มุ่งสร้างความร่วมมือและพัฒนากลยุทธ์ในการรับมือกับภัยคุกคามทางไซเบอร์ และเพื่อให้องค์กรมีความแข็งแกร่งและปลอดภัยจากภัยคุกคามทางไซเบอร์

2 การเสริมความเข้มแข็งกฎหมายไซเบอร์ เมื่อวันที่ 15 พฤศจิกายน 2566 และ 19 มกราคม 2567 ได้หารือกับสำนักอัยการสูงสุดถึงแนวทางในการปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และกฎหมายลำดับรองที่เกี่ยวข้อง เพื่อนำไปใช้ในการยกระดับการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

3 การแลกเปลี่ยนองค์ความรู้ระดับภูมิภาคในงาน Regional Technical Dialogue on Combatting Cyber Scams ในวันที่ 8 พฤษภาคม 2567 เข้าร่วมเสวนา แบ่งปันความรู้ประสบการณ์ กับหน่วยงาน U.S. Department of State, International Narcotics and Law Enforcement Affairs, Bangkok U.S. Homeland Security Investigations Bangkok และหน่วยงานบังคับใช้กฎหมายในประเทศไทย ในประเด็นที่สำคัญ อาทิ การสืบสวนอาชญากรรมทางไซเบอร์ การวิเคราะห์ข้อมูลนิติวิทยาศาสตร์ การฟอกเงินผ่านระบบอิเล็กทรอนิกส์ โดยมีผู้เข้าร่วมการประชุมจากต่างประเทศ เช่น กัมพูชา อินโดนีเซีย มาเลเซีย สิงคโปร์ และเวียดนาม

Strengthening Legal Enforcement to Tackle Cyber Threats

- 1 Fostering Global Collaboration at the Security Analysis Summit (SAS):** From October 25 to 27, 2023, NCSA participated in the Security Analysis Summit (SAS) organized by Kaspersky. The summit brought together visionary speakers from the digital world, cybersecurity experts, and global law enforcement agencies. It featured a panel discussion on “**Securing Supply Chains in the Open-Source Era,**” aiming to foster collaboration and develop strategies to combat cyber threats. The initiative focused on strengthening organizational defenses and ensuring protection against cybersecurity risks.
- 2 Strengthening Cybersecurity Legislation:** On November 15, 2023, and January 19, 2024, the Office of the Attorney General held discussions to outline approaches for implementing the **Cybersecurity Act B.E. 2562 (2019)** and related secondary legislation. These efforts aimed to enhance prevention, response, and risk mitigation strategies against cyber threats, ultimately fortifying the nation's cybersecurity framework.
- 3 Regional Knowledge Sharing at the Regional Technical Dialogue on Combatting Cyber Scams:** On May 8, 2024, NCSA participated in the dialogue, exchanging knowledge and experiences with the U.S. Department of State, International Narcotics and Law Enforcement Affairs, U.S. Homeland Security Investigations Bangkok, and Thai law enforcement agencies. Key topics included cybercrime investigations, forensic data analysis, and electronic money laundering. Delegates from international agencies, including Cambodia, Indonesia, Malaysia, Singapore, and Vietnam, also attended the dialogue to enhance regional cooperation and expertise.



ประเมินผลสัมฤทธิ์พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

สทกช. ได้จัด **การประชุมรับฟังความคิดเห็น** เพื่อประเมินผลสัมฤทธิ์ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และกฎหมายลำดับรองที่เกี่ยวข้อง เมื่อวันที่ **14 สิงหาคม 2567** โดยมีผู้แทนจากหน่วยงานภาครัฐ หน่วยงานกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภาคเอกชน นักวิชาการ และประชาชนกว่า **400 คน** เข้าร่วมทั้งในรูปแบบ On-site และ Online ประเด็นสำคัญในการประชุม เช่น ความเหมาะสมของคำจำกัดความ “ภัยคุกคามทางไซเบอร์” อำนาจในการรวบรวมพยานหลักฐานของเจ้าหน้าที่ การอุทธรณ์คำสั่งรับมือภัยคุกคามร้ายแรง และวิกฤต ความคิดเห็นและข้อมูลที่ได้รับจะนำไปใช้ในการประเมินและพัฒนาเพื่อนำไปสู่การเสนอให้มีการแก้ไขเพิ่มเติมกฎหมายต่อไป



Evaluation of the Cybersecurity Act B.E. 2562 (2019): On August 14, 2024

The NCSA hosted a **public consultation meeting** to evaluate the Cybersecurity Act B.E. 2562 (2019) effectiveness and its related subordinate laws, which included participation from government agencies, regulators, organizations of critical information infrastructure, private organizations, academics, and over **400 attendees** in both On-site and Online formats. Key discussion topics included the authority for evidence collection by officials, and the appeal process for orders addressing severe and critical cyber threats.

The feedback and insights collected will inform **future amendments** to address existing gaps and challenges, ensuring the Cybersecurity Act effectively **enhances national prevention, response capabilities, and cyber resilience** against evolving threats.



กลยุทธ์ที่ 3.3 : การปกป้องระบบข้อมูล และเครือข่ายของหน่วยงานภาครัฐ Strategy 3.3 : Protecting the Information Systems and Networks of Government Agencies

มุ่งเน้นการสร้างความปลอดภัยตั้งแต่ขั้นพื้นฐานจนถึงการจัดการภัยคุกคามไซเบอร์สมัยใหม่ โดยกำหนดมาตรฐานขั้นต่ำที่ทุกหน่วยงานภาครัฐต้องปฏิบัติตาม พร้อมทั้งประเมินความเสี่ยงจากการใช้เทคโนโลยีตั้งแต่เริ่มต้นใช้งาน อีกทั้งยังสนับสนุนการมองภาพรวมของการดำเนินงานด้านไซเบอร์ในเชิงบูรณาการ พร้อมเตรียมความพร้อมในทุกมิติ ไม่ว่าจะเป็นบุคลากร ข้อมูล เทคโนโลยี และกระบวนการ เพื่อให้สามารถรับมือกับภัยคุกคามที่เปลี่ยนแปลงอยู่ตลอดเวลาได้อย่างมีประสิทธิภาพ

Establishing robust cybersecurity measures, from fundamental standards to advanced threat management. This includes enforcing minimum security policies for all government agencies, conducting risk assessments for technology use from the outset, and fostering a unified approach to cybersecurity operations. Additionally, it emphasizes comprehensive readiness in personnel, data, technology, and processes to counter evolving cyber threats effectively in the modern era.

กิจกรรมประเมินความเสี่ยงต่อภัยคุกคามไซเบอร์

สทท. ได้ริเริ่มกิจกรรม **ประเมินความเสี่ยงต่อภัยคุกคามไซเบอร์** ซึ่งเป็นโครงการสำคัญที่ดำเนินการต่อเนื่องทุกปี เพื่อวิเคราะห์และติดตามระดับความเสี่ยงทางไซเบอร์ของประเทศ โดยมุ่งเน้นการเตรียมพร้อมรับมือกับภัยคุกคามที่เปลี่ยนแปลงอยู่ตลอดเวลา กิจกรรมนี้ไม่เพียงช่วยให้เข้าใจภาพรวมของภัยคุกคามไซเบอร์ แต่ยังเป็นข้อมูลพื้นฐานที่สำคัญสำหรับการวางแผนป้องกันและลดความเสี่ยงตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

เมื่อวันที่ 6 กันยายน 2567 สทท. ได้จัดงานประชุมเพื่อรับฟังความคิดเห็นเกี่ยวกับ (ร่าง) กรอบการประเมินความเสี่ยงจากภัยคุกคามไซเบอร์ของประเทศไทย โดยมีผู้แทนจากหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศกว่า 100 คนเข้าร่วม งานนี้เป็นเวทีสำคัญที่เปิดโอกาสให้ทุกภาคส่วนได้แลกเปลี่ยนความคิดเห็นผ่านการ Focus Group เพื่อนำข้อมูลดังกล่าวมาปรับปรุง (ร่าง) **กรอบการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ของประเทศไทย** หรือ **Thailand National Cyber Risk Assessment Framework (NCRAF)** ให้สมบูรณ์แบบยิ่งขึ้น และสร้างมาตรฐานการประเมินความเสี่ยงไซเบอร์ระดับประเทศที่ครอบคลุม





Strengthening Cybersecurity with a National Risk Assessment Framework

The NCSA has launched the **Cyber Threat Risk Assessment initiative**, a key annual project designed to analyze and monitor the nation's cyber risks. This initiative offer an in-depth-view of emerging cyber threats, serving as a foundation for strategies to prevent, mitigate, and reduce such risks following the Cybersecurity Act B.E. 2562.

On September 6, 2024, NCSA hosted a stakeholder consultation meeting to gather feedback on the draft **Thailand National Cyber Risk Assessment Framework (NCRAF)**. The event brought together over 100 representatives from government agencies, regulators, organizations of critical information infrastructure. This forum served as a platform for constructive dialogue, enabling stakeholders to share insights and refine the draft framework. The goal is establishing a robust national standard for cyber risk assessment, ensuring preparedness against ever-evolving cyber threats.

การปกป้องระบบข้อมูลและเครือข่ายของหน่วยงาน

สทช. ได้มีการดำเนินการปกป้องระบบข้อมูลและเครือข่ายของหน่วยงาน เพื่อป้องกันภัยคุกคามทางไซเบอร์ให้กับหน่วยงานอย่างมีประสิทธิภาพ ดังนี้

1 ความร่วมมือกับเมตาในการสนับสนุนเครื่องหมาย Meta Verified

สทช. ร่วมกับ Meta Platforms และ สภาองค์กรของผู้บริโภค เพื่อแก้ปัญหาการเพิ่มขึ้นของเฟกปลอมที่แอบอ้างเป็นหน่วยงานภาครัฐ โดยมีเป้าหมายป้องกันความเสียหายต่อรัฐและประชาชน และมีการจัดอบรมเชิงปฏิบัติการ เรื่องการสร้างความตระหนักและแนวทางการแก้ปัญหาเฟกปลอม เมื่อวันที่ 24 กรกฎาคม 2567 โดยมีหน่วยงานเข้าร่วมกว่า 5,000 หน่วยงาน



Meta Verified คืออะไร?

Meta Verified คือ ระบบยืนยันตัวตนที่ทาง Meta ทำขึ้นมา เพื่อแก้ไขปัญหาเฟกปลอมและการแอบอ้างนำรูปไปใช้ในช่องทางโซเชียลมีเดีย ซึ่งมีความสำคัญอย่างยิ่งในการหลอกลวงผู้คนในโซเชียลมีเดีย ไม่ว่าจะเป็นการหลอกลวงเงิน นามข้อมูลไปใช้ และอื่น ๆ อีกมากมาย

Meta Verified มีข้อดีอย่างไรบ้าง

การสมัครสมาชิก Meta Verified จะได้รับเครื่องหมายยืนยันรับรองการมีตัวตน เพื่อให้ผู้ติดตามหรือผู้ใช้งาน Facebook คนอื่น ๆ ได้ติดตามบัญชีจริงเท่านั้น ป้องกันการแอบอ้างข้อมูลเข้าถึงข้อมูล และได้รับการช่วยเหลือจากทีมพัฒนาอย่างรวดเร็ว Meta Verified

ประโยชน์ของ Meta Verified

1. ตราสัญลักษณ์ยืนยันตัวตน (Verified Badge) トラสัญลักษณ์ยืนยันตัวตนกว่า 100 ล้านคนทั่วโลก ได้รับจากบริษัทเทคโนโลยีชั้นนำ
2. การปกป้องบัญชีจากการปลอมแปลง ระบบจะตรวจสอบและแจ้งเตือนการปลอมแปลงบัญชีให้ผู้ใช้ทราบ เพื่อความปลอดภัยของบัญชี
3. บริการช่วยเหลือพิเศษสำหรับ Meta Verified สามารถติดต่อขอรับบริการช่วยเหลือผ่านทางอีเมลและแชทได้โดยตรง เมื่อแก้ไขปัญหาต่าง ๆ ที่เกี่ยวข้องกับบัญชี
4. โปรไฟล์ที่โดดเด่นยิ่งขึ้น เพิ่มสิ่งกีดขวางการปลอมแปลงโปรไฟล์ให้ชัดเจนยิ่งขึ้น เพื่อสร้างความน่าเชื่อถือและดึงดูดผู้ติดตาม
5. สติ๊กเกอร์พิเศษเฉพาะสมาชิก รับสติ๊กเกอร์พิเศษสำหรับใช้งานบน Stories และ Reels เพิ่มความโดดเด่นและสร้างความแตกต่างให้กับเนื้อหาของคุณ

หน่วยงานของท่านได้ผ่านการตรวจสอบหลักฐานเบื้องต้น และได้รับอนุญาตให้เข้าร่วมกิจกรรมดังกล่าวแล้ว สทช. ได้ส่งอีเมลแจ้งเตือนและเชิญชวนให้ท่านเข้าร่วมกิจกรรมแล้ว กรุณาตรวจสอบอีเมลที่ท่านลงทะเบียนไว้เพื่อรับสิทธิ์ 20 กรกฎาคม 2567 จนถึงวันหมดเขต

สอบถามรายละเอียดเพิ่มเติมได้ที่
thaicert@nca.or.th
02-114-3531



กำหนดการอบรมเชิงปฏิบัติการ เรื่อง สร้างความตระหนัก การจัดการปัญหา Facebook Page ปลอม ที่แอบอ้างเป็นหน่วยงานราชการ วันพุธที่ 24 กรกฎาคม 2567

09:30 - 10:00 น. ลงทะเบียนเพื่อรับบัตร เข้าร่วมอบรม

10:00 - 10:15 น. พิธีเปิดการอบรม และบรรยายในหัวข้อ "การสร้างความปลอดภัยและการจัดการ Facebook Page ปลอมในประเทศไทย"

10:15 - 10:25 น. บรรยายในหัวข้อ "การปฏิบัติการเชิงรุกเพื่อแก้ไขปัญหาการหลอกลวงโดยวิธีสังเกตและป้องกัน"

10:25 - 10:35 น. บรรยายในหัวข้อ "ปัญหาการใช้สื่อสังคมออนไลน์กับภัยคุกคามทางไซเบอร์ด้านสาธารณะ"

10:35 - 10:45 น. บรรยายในหัวข้อ "บทบาทของผู้บริโภคในการแก้ไขปัญหาเฟกปลอม"

10:45 - 10:50 น. บรรยายในหัวข้อ "วิธีสังเกตและแก้ไขเฟกปลอม Meta และแอปพลิเคชันอื่น ๆ กับสำนักงานคณะกรรมการการหักภาษีเงินได้บุคคลธรรมดา (กรมสรรพากร)"

10:50 - 11:55 น. ช่วงอบรมเชิงปฏิบัติการและแลกเปลี่ยนเรียนรู้การตรวจสอบบัญชี Meta Verified

- แนะนำระบบการแจ้งเตือนและความปลอดภัยสำหรับบัญชีผู้ใช้งาน
- วิธีการใช้งานพื้นฐาน
- แนวทางการใช้งานและรักษาความปลอดภัยของบัญชีผู้ใช้งาน
- แหล่งข้อมูลเพิ่มเติมที่เป็นประโยชน์

12.00 น. สรุปกิจกรรมวันและปิดการอบรม

หน่วยงานของท่านได้มีการตรวจสอบหลักฐานเบื้องต้น และได้รับอนุญาตให้เข้าร่วมกิจกรรมดังกล่าวแล้ว สทช. ได้ส่งอีเมลแจ้งเตือนและเชิญชวนให้ท่านเข้าร่วมกิจกรรมแล้ว กรุณาตรวจสอบอีเมลที่ท่านลงทะเบียนไว้เพื่อรับสิทธิ์ 20 กรกฎาคม 2567 จนถึงวันหมดเขต

สอบถามรายละเอียดเพิ่มเติมได้ที่
thaicert@nca.or.th
02-114-3531

2 ศูนย์ปฏิบัติการเฝ้าระวังและตอบสนองภัยคุกคามทางไซเบอร์ สำหรับระบบสนับสนุนการเลือกตั้งสมาชิกวุฒิสภา 2567

สทช. ได้จัดตั้งศูนย์ปฏิบัติการเฝ้าระวังและตอบสนองภัยคุกคามทางไซเบอร์ สำหรับระบบสนับสนุนการเลือกตั้งสมาชิกวุฒิสภา 2567 ระหว่างวันที่ 14 มิถุนายน 2567 - 4 กรกฎาคม 2567 โดยในห้วงดังกล่าว สทช. ตรวจพบช่องโหว่ที่ผู้ไม่หวังดีอาจนำข้อมูลส่วนบุคคลออกมาเผยแพร่ สทช. ได้ดำเนินการประสานเร่งด่วนไปยังสำนักงานคณะกรรมการการเลือกตั้ง (กกต.) โดยให้คำแนะนำและดำเนินการแก้ไข เพื่อให้หน่วยงานสามารถป้องกันเหตุภัยคุกคามทางไซเบอร์ได้

Protecting Agency Data Systems and Networks

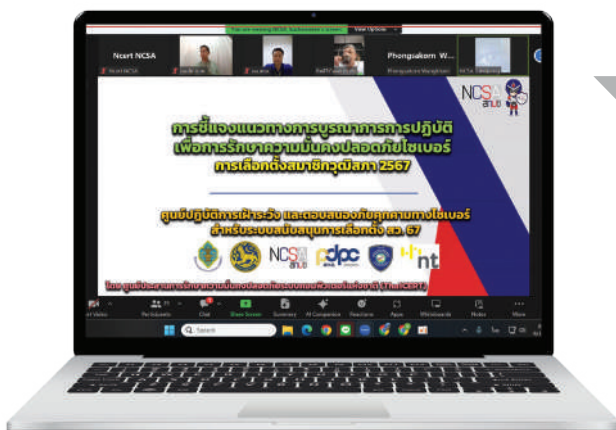
The NCSA has undertaken measures to safeguard agency information systems and networks, ensuring effective protection against cyber threats.

1. Collaboration with Meta to Implement Meta Verified for Government Pages

To address the rising number of fake government pages, NCSA collaborated with **Meta Platforms and the Consumer Council** to prevent potential damage to the state and the public. On **July 24, 2024, over 5,000 agencies** participated in a workshop on awareness and managing fake Facebook pages.

2. Cyber Threat Monitoring and Response Center for the 2024 Senate Election Support System

The NCSA established a **Cyber Threat Monitoring and Response Center to support the 2024 Senate Election System**, operating from June 14 to July 4, 2024. During this period, NCSA identified vulnerabilities that could potentially allow malicious actors to expose personal data. NCSA took immediate action by coordinating with the **Office of the Election Commission of Thailand (ECT)** to address and resolve the issue, providing guidance to ensure the agency could effectively prevent further cyber threats.



ยุทธศาสตร์ที่ 4

สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพ และมาตรฐาน (Standard)

Strategy 4: Enhancing the Capacity and Standards of National Agencies (Standard)

เน้นการเสริมสร้างศักยภาพและมาตรฐานของหน่วยงานระดับชาติ เพื่อให้การบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพและครอบคลุมทุกมิติ โดยมุ่งสู่การบริหารจัดการแบบบูรณาการ การพัฒนามาตรการป้องกันภัยคุกคาม และการแบ่งปันข้อมูลที่มีประสิทธิภาพ เพื่อความมั่นคงปลอดภัยของโครงสร้างพื้นฐานสำคัญของประเทศ

Enhancing the capacity and standards of national agencies to ensure effective and comprehensive cybersecurity management. It aims to promote integrated governance, develop robust threat prevention measures, and enable efficient information sharing to safeguard the nation's critical infrastructure.





กลยุทธ์ที่ 4.1 : เพิ่มขีดความสามารถในการรับมือ และตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับ ความมั่นคงปลอดภัยไซเบอร์

Strategy 4.1 : Enhance the Capacity to Handle and Respond to Cybersecurity Incidents

มุ่งเพิ่มขีดความสามารถในการรับมือและตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ด้วยการทบทวนนโยบายและศักยภาพที่มีอยู่ กำหนดกลไกการขับเคลื่อนที่ชัดเจน พัฒนาคมน กระบวนการ และเทคโนโลยีให้ได้มาตรฐาน พร้อมสนับสนุนการจัดตั้งทีม CSIRT และแผนฉุกเฉิน เพื่อเสริมความมั่นคงและสร้างความเชื่อมั่นในระบบโครงสร้างพื้นฐาน

Enhancing the capacity to respond to cybersecurity incidents involves reviewing existing policies and capabilities, establishing precise strategic mechanisms, and advancing people, processes, and technology to meet industry standards. This includes forming a CSIRT team and developing emergency plans to strengthen the resilience of critical infrastructure and build stakeholder confidence.

กิจกรรมการพัฒนาระบบ Smart Back Office ให้สามารถสนับสนุนงานหลักได้ทุกกระบวนการ

สกมช. ได้เพิ่มขีดความสามารถในการรับมือและตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ โดยมีการใช้งานระบบ e-Saraban ที่เสริมการจัดการเอกสารดิจิทัลให้มีประสิทธิภาพ นำระบบ Zabbix ซึ่งพัฒนามาจาก OpenSource มาใช้สำหรับตรวจสอบและเฝ้าระวังโครงสร้างพื้นฐานไอที เช่น เครือข่าย เซิร์ฟเวอร์ และบริการคลาวด์ ส่งผลให้ สกมช. มีความพร้อมมากขึ้นในการดูแลและฟื้นฟูบริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างทันต่อภัยคุกคาม

Development of the Smart Back Office System to Support All Core Processes

The NCSA has enhanced its capacity to handle and respond to cybersecurity incidents by **implementing the e-Saraban system, which improves the efficiency of digital document management. Additionally, NCSA has adopted Zabbix, an open-source system for monitoring and managing IT infrastructure, including networks, servers, and cloud services.** These advancements have significantly enhanced the NCSA's ability to efficiently manage and restore critical information infrastructure services in the event of potential threats.



กิจกรรมการจัดทำแผนแม่บท ICT และ Enterprise Architecture และปรับปรุงระบบเทคโนโลยีสารสนเทศสำนักงาน

สทศ. ได้พัฒนาและปรับปรุงแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Master Plan) และสถาปัตยกรรมองค์กร (Enterprise Architecture) ระยะ 5 ปี (พ.ศ. 2566 – 2570) ให้ทันสมัยและสอดคล้องกับ Cloud First Policy ของรัฐบาล กรอบมาตรฐานสากล เช่น NIST Framework 2.0 รวมถึงการเปลี่ยนแปลงของเทคโนโลยีในปัจจุบัน อีกทั้งยังได้เพิ่ม Security Architecture เพื่อให้ครอบคลุมประเด็นด้านความมั่นคงปลอดภัยไซเบอร์อย่างรอบด้าน แผนดังกล่าวได้รับการลงนามโดย เลขาธิการฯ เมื่อวันที่ 24 กันยายน 2567 ซึ่งสะท้อนถึงความมุ่งมั่นในการพัฒนาระบบเทคโนโลยีสารสนเทศที่รองรับการเปลี่ยนแปลงและยกระดับความมั่นคงปลอดภัยไซเบอร์ของประเทศ

Development of the ICT Master Plan and Enterprise Architecture and Enhancement of Office IT Systems

The NCSA has modernized its **ICT Master Plan and Enterprise Architecture for 2023–2027** to align with the government's Cloud First Policy, international standards such as the NIST Framework 2.0, and the rapidly evolving technological landscape. The updated architecture now includes a Security Architecture to comprehensively address cybersecurity concerns. This initiative highlights the NCSA's commitment to advancing its IT systems to adapt to change while strengthening national cybersecurity resilience. The Secretary-General of the National Cybersecurity Committee officially signed the plan on September 24, 2024.



SECURITY ARCHITECTURE

การพัฒนาความรู้และทักษะด้านไซเบอร์บุคลากร สกมช.

สกมช. มุ่งมั่นในการเสริมสร้างศักยภาพด้านความมั่นคงปลอดภัยทางไซเบอร์ให้แก่บุคลากรอย่างรอบด้านและทันสมัยอยู่เสมอ สะท้อนความตั้งใจในการสร้างทีมที่มีประสิทธิภาพและพร้อมเผชิญหน้ากับความท้าทายใหม่ ๆ บนโลกดิจิทัลผ่านกิจกรรมต่าง ๆ ต่อไปนี้

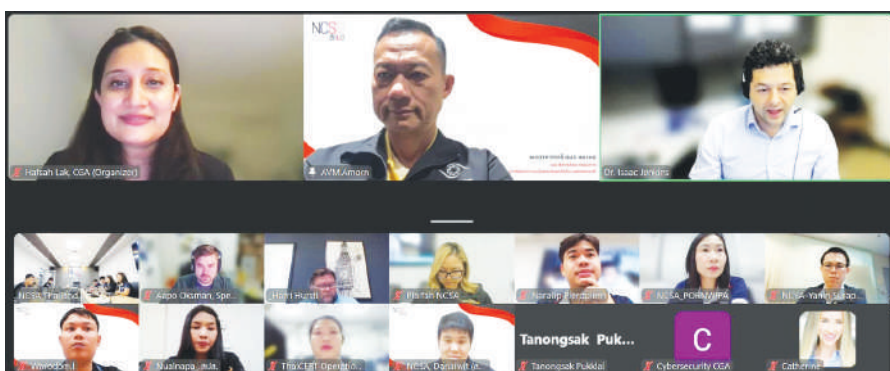
- 1 The Global Cyber Awareness Month Training** เมื่อวันที่ 13 พฤศจิกายน 2566 สกมช. ได้จัดอบรมให้แก่บุคลากรจำนวนกว่า **40 คน** โดยมีคุณจิตรกร จูภากาญจน์ ผู้อำนวยการความมั่นคงปลอดภัยไซเบอร์ ธนาคาร HSBC ประเทศไทย เป็นวิทยากร ถ่ายทอดประสบการณ์เพื่อพัฒนาความรู้และทักษะเชิงปฏิบัติสำหรับผู้ปฏิบัติงาน สร้างศักยภาพในการรับมือภัยคุกคามไซเบอร์ พร้อมนำเสนอแนวปฏิบัติที่สามารถนำไปปรับใช้ได้จริง



- 2 NCSA: GenAI for Smart Workforce** วันที่ 24 มกราคม 2567 ได้จัดอบรมให้บุคลากร **60 คน** เพื่อส่งเสริมการประยุกต์ใช้เทคโนโลยี AI ในการทำงานอย่างมีประสิทธิภาพ การอบรมเน้นการใช้งานที่เหมาะสมและการแก้ปัญหาโดยใช้ AI เพื่อสนับสนุนการดำเนินงานในยุคดิจิทัล



- 3 การอบรมขั้นสูงด้านความมั่นคงปลอดภัยทางไซเบอร์** ในวันที่ 29-30 สิงหาคม 2567 ร่วมมือกับ Cambridge Global ประเทศสหรัฐอเมริกา จัดการอบรมเชิงปฏิบัติการด้าน **Threat Landscape, AI, และการป้องกันระบบ ICS/SCADA** ให้กับบุคลากร **31 คน** เพื่อพัฒนาความรู้และกลยุทธ์เชิงลึกด้านความมั่นคงปลอดภัยไซเบอร์



Cybersecurity Knowledge Enhancement Programs

- 1. Global Cyber Awareness Month Training:** On November 13, 2023, the NCSA organized a “Global Cyber Awareness Month” training session attended by over 40 personnel. The session focused on cybersecurity expert **Mr. Jitrakorn Juthakarn, Director of Cybersecurity at HSBC Thailand**, sharing best practices and real-world experiences for implementing cyber awareness initiatives.
- 2. NCSA: GenAI for Smart Workforce:** On January 24, 2024, the NCSA conducted the training, which gathered **60 personnel** to explore integrating AI tools in enhancing daily operations. The training emphasized AI's efficient and ethical application in communication, research, and problem-solving, equipping attendees with skills to maximize AI benefits while mitigating risks.
- 3. Advanced Cybersecurity Workshops:** In collaboration with **Cambridge Global (USA)**, the NCSA hosted an advanced cybersecurity workshop on August 29-30, 2024, with 31 participants. Topics included Threat Landscape, Threat Hunting & Intelligence, Vehicle Forensic Investigation, AI, and ICS/SCADA system threats.

การพัฒนาทักษะการรับฟังและการให้คำปรึกษาให้เจ้าหน้าที่ AOC

สภมช. ร่วมกับกระทรวงดิจิทัลฯ และ NT จัดอบรม “Deep Listening: Listening with Heart” ใ้บุคลากรศูนย์ AOC (Anti Online Scam Operation Center) จำนวน **60 คน** เพื่อพัฒนาทักษะการรับฟังและการให้คำปรึกษาที่มีประสิทธิภาพแก่ผู้ที่ได้รับผลกระทบจากภัยคุกคามไซเบอร์ โดยมีผู้เชี่ยวชาญจากกระทรวงสาธารณสุขเป็นวิทยากร

Listening and Counseling Skill Training for AOC Staff

The NCSA with MDES and NT conducted the “Deep Listening: Listening with Heart” workshop for **60 AOC staff**. The training focused on enhancing empathetic listening, counseling skills, and stress management to better support cybercrime victims while safeguarding the mental well-being of the counselors themselves.



การสื่อสาร บทบาทและส่งเสริม ภาพลักษณ์องค์กร

NEWS CLIPPING
407 ข่าว



EXHIBITIONS

23
ครั้ง



**การเผยแพร่
ผ่านช่องทาง
SOCIAL MEDIA**
Social Media Posts

645
โพสต์



**กิจกรรม
CSR**

4
ครั้ง



รวมทั้งหมด 1,079
ครั้ง

Communicating Organizational Roles and Responsibilities to Raise Cybersecurity Awareness in the Public



เครือข่ายประชาสัมพันธ์ PUBLIC RELATIONS NETWORK

สร้างเครือข่ายความร่วมมือกับชุมชนและองค์กรท้องถิ่น รวมถึงภาคีเครือข่ายกว่า 10 หน่วยงาน ในการประชาสัมพันธ์ ข้อมูลไปยังชุมชน องค์กรปกครองส่วนท้องถิ่น หรือสถานศึกษา เพื่อช่วยเผยแพร่ข้อมูลไปถึงประชาชนในวงกว้าง



สภมช. X WHOSCALL แจ้งเตือนภัยไซเบอร์ผ่าน SCAM ALERTS

ผู้ใช้งาน Whoscall สามารถเปิดการแจ้งเตือนอัตโนมัติบนแอปพลิเคชันเพื่อรับข้อมูลแจ้งเตือนภัยมิจฉาชีพที่สำคัญและเร่งด่วน แบบเรียลไทม์



รายการสายลับไซเบอร์

ออกอากาศทาง FM 96.0 MHz เป็นประจำทุกวันอาทิตย์ พร้อมนำเสนอสารความรู้และข่าวสารเกี่ยวกับโลกไซเบอร์ การอัปเดตเทคโนโลยี และเรื่องราวน่าสนใจ ที่จะช่วยให้คุณพร้อมรับมือกับภัยในโลกดิจิทัล



โครงการ "ดิจิทัลพลัส" แอปพลิเคชัน "ทางรัฐ" ปลดล็อกใหม่ ห้าอะไรได้น่าใจ ep.1 สานสนไซเบอร์



Romance Scam แก๊งหลอกกรอออนไลน์ ที่ผู้หญิงหรือผู้ชายตกเป็นเหยื่อได้ ep.9 สานสนไซเบอร์

การส่งเสริมความร่วมมือในประชาคมไซเบอร์

สทศ. ได้จัดกิจกรรม 4 ครั้งที่สำคัญ โดยเน้นการเชื่อมโยงหน่วยงานทั้งภาครัฐ เอกชน และภาคประชาสังคม เพื่อแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ องค์ความรู้ และแนวทางปฏิบัติที่ทันสมัย รวมถึงการส่งเสริมความตระหนักรู้ในระดับประเทศ และยกระดับขีดความสามารถของเศรษฐกิจดิจิทัล

ครั้งที่ 1 การประชุมหารือแนวทางจัดตั้งประชาคมไซเบอร์แห่งชาติ มีเป้าหมายเพื่อบูรณาการการดำเนินการในด้านการเฝ้าระวังและตอบสนองภัยคุกคามทางไซเบอร์ พร้อมทั้งแลกเปลี่ยนแนวคิดและข้อเสนอแนะในการแก้ปัญหาความมั่นคงปลอดภัย รวมถึงข้อจำกัดที่ต้องปรับปรุงให้เกิดผลลัพธ์ที่ยั่งยืน

ครั้งที่ 2 กิจกรรมอบรมสัมมนาเชิงปฏิบัติการความมั่นคงทางไซเบอร์ ให้กับหน่วยงาน Sectoral CERT ต่าง ๆ หน่วยงาน CII หน่วยงานกำกับดูแล หน่วยงานรัฐ และหน่วยงานอื่น ๆ เพื่อให้เกิดความเชื่อมโยงและแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ ได้อย่างมีประสิทธิภาพ

ครั้งที่ 3 การหารือด้านความมั่นคงปลอดภัยของการใช้บริการคลาวด์ ส่งเสริมการพัฒนาเศรษฐกิจดิจิทัลที่ยั่งยืน และการยกระดับความสามารถทางการแข่งขัน โดยผลักดันให้เกิดเครือข่ายความร่วมมือที่เข้มแข็ง

ครั้งที่ 4 มุ่งเน้นด้านการศึกษาเพื่อสร้าง “พลเมืองไซเบอร์” ที่มีความรู้ ความเข้าใจ และสามารถปกป้องตนเองจากภัยคุกคามบนโลกออนไลน์ พร้อมสนับสนุนการปรับปรุงหลักสูตรให้สอดคล้องกับเทคโนโลยีและการใช้งานออนไลน์



Enhancing Collaboration within the Cyber Community

The NCSA organized four key activities to foster a robust network of collaboration in the cyber community, connecting public, private, and civil sectors. These events emphasized threat intelligence exchange, modernizing best practices, and raising national awareness to strengthen cybersecurity while boosting the digital economy.

- ▶ **Event 1: A national dialogue to establish the Cyber Community** to integrate monitoring and response mechanisms for cyber threats. Participants exchanged insights and proposed improvements to address challenges, ensuring sustainable outcomes.
- ▶ **Event 2: A cybersecurity workshop** and training program was conducted for Sectoral CERTs, organizations of critical information infrastructure, regulators, government agencies, and other entities to enhance collaboration and facilitate effective cyber threat information sharing.
- ▶ **Event 3: Discussion on the importance of secure cloud usage** and fostering a sustainable digital economy. Discussions emphasized building a strong collaborative network to enhance competitiveness and national digital capabilities.
- ▶ **Event 4: Centered on education to develop “cyber citizens”** with the knowledge and skills to protect themselves from online threats. It also promoted curriculum updates to match the rapid evolution of digital technology and online safety requirements.

These four activities collectively attracted 19,542 participants, reflecting the NCSA's success in driving national collaboration and awareness in the cybersecurity landscape.



กิจกรรมการปรับปรุงพัฒนาพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

The Enhancement of the Cybersecurity Act

สภมช. มุ่งมั่นดำเนินการเพื่อยกระดับการป้องกันและรับมือภัยคุกคามไซเบอร์ในระดับประเทศ ด้วยเป้าหมายเพื่อเสริมสร้างมาตรฐานและกรอบกฎหมายให้สอดคล้องกับสถานการณ์ในปัจจุบันและแนวโน้มในอนาคต โดยสามารถดำเนินงานตามคำเป้าหมายขั้นสูงได้สำเร็จ นำส่งกฎหมายลำดับรองไปประกาศในราชกิจจานุเบกษา รวมทั้งสิ้น 6 ฉบับ

Enhancing the Cybersecurity Act is a critical initiative undertaken by the NCSA to strengthen national capabilities in combating cyber threats. This effort aims to modernize legal frameworks and establish robust standards to address current and emerging cybersecurity challenges.

- 1 ประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 (ประกาศในราชกิจจานุเบกษา เล่มที่ 141 ตอนพิเศษ 18 ง ลงวันที่ 18 ม.ค. 67)
Notification of the National Cyber Security Committee (NCSC) on Cybersecurity Standards for Information or Information Systems, B.E. 2566 (2023) (Published in the Royal Gazette, Volume 141, Special Part 18 Ng, dated January 18, 2024)



- 2 ประกาศ กมช. เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 (ประกาศในราชกิจจานุเบกษา เล่มที่ 141 ตอนพิเศษ 18 ง ลงวันที่ 18 ม.ค. 67)
Notification of the National Cyber Security Committee (NCSC) on Minimum Standards for Information or Information Systems, B.E. 2566 (2023) (Published in the Royal Gazette, Volume 141, Special Part 18 Ng, dated January 18, 2024)



- 3 ประกาศ กมช. เรื่อง มาตรฐานและแนวทางการส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566 (ประกาศในราชกิจจานุเบกษา เล่มที่ 141 ตอนพิเศษ 18 ง ลงวันที่ 18 ม.ค. 67)
Notification of the National Cyber Security Committee (NCSC) on Standards and Guidelines for Promoting and Developing Cybersecurity Service Systems, B.E. 2566 (2023) (Published in the Royal Gazette, Volume 141, Special Part 18 Ng, dated January 18, 2024)



- 4 ประกาศ กกม. เรื่อง หน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานควบคุมหรือกำกับดูแล พ.ศ. 2567 (ประกาศในราชกิจจานุเบกษา เล่มที่ 141 ตอนพิเศษ 51 ง ลงวันที่ 22 ก.พ. 67)
Notification of the Cybersecurity Regulating Committee (CRC) on Obligations for Critical Information Infrastructure Organizations and Regulatory Agencies, B.E. 2567 (2024) (Published in the Royal Gazette, Volume 141, Special Part 51 Ng, dated February 22, 2024)



- 5 ประกาศ กมช. เรื่อง มาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2567 (ประกาศในราชกิจจานุเบกษา เล่มที่ 141 ตอนพิเศษ 248 ง ลงวันที่ 10 ก.ย. 67)
Notification of the National Cyber Security Committee (NCSC) on Measures and Guidelines for Enhancing Knowledge, Skills, and Expertise in Cybersecurity, B.E. 2567 (2024) (Published in the Royal Gazette, Volume 141, Special Part 248 Ng, dated September 10, 2024)



หน้า ๕
เล่ม ๑๔๑ ตอนพิเศษ ๑๘ ง ราชกิจจานุเบกษา ๑๘ มกราคม ๒๕๖๗
ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์
ให้แก่ข้อมูลหรือระบบสารสนเทศ
พ.ศ. ๒๕๖๖

หน้า ๙
เล่ม ๑๔๑ ตอนพิเศษ ๑๘ ง ราชกิจจานุเบกษา ๑๘ มกราคม ๒๕๖๗
ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ
พ.ศ. ๒๕๖๖

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้
คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีหน้าที่และอำนาจตามพระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับการรักษา
ระบบคอมพิวเตอร์ หรือโปรแกรมคอมพิวเตอร์ จึงสมควรมีมาตรการในการควบคุมลักษณะความมั่นคง
ปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ เพื่อประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นแก่
ข้อมูลหรือระบบสารสนเทศอันเนื่องมาจากการเลือกมาตรการในการควบคุมความมั่นคงปลอดภัยไซเบอร์
เพื่อให้การดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ
และบรรลุวัตถุประสงค์

โดยที่พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัย
พ.ศ. ๒๕๖๒ ประกอบกับ
ใบตรวจการประชุมนัดที่
ความมั่นคงปลอดภัยไซเบอร์

104 รายงานประจำปี 2567 สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

6

ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 (ประกาศในราชกิจจานุเบกษา เล่มที่ 141 ตอนพิเศษ 248 ง ลงวันที่ 10 ก.ย. 67)

Notification of the National Cyber Security Committee (NCSC) on Cybersecurity Standards for Cloud Systems, B.E. 2567 (2024) (Published in the Royal Gazette, Volume 141, Special Part 248 Ng, dated September 10, 2024)



ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567



ประกาศในราชกิจจานุเบกษา
10 กันยายน 2567

มีผลบังคับใช้
เมื่อพ้นกำหนดสองปี
นับตั้งแต่วันที่ประกาศในราชกิจจานุเบกษา



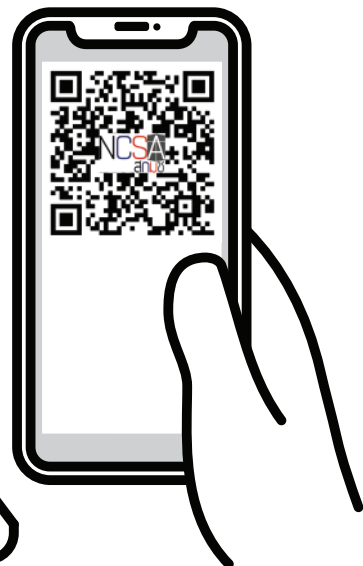
- ▶ บังคับใช้กับหน่วยงาน GOV REG CII ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 รวมถึงผู้ให้บริการคลาวด์กับหน่วยงานดังกล่าวข้างต้นด้วย
- ▶ กำหนดมาตรการฯ สำหรับผู้ใช้บริการคลาวด์ รวมถึงผู้ให้บริการคลาวด์สาธารณะ (Public Cloud Service Provider) เฉพาะที่ต้องให้บริการกับผู้ใช้บริการคลาวด์ที่เป็นหน่วยงาน GOV REG CII ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยใช้ฐานสัญญาณระหว่างผู้ใช้บริการคลาวด์กับผู้ให้บริการคลาวด์
- ▶ ผู้ที่เกี่ยวข้องกับมาตรฐานฉบับนี้ ประกอบด้วย หน่วยงาน GOV REG CII ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 รวมถึงผู้ตรวจสอบภายในด้านความมั่นคงปลอดภัยไซเบอร์และหน่วยงานให้บริการตรวจสอบรับรอง (Certity Body)



เจตนารมณ์

ด้วยนโยบายของรัฐบาลที่ต้องการขับเคลื่อนทางเศรษฐกิจ การเมือง สังคม และสิ่งแวดล้อม ด้วยข้อมูลที่แม่นยำและทันสมัย เป็นรัฐบาลที่น่าเอาเทคโนโลยีและระบบดิจิทัล มาใช้อย่างเต็มรูปแบบ เพื่อประโยชน์ของประเทศชาติและประชาชน มุ่งเน้นการบริหารประเทศในรูปแบบบูรณาการการทำงานร่วมกันระหว่างหน่วยงาน

สทกช. ในฐานะหน่วยงานระดับชาติที่มีหน้าที่รับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ จึงได้จัดทำ ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 เพื่อสนับสนุนนโยบาย Cloud First Policy และเพื่อให้หน่วยงานของรัฐ รวมทั้งภาคเอกชนที่เกี่ยวข้อง ได้รับประโยชน์สูงสุดจากการดำเนินการตามนโยบายดังกล่าว



กิจกรรมพัฒนาศักยภาพพนักงานเจ้าหน้าที่ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Protection Team – CPT)

ในปี 2567 สกมช. ได้เสริมสร้างศักยภาพและความพร้อมของพนักงานเจ้าหน้าที่ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือ CPT ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 จำนวน **87 ราย** ให้มีความเชี่ยวชาญตามอำนาจและหน้าที่ตามมาตรา 62 และมาตรา 66 เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยมีบทบาทสำคัญ เช่น การวิเคราะห์สถานการณ์ภัยคุกคาม การเข้าถึงข้อมูลสำคัญและการตรวจสอบสถานที่และระบบไอทีที่เกี่ยวข้อง เพื่อยกระดับการปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศให้มีประสิทธิภาพสูงสุด



Capacity Development Program for Cyber Protection Team (CPT) under the Cybersecurity Act

In 2024, the NCSA enhanced the capabilities and readiness of **87 Cybersecurity Protection Team (CPT) officials** under the Cybersecurity Act B.E. 2562 (2019). These officials were trained to specialize in their roles and responsibilities as outlined in Sections 62 and 66 of the Act. Their duties include analyzing threat scenarios, accessing critical information, and inspecting relevant locations and IT systems. These efforts aim to strengthen the nation's ability to prevent, respond to, and mitigate cyber threats, ensuring maximum effectiveness in cybersecurity operations across the country.

การสร้างรายได้จากการให้บริการด้านความมั่นคงปลอดภัยไซเบอร์

สกมช. ได้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อสร้างรายได้และเสริมความเข้มแข็งให้กับองค์กร โดยได้ดำเนินการ **ให้บริการงานประเมินความเสี่ยงและทดสอบช่องโหว่ของระบบ (Pentest) สำหรับระบบ Incentive OSS** เฉพาะหน้าเว็บ ซึ่งเป็นบริการที่ช่วยเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับระบบสำคัญของหน่วยงานต่าง ๆ สะท้อนถึงความเชื่อมั่นของหน่วยงานที่ใช้บริการ พร้อมตอกย้ำความเชี่ยวชาญของ สกมช. ในการสนับสนุนการป้องกันภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ

Revenue Generation Initiative through Cybersecurity Services

The NCSA has generated revenue and strengthened its operational capabilities by **providing risk assessment and vulnerability testing services (Pentest) for the Incentive OSS system**, focusing specifically on its web interface. This service, aimed at enhancing the cybersecurity resilience of critical system. This initiative reflects the trust and confidence placed in the NCSA's expertise and highlights its commitment to delivering effective cybersecurity solutions to mitigate evolving cyber threats.

การย้ายและปรับปรุงสำนักงาน สกมช. ณ ศูนย์ราชการเฉลิมพระเกียรติฯ โซนซี

สกมช. ได้ดำเนินการย้ายและปรับปรุงสำนักงานใหม่ ณ ศูนย์ราชการเฉลิมพระเกียรติฯ โซนซี อย่างมีประสิทธิภาพ โดยสรุปผลการดำเนินงานสำคัญ ดังนี้

- 1** บริหารงบประมาณประจำปี 2567 ได้อย่างมีประสิทธิภาพและโปร่งใส
- 2** จัดทำบัญชีวัสดุ อุปกรณ์ และครุภัณฑ์ ที่ต้องการขนย้าย พร้อมรายการวัสดุที่ส่งคืน
- 3** สำรวจพื้นที่เพื่อวางแผนดำเนินงาน และติดตามความคืบหน้าของการก่อสร้าง
- 4** ได้รับอนุมัติโครงการและแต่งตั้ง คณะกรรมการที่เกี่ยวข้องเพื่อสนับสนุน การดำเนินงาน
- 5** ปฏิบัติตามแผนงานที่กำหนด โดยเข้าสำรวจ พื้นที่ก่อสร้างตั้งแต่วันที่เดือนมกราคม 2567 หลังได้รับอนุญาตจากบริษัท ธนาภิรมย์ พัฒนาสินทรัพย์ จำกัด (swa.)

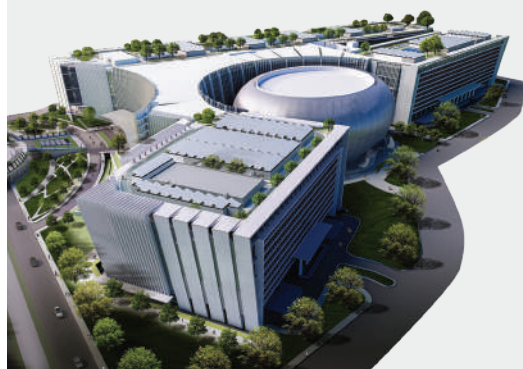
การย้ายสำนักงานครั้งนี้ไม่เพียงเสริมศักยภาพด้านการบริหารจัดการ แต่ยังยกระดับความพร้อมในการสนับสนุนภารกิจ ด้านความมั่นคงปลอดภัยไซเบอร์อย่างเต็มรูปแบบ

Relocation and Renovation of the NCSA Office to Government Complex Zone C

The NCSA successfully managed the relocation and renovation of its office to the Government Complex Zone C, with key achievements summarized as follows:

1. Efficient and transparent budget management for the fiscal year 2024.
2. Complete an inventory of materials, equipment, and assets to be moved, as well as items to be returned.
3. Conducted site surveys to monitor construction progress and plan subsequent operations.
4. Secured project approval and appointed a committee to oversee and support the relocation process.
5. Executed the project according to the timeline, including site inspections in January 2024 after obtaining access from The Dhanarak Asset Development Co., Ltd.

This relocation enhances administrative capabilities and strengthens the NCSA's readiness to fully support its mission in national cybersecurity.



กิจกรรมจัดทำแผนเผชิญเหตุด้านไซเบอร์ (National Cyber Incident Response Plan)

ในยุคดิจิทัลที่ภัยคุกคามไซเบอร์มีความซับซ้อนและหลากหลาย การเตรียมความพร้อมในการรับมือกับสถานการณ์ที่อาจเกิดขึ้นกลายเป็นสิ่งสำคัญอย่างยิ่ง

สภมช. ได้ริเริ่มกิจกรรมการจัดทำแผนเผชิญเหตุด้านไซเบอร์ (National Cyber Incident Response Plan) เพื่อเสริมสร้างศักยภาพและความพร้อมของหน่วยงานต่าง ๆ ในการรับมือกับความท้าทายของภัยคุกคามไซเบอร์ในทุกระดับ โดยได้ดำเนินการจัดอบรมเชิงปฏิบัติการในเดือนกุมภาพันธ์ 2567 เพื่อยกระดับความพร้อมของหน่วยงานต่าง ๆ ในการจัดทำแผนเผชิญเหตุด้านไซเบอร์

การอบรมครั้งนี้มุ่งเน้นให้ความรู้และเสริมศักยภาพแก่หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใน 5 กลุ่มภารกิจ ได้แก่ 1. ด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ 2. หน่วยงานของรัฐ 3. ด้านการศึกษา ด้านสาธารณสุข 4. ด้านพลังงานและสาธารณูปโภค ด้านขนส่งและโลจิสติกส์ 5. ด้านการเงินและการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม

การอบรมช่วยให้ผู้เข้าร่วม **1,986 คน** ได้เรียนรู้โครงสร้างและข้อกำหนดสำคัญในการจัดทำแผนรับมือภัยคุกคามไซเบอร์ สามารถนำไปปฏิบัติและตอบสนองต่อเหตุการณ์ไซเบอร์ระดับต่าง ๆ ได้อย่างมีประสิทธิภาพ นับเป็นอีกก้าวสำคัญในการสร้างความพร้อมรับมือภัยคุกคามในยุคดิจิทัล

National Cyber Incident Response Plan Development Initiative

In an era where cyber threats grow increasingly complex, preparedness for potential incidents is now essential. The NCSA launched the **National Cyber Incident Response Plan** initiative to enhance the capability and readiness of various organizations to address and respond to cyber threats effectively at all levels.

The NCSA conducted a hands-on workshop in February 2024 to strengthen the preparedness of various agencies in developing a comprehensive National Cyber Incident Response Plan. This training program focused on providing knowledge and enhancing the capabilities of government agencies, regulators, organizations of critical information infrastructure across five key mission areas: 1) National Security and Critical Government Service, 2) Government Agencies, 3) Education and Public Health, 4) Energy, Utilities, Transportation, and Logistics, 5) Finance, Banking, Information Technology, and Telecommunications.

With **1,986 participants**, the program empowered personnel's capacity to create actionable plans tailored to various cyber threat response plans. This marks a pivotal step in equipping organizations to address evolving cyber threats and safeguard national digital resilience proactively.



NATIONAL CYBER INCIDENT RESPONSE PLAN



กิจกรรมยกระดับการรักษาความมั่นคงปลอดภัย หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

การเสริมสร้างความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยเฉพาะหน่วยงานด้านสาธารณสุข ถือเป็นเรื่องสำคัญที่ต้องดำเนินการอย่างเร่งด่วน เพื่อป้องกันและลดผลกระทบจากเหตุการณ์ที่ไม่พึงประสงค์ รวมถึงการรักษาความเชื่อมั่นของประชาชนต่อระบบบริการสุขภาพของประเทศ

สมทช. ได้ยกระดับความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานด้านสาธารณสุข ภายใต้โครงการพัฒนาขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยโครงการนี้ได้ดำเนินการติดตั้งอุปกรณ์เฝ้าระวังภัยคุกคามไซเบอร์ให้กับโรงพยาบาล 10 แห่งทั่วประเทศ ได้แก่ sw.พระนั่งเกล้า (จ.นนทบุรี) sw.พุทธโสธร (จ.ฉะเชิงเทรา) sw.เจ้าพระยายมราช (จ.สุพรรณบุรี) sw.สวรรค์ประชารักษ์ (จ.นครสวรรค์) sw.บุรีรัมย์ (จ.บุรีรัมย์) sw.เชียงใหม่ประชานุเคราะห์ (จ.เชียงใหม่) sw.วชิระภูเก็ต (จ.ภูเก็ต) sw.อุดรดิตถ์ (จ.อุดรดิตถ์) sw.สกลนคร (จ.สกลนคร) sw.สรรพสิทธิ์ประสงค์ (จ.อุบลราชธานี) พร้อมทั้งจัดอบรมเจ้าหน้าที่ของ สมทช. และโรงพยาบาลให้สามารถใช้เครื่องมือและบริการในโครงการได้อย่างเต็มประสิทธิภาพ

กิจกรรมนี้มีเป้าหมายเพื่อเฝ้าระวังภัยตลอด 24/7 ตรวจสอบและแจ้งเตือนภัยคุกคามล่วงหน้า รวมถึงการวิเคราะห์และตอบสนองต่อเหตุการณ์ไม่คาดคิดได้อย่างรวดเร็ว ปัจจุบันมีโรงพยาบาลในโครงการที่ได้รับการดูแลด้านไซเบอร์แล้วรวม 26 แห่ง

Enhancing Cybersecurity for Organization of Critical Information Infrastructure

Enhancing cybersecurity for organization of critical information infrastructure, particularly in the public health sector, is necessary in the rapidly evolving digital era. This initiative aims to safeguard vital healthcare systems against cyber threats, ensuring public confidence in the nation's healthcare services.

The NCSA launched a program to bolster cybersecurity for healthcare institutions under the **Cybersecurity Capacity Building Project for Organization of Critical Information Infrastructure**. The initiative includes installing advanced cyber threat monitoring tools in **10 hospitals nationwide**. Training sessions were also organized for hospital staff to ensure optimal use of the project's tools and services.

The program is designed to deliver 24/7 threat monitoring, proactive alerts for high-risk incidents, and swift responses to unexpected events. **Currently, 26 hospitals nationwide benefit from cybersecurity monitoring under this initiative.**





กิจกรรมยกระดับขีดความสามารถการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Self-Assessment)

ในยุคที่ภัยคุกคามทางไซเบอร์มีความซับซ้อนและเพิ่มขึ้นอย่างรวดเร็ว การเตรียมพร้อมและยกระดับความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานทั้งภาครัฐและเอกชนจึงเป็นเรื่องสำคัญ สกมช. ได้ริเริ่มกิจกรรม Cybersecurity Self-Assessment เพื่อสนับสนุนหน่วยงานต่าง ๆ ในการประเมินและพัฒนาขีดความสามารถของตนเองด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กิจกรรมนี้มุ่งเป้าไปยังหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ **กว่า 100 หน่วยงาน โดยจัดให้มีการประเมินตนเองด้านความมั่นคงปลอดภัยไซเบอร์** เพื่อให้หน่วยงานเหล่านี้ทราบถึงสถานภาพและช่องโหว่ที่อาจเกิดขึ้นในระบบของตน นอกจากนี้ สกมช. **ยังให้คำปรึกษาในการจัดทำแผนปรับปรุงแก้ไขแก่ 30 หน่วยงาน** ซึ่งครอบคลุมทั้งกระบวนการและมาตรการเพื่อเพิ่มความปลอดภัยและลดความเสี่ยงจากภัยคุกคาม

Enhancing Cybersecurity Capabilities through Self-Assessment

In today's rapidly evolving digital landscape, the increasing complexity and frequency of cyber threats require strong organizational preparedness. The NCSA has launched the Cybersecurity Self-Assessment initiative, designed to empower government agencies and critical sectors to strengthen their cybersecurity defenses.

This activity targets **over 100 public sector agencies, regulators, and organizations of critical information infrastructure**. It involves conducting **cybersecurity self-assessments** to help these agencies identify their status and potential vulnerabilities within their systems. Additionally, the NCSA has **detailed consultations with 30 agencies**, assisting them in developing improvement plans. These plans encompass processes and measures to enhance cybersecurity and reduce risks from potential threats.



กลยุทธ์ที่ 4.2 : ส่งเสริมและสนับสนุนการแบ่งปันข้อมูลภัยคุกคาม

Strategy 4.2 : Promote and Support Cyber Threat Information Sharing

ในยุคที่ภัยคุกคามทางไซเบอร์ซับซ้อนขึ้นและส่งผลกระทบเป็นวงกว้าง การแบ่งปันข้อมูลข่าวกรองและองค์ความรู้ด้านภัยคุกคามถือเป็นหัวใจสำคัญของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อเสริมสร้างความแข็งแกร่งและพร้อมรับมือกับภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ

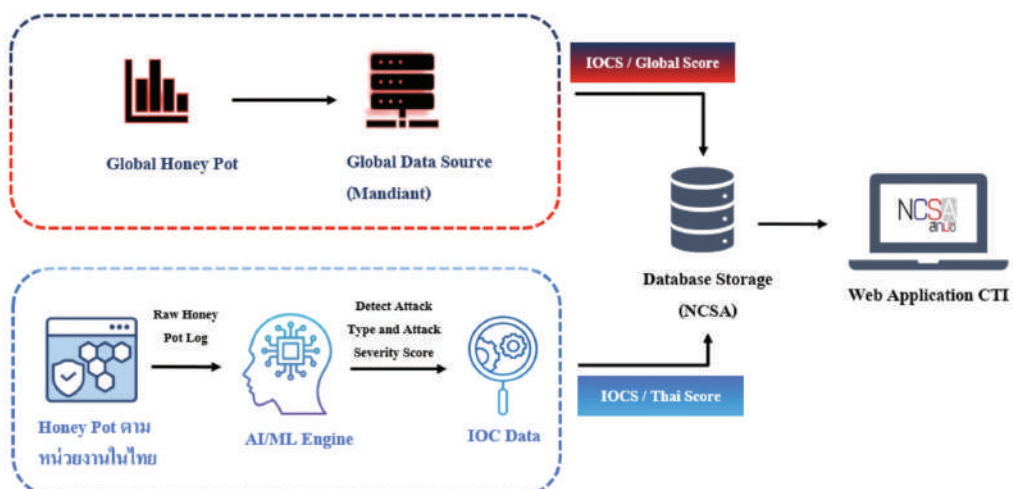
In an era of increasingly complex and pervasive cyber threats, the exchange of threat intelligence and knowledge is vital for building robust cybersecurity, bolstering resilience, and enhancing preparedness to counter cyber risks effectively.

กิจกรรมพัฒนาระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะ (CTI)

สภมช. มุ่งเน้นการสร้างเครือข่ายความร่วมมือระหว่างหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานภาครัฐ และภาคเอกชน ปัจจุบัน มีหน่วยงานเข้าร่วมใช้งานระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะ จำนวน **28 หน่วยงาน** ถือเป็นเครื่องมือสำคัญที่ช่วยเสริมสร้างความร่วมมือและการแบ่งปันข้อมูลภัยคุกคามระหว่างหน่วยงาน ทั้งยังช่วยยกระดับมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ของประเทศให้พร้อมรับมือกับความท้าทายที่เปลี่ยนแปลงไปในยุคดิจิทัล

Development of the Cyber Threat Intelligence Center

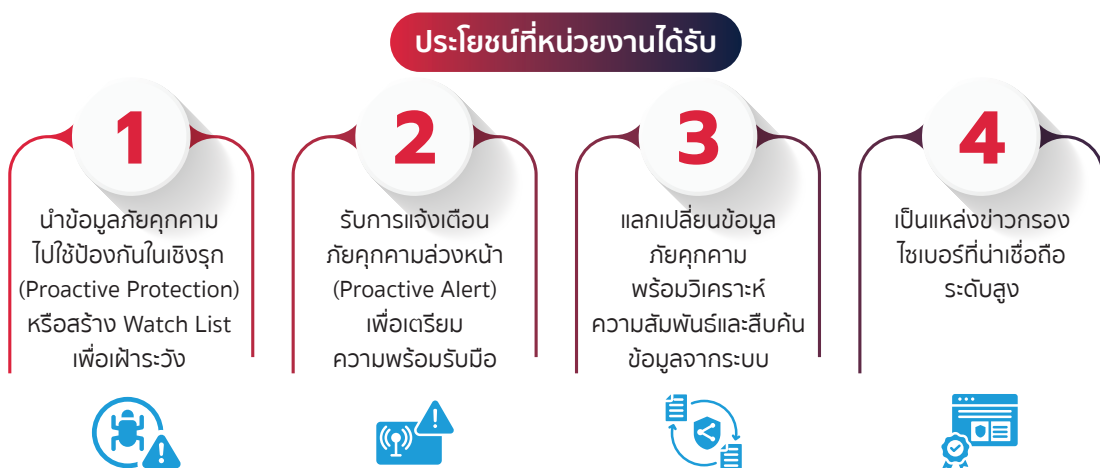
As cyber threats grow increasingly complex and unpredictable, information sharing is crucial for bolstering cybersecurity resilience. The NCSA established the Cyber Threat Intelligence Center to address this, fostering systematic and efficient collaboration among organizations in sharing threat intelligence. **Currently utilized by 28 organizations**, the system significantly enhances their ability to monitor threats, analyze data, and respond swiftly to cyber incidents.



กิจกรรมพัฒนาแพลตฟอร์มการรับและแบ่งปันเหตุการณ์ภัยคุกคามทางไซเบอร์ (Malware Information Sharing Platform - MISP)

สทท. ได้พัฒนาแพลตฟอร์ม MISP เพื่อเชื่อมโยงการรับและแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์แบบอัตโนมัติ โดยร่วมมือกับศูนย์ประสานงานความมั่นคงปลอดภัยไซเบอร์ภาคการธนาคาร หรือ TB-CERT และหน่วยงานนำร่องต่าง ๆ ที่ครอบคลุม 7 กลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure) ทั้งในประเทศ 30 หน่วยงาน และต่างประเทศ 2 หน่วยงาน (Brazil CERT และ Forum of Incident Response and Security Teams: FIRST) ทั้งนี้ สทท. ได้ดำเนินการแชร์ Indicator of compromise (IOC) ที่ได้วิเคราะห์จากทั้งสองหน่วยงาน และนำมาแชร์ในระบบ MISP โดยแบ่งเป็น Events: 235,672 และ Attributes: 54,568,710

ระบบนี้เน้นการแชร์ข้อมูลภัยคุกคามในเชิงรุก (Proactive Protection) เช่น ตัวบ่งชี้ภัยคุกคามและกลุ่ม Hacker ที่มีความเสี่ยงต่อประเทศไทย ด้วยแนวทางการพัฒนาแบบ Scalable รองรับการขยายตัวในอนาคต พร้อมใช้ Traffic Light Protocol เพื่อสร้างความน่าเชื่อถือในการแลกเปลี่ยนข้อมูล



ด้วยความร่วมมือจากหลายหน่วยงาน โครงการนี้ช่วยยกระดับการป้องกันภัยไซเบอร์ในประเทศไทยให้แข็งแกร่งขึ้น รองรับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และเตรียมพร้อมขยายความร่วมมือไปยังประเทศอื่น ๆ ในอนาคต โดยโครงการได้มีการแถลงความสำเร็จเมื่อวันที่ 19 กันยายน 2567 เพื่อแสดงถึงความพร้อมของประเทศไทยในการก้าวสู่มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสากล



Development of the Malware Information Sharing Platform (MISP)

The NCSA has developed the **MISP platform** to facilitate automated sharing and receiving of cyber threat intelligence. In collaboration with Thailand Banking Sector Computer Emergency Response Team (TB-CERT) and pilot agencies across seven critical information infrastructure (CII) sectors, this initiative **connects 30 domestic and 2 international organizations** (Brazil CERT and the Forum of Incident Response and Security Teams: FIRST). NCSA has shared Indicators of Compromise (IOC) analyzed from both organizations and uploaded them to the MISP system, categorized into 235,672 events and 54,568,710 attributes.

The platform focuses on proactive protection by sharing key indicators of compromise and potential hacker groups targeting Thailand. It is designed with scalability and incorporates the Traffic Light Protocol to ensure trusted and secure information exchange.

Benefits for Participating Organizations

1. Utilize threat intelligence for proactive protection or create watch lists for continuous monitoring.
2. Receive proactive alerts on emerging threats to prepare adequate responses.
3. Exchange threat data, analyze correlations, and retrieve relevant insights from the system.
4. Access a reliable and systematic national-level cyber intelligence repository.

This initiative marks a significant step in strengthening Thailand's cybersecurity resilience. It aligns with the Cybersecurity Act B.E. 2562 and provides a proactive mechanism to combat cyber threats, enhancing national security. **The project's success was officially announced on September 19, 2024, reflecting Thailand's readiness to meet global cybersecurity standards and expand its collaboration with other nations in the future.**



กลยุทธ์ที่ 4.3 : ส่งเสริมและสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์ Strategy 4.3 : Promoting and Supporting Cybersecurity

มุ่งสร้างความเชื่อมั่นให้กับทุกภาคส่วน ยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานที่ให้บริการที่สำคัญ และผลักดันการพัฒนาบริการด้านความมั่นคงปลอดภัยไซเบอร์ให้มีความพร้อมและประสิทธิภาพ เพื่อสร้างภูมิคุ้มกันที่เข้มแข็งต่อภัยคุกคามในยุคดิจิทัล

Building trust among all sectors, enhancing critical service providers' cybersecurity standards, and advancing cybersecurity services' development. This strategy aims to establish a robust framework to protect against emerging cyber threats in the digital era.

กิจกรรมยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐาน Global Cyber Index (GCI)

ภายใต้โครงการยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐาน Global Cyber Index (GCI) สกมช. ได้ดำเนินกิจกรรมสำคัญเพื่อสร้างรากฐานในการพัฒนาความมั่นคงปลอดภัยไซเบอร์ของประเทศ ได้แก่

1

การคุ้มครองเด็กในโลกออนไลน์: จัดกิจกรรมเมื่อวันที่ 2, 6 และ 15 สิงหาคม 2567 เพื่อหาหรือการปกป้องเด็กจากภัยออนไลน์ มุ่งเน้นการพัฒนามาตรฐานและแนวปฏิบัติสำหรับพื้นที่ปลอดภัยในโลกออนไลน์ พร้อมระดมสมองจากหน่วยงานต่าง ๆ เพื่อแก้ไขปัญหาการเข้าถึงสื่อที่ไม่เหมาะสม



2

การสนับสนุนอุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์: จัดประชุมรับฟังความคิดเห็นในวันที่ 4 กันยายน และ 25 ตุลาคม 2567 เพื่อกำหนดมาตรฐานและรับรองผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ในประเทศไทย พร้อมเสนอแผนร่วมมือกับองค์กรระดับสากล



3

การยกระดับ Sectoral CERT: จัดประชุมวันที่ 16 กันยายน และ 11 พฤศจิกายน 2567 เพื่อประเมินสถานะและพัฒนาศักยภาพ Sectoral CERT ในประเทศไทย โดยมุ่งเน้นให้เป็นสมาชิกหน่วยงานระหว่างประเทศ เช่น FIRST และ AP-CERT



Activities to Enhance Cybersecurity under the Global Cyber Index (GCI)

As part of the initiative to elevate cybersecurity under the Global Cyber Index (GCI), the NCSA has undertaken three key activities aimed at strengthening the nation's cybersecurity framework:

- 1. Online Child Protection:** Held on August 2, 6, and 15, 2024, these activities focused on safeguarding children from online threats. Discussions centered on developing standards and best practices for creating safe online spaces, with input from public and private sectors to address access to inappropriate content.
- 2. Cybersecurity Industry Development:** Public hearings were held on September 4 and October 25, 2024, to establish standards and certification criteria for cybersecurity service providers in Thailand. The meetings also explored collaborative plans with international organizations to enhance global competitiveness.
- 3. Enhancing Sectoral CERTs:** Meetings on September 16 and November 11, 2024, assessed the status and challenges of Sectoral CERTs in Thailand. Efforts were made to enable these CERTs to join international organizations such as FIRST and AP-CERT, strengthening cooperation and effectiveness in addressing global cyber threats.



Prime Minister Awards: Thailand Cybersecurity Excellence Awards 2024

กิจกรรมและพิธีมอบรางวัลอันทรงเกียรติ “Prime Minister Awards: Thailand Cybersecurity Excellence Awards 2024” เพื่อเชิดชูองค์กรที่มีผลงานโดดเด่นด้านความมั่นคงปลอดภัยไซเบอร์ โดยมีเป้าหมายเพื่อยกระดับมาตรฐานความปลอดภัยทางไซเบอร์ของประเทศไทย และเสริมสร้างบทบาทของประเทศไทยในฐานะศูนย์กลางความมั่นคงปลอดภัยไซเบอร์แห่งภูมิภาคอาเซียน โดยพิธีมอบรางวัล ได้รับเกียรติจาก **ดร.ณทภัย ทิวไพงาม** ผู้ช่วยรัฐมนตรีประจำสำนักนายกรัฐมนตรี เป็นประธานในพิธี ท่ามกลางตัวแทนจากหน่วยงานรัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) บริษัทเอกชน ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (CERT) และผู้ให้บริการระบบคลาวด์ (CSP) ที่เข้าร่วมอย่างคับคั่ง

ภายในงานได้มอบรางวัลให้กับองค์กรที่แสดงถึงความเป็นเลิศด้านไซเบอร์ใน 3 ประเภทสำคัญ ได้แก่

1. **Best Performance Award** สำหรับองค์กรที่มีผลงานโดดเด่นในการป้องกันและรับมือภัยคุกคามไซเบอร์
2. **Most Contribution Award** สำหรับองค์กรที่มีบทบาทสำคัญในการพัฒนาขีดความสามารถด้านไซเบอร์ของประเทศ
3. **Special Awards** สำหรับองค์กรที่สร้างการเปลี่ยนแปลงเชิงบวกในอุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์

ผู้ชนะรางวัลทุกประเภทได้รับการประเมินจากเกณฑ์ที่เข้มงวด ครอบคลุมทั้งด้านการบริหารความเสี่ยง การปฏิบัติตามมาตรฐานสากล เช่น ISO 27001 และ GDPR รวมถึงการพัฒนาศักยภาพบุคลากร เป็นต้น

The Prime Minister Awards: Thailand Cybersecurity Excellence Awards 2024 is a prestigious event recognizing organizations with outstanding achievements in cybersecurity. The awards aim to elevate Thailand's cybersecurity standards and strengthen the country's role as a cybersecurity hub in the ASEAN region.

The ceremony was honored by **Dr. Nahathai Thewphaingarm, Assistant Minister to the Prime Minister's Office**, who presided over the event. The awards brought together representatives from **government agencies, organizations of critical information infrastructure, private sector companies, computer emergency response teams (CERTs), and cloud service providers (CSPs)**. The awards were presented in three key categories:

1. **Best Performance Award** - Honoring the organizations that excel in cybersecurity threat prevention and incident response.
2. **Most Contribution Award** - Honoring the organizations that play a pivotal role in enhancing the nation's cybersecurity capabilities.
3. **Special Awards** - Honoring the organizations that drive positive transformations in the cybersecurity industry.

กิจกรรมทั้งหมดนี้ได้รับความสนใจจาก



และถือเป็นก้าวสำคัญในการยกระดับความมั่นคงปลอดภัยไซเบอร์ของประเทศให้สอดคล้องกับมาตรฐานระดับสากล

These activities, attended by **770 participants**, lay a vital foundation for elevating Thailand's cybersecurity to meet global standards.

กิจกรรมการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT)

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ หรือ ThaiCERT ตั้งขึ้นตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อทำหน้าที่เฝ้าระวังและตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ ในปีงบประมาณ 2567 ได้ดำเนินการช่วยเหลือและฟื้นฟูเหตุการณ์ด้านไซเบอร์ให้กับหน่วยงานที่ร้องขอ 38 แห่ง

Establishment of the National CERT

As the National CERT, ThaiCERT was established under the Cybersecurity Act B.E. 2562 (2019) to monitor, analyze, and respond effectively to cyber threats. In fiscal year 2024, ThaiCERT **provided incident response and recovery support to 38 organizations**, ensuring a secure cyber environment for key institutions across the country.



กิจกรรมการจัดตั้งห้องปฏิบัติการร่วมทางไซเบอร์ (NCSA War Room)

NCSA War Room ดำเนินการโดย ThaiCERT ทำหน้าที่เฝ้าระวัง แจ้งเตือน และสนับสนุนการแก้ไขเหตุการณ์คุกคามทางไซเบอร์ ตลอด 24 ชั่วโมง ในปีงบประมาณ 2567 ห้องปฏิบัติการนี้ดำเนินการให้บริการกับ **638 หน่วยงาน** พร้อมผลิตรายงานความมั่นคงปลอดภัย **1,827 ฉบับ** ช่วยยกระดับประสิทธิภาพการรับมือภัยคุกคามและสร้างความเชื่อมั่นให้กับทุกภาคส่วน



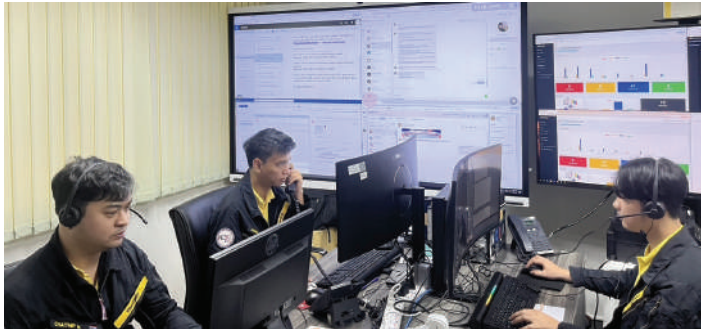
Establishment of the NCSA War Room

The NCSA War Room, operated by ThaiCERT, is responsible for monitoring, alerting, and supporting the resolution of cyber threats 24/7. During the fiscal year 2024, this operation served **638 agencies** and produced **1,827 cybersecurity reports**, significantly enhancing the effectiveness of threat response and fostering confidence across all sectors.



กิจกรรมระบบช่วยเหลือ (Help Desk) ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ Cybersecurity Help Desk Activities by ThaiCERT

ระบบช่วยเหลือด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Help Desk) ของ ThaiCERT ได้รับการพัฒนาเป็นศูนย์กลางการให้คำปรึกษาและรับแจ้งเหตุภัยคุกคามทางไซเบอร์จากหน่วยงานรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อรับมือภัยคุกคามได้อย่างมีประสิทธิภาพ



The Cyber Security Help Desk, operated by ThaiCERT is a central hub for consultation and incident reporting on cyber threats. It efficiently supports government agencies, regulators, organizations of critical information infrastructure, enhancing cyber incident response.

สรุปผลการดำเนินงาน Help Desk ปีงบประมาณ พ.ศ. 2567 Summary of Help Desk Operations for Fiscal Year 2024



รับแจ้งเหตุภัยคุกคามทางไซเบอร์
(Cyber incident reports received):
1,489 รายการ (cases)



ผ่านโทรศัพท์ (Via telephone):
1,304 รายการ (cases)



ผ่านอีเมล/แอปพลิเคชัน
(Via email/applications):
185 รายการ (cases)



เหตุการณ์ระดับ Critical (IOC)
(Critical-level incidents):
**2,224 เหตุการณ์
(incidents)**



เหตุการณ์ระดับ High (IOC)
(High-level incidents):
**1,177,676 เหตุการณ์
(incidents)**



ตรวจสอบเพจมิถิชาชีพ/ปลอม (Scanned and
reviewed fraudulent/fake pages):
1,066 เพจ (pages)



ประสานงานโครงการ Meta Verified
(Coordinated Meta Verified
project): **9,320 หน่วยงาน
(organizations)**



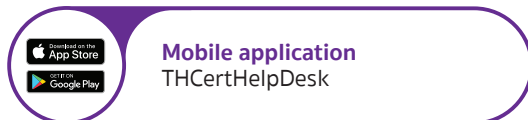
ประสานแก้ไขเพจ Facebook ที่ถูกโจมตี
Coordinated fixes for hacked
Facebook pages: **57 เพจ (pages)**



ประสานงานโครงการป้องกัน
Ransomware (Coordinated
Ransomware Protection project):
**3,876 หน่วยงาน
(organizations)**



ตรวจสอบภัยคุกคาม (Threat monitoring):
15 โรงพยาบาล (hospitals)



สแกนเลย!



LINE: @thaicert



App: THCertHelpDesk

กิจกรรมติดตามและประเมินผลนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์

สทศ. ดำเนินกิจกรรมติดตามและประเมินผลการดำเนินงานตามนโยบายและแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ ประจำปีงบประมาณ 2567 เพื่อผลักดันการดำเนินงานให้เป็นไปตามเป้าหมายที่กำหนด โดยมีการจัดกิจกรรมติดตามและประเมินผลทั้งในกรุงเทพฯ ปริมณฑล และภูมิภาค จำนวน **4 ครั้ง**



ครอบคลุม 98 หน่วยงาน ได้แก่



หน่วยงานควบคุม
หรือกำกับดูแล (Regulator)
19 หน่วยงาน



หน่วยงานโครงสร้างพื้นฐาน
สำคัญทางสารสนเทศ (CII)
61 หน่วยงาน



หน่วยงานของรัฐ
18 หน่วยงาน

มีผู้เข้าร่วมกิจกรรมทั้งหมด 594 คน

(Onsite 335 คน และ Online 259 คน) นอกจากนี้ ยังมีการจัดทำกรอบนโยบายและแผนปฏิบัติการฯ ฉบับใหม่ (พ.ศ. 2571-2575) ซึ่งปัจจุบันดำเนินการสำเร็จแล้ว 70%

นับเป็นอีกก้าวสำคัญในการสร้างมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของประเทศให้แข็งแกร่งยิ่งขึ้น

Monitoring and Evaluating Cybersecurity Policy Implementation

The NCSA conducted monitoring and evaluation activities under the Cybersecurity Policy and Plan for Fiscal Year 2024, ensuring the effective execution of its goals.

The activities included four sessions in Bangkok, its surrounding provinces, and regional areas, engaging **98 target organizations** comprising 19 regulators, 61 organizations of critical information infrastructure, and 18 government agencies.

A total of **594 participants** joined (335 onsite and 259 online). Additionally, progress was made on drafting the new Cybersecurity Policy and Action Plan (2028–2032), with 70% of the work completed.

These initiatives mark a significant step toward strengthening the country's cybersecurity standards and preparedness for emerging threats.

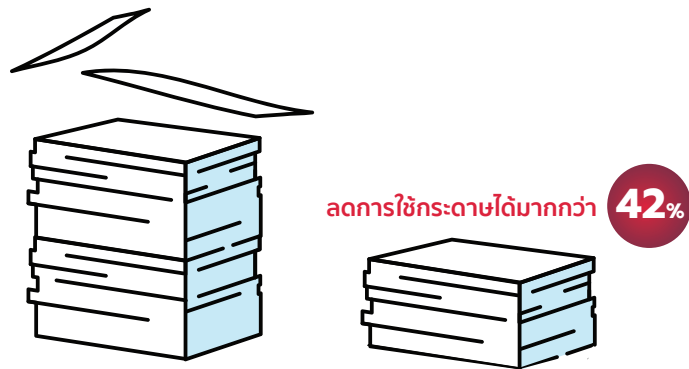


ผลงานอื่น ๆ

Other Key Achievements

การนำระบบดิจิทัลมาใช้เพื่อลดการใช้กระดาษ

สกมช. ได้นำระบบเอกสารอิเล็กทรอนิกส์มาใช้แทนการจัดเก็บเอกสารในรูปแบบกระดาษ ช่วยเพิ่มประสิทธิภาพในการจัดการข้อมูล การค้นหา การแชร์ และการเข้าถึงเอกสาร นอกจากนี้ยังลดความซับซ้อนของการอนุมัติเอกสาร การส่งแบบฟอร์ม และการบันทึกข้อมูลออนไลน์ ส่งผลให้การดำเนินงานรวดเร็ว โปร่งใส และถูกต้องยิ่งขึ้น การเปลี่ยนแปลงนี้ช่วยลดการใช้ทรัพยากรธรรมชาติ ลดการปล่อยก๊าซคาร์บอนไดออกไซด์ และลดปริมาณขยะที่ต้องกำจัด ทั้งยังช่วยประหยัดพื้นที่จัดเก็บและต้นทุนในระยะยาว โดย**สามารถลดการใช้กระดาษได้มากกว่า 42%** ซึ่งเป็นการสนับสนุนการพัฒนาอย่างยั่งยืนขององค์กร



Digital Transformation for Paperless Operations

The NCSA has adopted an e-document system to replace traditional paper-based document storage. Enhance efficiency in managing, searching, sharing, and accessing documents. Additionally, simplify processes such as document approval, form submission, and online data recording, resulting in faster, more transparent, and more accurate operations. Additionally, the shift reduces natural resource consumption, lowers carbon emissions, and minimizes waste, contributing to environmental sustainability. It also decreases storage space requirements and long-term operational costs. The NCSA has successfully **reduced paper usage by over 42%**, demonstrating its commitment to sustainable development.

การดำเนินงานตามแผนการจัดซื้อจัดจ้าง ประจำปีงบประมาณ 2567

สกมช. สามารถดำเนินการผูกพันสัญญาได้ถึง 29 สัญญา จากจำนวนโครงการทั้งหมด 31 โครงการ โดยดำเนินการในรูปแบบต่าง ๆ รวมถึงวิธีเฉพาะเจาะจง จำนวน 108 ใบสั่งซื้อ/สั่งจ้าง การดำเนินงานนี้สะท้อนถึงความสามารถในการบริหารจัดการแผนการจัดซื้อจัดจ้างที่มีประสิทธิภาพ ช่วยให้องค์กรสามารถดำเนินการตามเป้าหมายได้อย่างมีประสิทธิภาพและตรงเวลา

Procurement Plan Execution for Fiscal Year 2024

The NCSA successfully **executed 29 contracts out of 31 planned projects** for the fiscal year 2024, including 108 purchase orders/contracts through a specific procurement method. This achievement underscores the organization's efficient management of procurement plans, ensuring that objectives are met effectively and within the designated timeframe.

การเสริมสร้างความรู้เกี่ยวกับ RoPA และ DPA

สทท. มุ่งเน้นเสริมสร้างความรู้ด้านการคุ้มครองข้อมูลส่วนบุคคลให้แก่บุคลากรในองค์กร โดยเมื่อวันที่ 25 กรกฎาคม 2567 ได้จัดอบรมเชิงปฏิบัติการเกี่ยวกับการจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA) และข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA) การฝึกอบรมประกอบด้วยการจำลองสถานการณ์เพื่อบันทึกข้อมูลใน RoPA เพื่อให้ผู้เข้าร่วมมีความเข้าใจและสามารถนำไปปรับใช้ในการปฏิบัติงานได้อย่างเหมาะสม สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

Capacity Building in Personal Data Protection: RoPA and DPA Training

The NCSA emphasizes building awareness of personal data protection among its staff. On July 25, 2024, it conducted a hands-on training workshop on creating **Records of Processing Activities (RoPA) and Data Processing Agreements (DPA)**. The workshop included simulated scenarios for recording data in RoPA, ensuring participants gained practical understanding and the ability to apply these skills effectively. This initiative aligns with the Personal Data Protection Act, B.E. 2562 (2019), enhancing the organization's compliance and operational efficiency.



การตรวจสอบภายใน

สทท. ได้พัฒนาการดำเนินงานด้านการตรวจสอบภายในให้มีประสิทธิภาพและได้มาตรฐานตลอดปีงบประมาณ 2567 โดยมีการจัดทำแผนงานประจำปี การมอบหมายงานบุคคล และพัฒนาศักยภาพบุคลากรให้ทันสมัย พร้อมจัดทำ **กฎบัตรคณะกรรมการตรวจสอบ พ.ศ. 2567** และ **กฎบัตรหน่วยงานตรวจสอบภายใน พ.ศ. 2567** เพื่อกำหนดบทบาทหน้าที่ และแนวทางการกำกับดูแลที่ชัดเจน ส่งเสริมธรรมาภิบาล ระบบควบคุมภายใน และการบริหารความเสี่ยง รวมถึงความโปร่งใส ในการจัดทำรายงานทางการเงินและการปฏิบัติตามกฎหมายที่เกี่ยวข้อง

Internal Audit Activities

The NCSA has advanced its internal audit operations for fiscal year 2024 to ensure efficiency, quality, and adherence to standards. This includes **annual operational planning**, individual work assignments, and personnel development to meet evolving requirements. Significant accomplishments include issuing the **Audit Committee Charter 2024** and the **Internal Audit Charter 2024**, which clarify objectives, responsibilities, and governance frameworks.



กฎบัตรหน่วยงานตรวจสอบภายใน 2567 &
และกฎบัตรคณะกรรมการตรวจสอบ 2567
The 2024 Internal Audit Charter &
The 2024 Audit Committee Charter



การบริหารความเสี่ยงและควบคุมภายใน

สทท. ได้ดำเนินการเสริมสร้างความมั่นคงในการบริหารความเสี่ยงและควบคุมภายในตามพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. 2561 โดยออก **นโยบายบริหารความเสี่ยง** และ **นโยบายควบคุมภายใน** เมื่อวันที่ 9 กรกฎาคม 2567 เพื่อแสดงถึงความมุ่งมั่นของผู้บริหารและบุคลากรทุกระดับ อีกทั้งได้จัด **ประชุมเชิงปฏิบัติการการบริหารความเสี่ยงทั่วทั้งองค์กร (ERM)** เมื่อวันที่ 14 พฤษภาคม 2567 เพื่อสร้างความเข้าใจและความร่วมมือในกระบวนการบริหารความเสี่ยงตามมาตรฐานสากล และจัดทำ **คู่มือการจัดทำแผนบริหารความเสี่ยง** เพื่อกำหนดแนวทางและองค์ประกอบสำคัญสำหรับการจัดทำแผนความเสี่ยงขององค์กรให้เป็นมาตรฐานเดียวกัน

Risk Management and Internal Controls

The NCSA has taken proactive steps to strengthen risk management and internal control systems in compliance with the State Financial and Fiscal Discipline Act B.E. 2561. Key actions include the **Risk Management and Internal Control policies**, issued on July 9, 2024, to demonstrate organizational commitment at all levels. A **Risk Management Workshop** was held on May 14, 2024; NCSA executives and staff collaborated to align risk management strategies with organizational missions. Additionally, the agency developed a **Risk Management Handbook** to standardize risk planning, outlining necessary laws, principles, and practices. These initiatives aim to embed a culture of risk awareness and shared responsibility across the agency.

ประกาศ สทท. เรื่องนโยบายบริหารความเสี่ยง



ประกาศ ณ วันที่ 9 กรกฎาคม พ.ศ. 2567

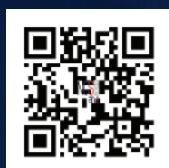




รายงานทางการเงิน

FINANCIAL REPORT

ดาวนี่โกลด์ รายงานทางการเงิน สกมช. 2567



รายงานของผู้สอบบัญชีรับอนุญาต
และรายงานการเงิน



รายงานการประเมินผล
การใช้จ่ายเงินและทรัพย์สิน



รายงานการสอบทาน
ระบบการควบคุมภายใน

ข้อมูลสำคัญทางการเงิน ปี 2567

รายงานของผู้สอบบัญชีรับอนุญาต

เสนอ คณะกรรมการ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ความเห็น

ข้าพเจ้าได้ตรวจสอบรายงานการเงินของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (หน่วยงาน) ซึ่งประกอบด้วยงบแสดงฐานะการเงิน ณ วันที่ 30 กันยายน 2567 งบแสดงผลการดำเนินงานทางการเงิน และงบแสดงการเปลี่ยนแปลงสินทรัพย์สุทธิ/ส่วนทุนสำหรับปีสิ้นสุดวันเดียวกันและหมายเหตุประกอบงบการเงิน รวมถึงสรุปนโยบายการบัญชีที่สำคัญ

ข้าพเจ้าเห็นว่า รายงานการเงินข้างต้นนี้แสดงฐานะการเงินของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ณ วันที่ 30 กันยายน 2567 และผลการดำเนินงาน สำหรับปีสิ้นสุดวันเดียวกันโดยถูกต้องตามที่ควรในสาระสำคัญตามมาตรฐานการบัญชีภาครัฐและนโยบายการบัญชีภาครัฐที่กระทรวงการคลังกำหนด

เกณฑ์ในการแสดงความเห็น

ข้าพเจ้าได้ปฏิบัติตามตรวจสอบตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินและมาตรฐานการสอบบัญชี ความรับผิดชอบของข้าพเจ้าได้กล่าวไว้ในวรรคความรับผิดชอบของผู้สอบบัญชีต่อการตรวจสอบรายงานการเงินในรายงานของข้าพเจ้า ข้าพเจ้ามีความเป็นอิสระจากหน่วยงานตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินที่กำหนดโดยคณะกรรมการตรวจเงินแผ่นดิน และประมวลจรรยาบรรณของผู้ประกอบวิชาชีพบัญชี รวมถึงมาตรฐานเรื่องความเป็นอิสระที่กำหนดโดยสภาวิชาชีพบัญชี (ประมวลจรรยาบรรณของผู้ประกอบวิชาชีพบัญชี) ในส่วนที่เกี่ยวข้องกับการตรวจสอบรายงานการเงิน และข้าพเจ้าได้ปฏิบัติตามความรับผิดชอบด้านจรรยาบรรณอื่น ๆ ซึ่งเป็นไปตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินและประมวลจรรยาบรรณของผู้ประกอบวิชาชีพบัญชี ข้าพเจ้าเชื่อว่าหลักฐานการสอบบัญชีที่ข้าพเจ้าได้รับเพียงพอและเหมาะสมเพื่อใช้เป็นเกณฑ์ในการแสดงความเห็นของข้าพเจ้า

เรื่องอื่น

รายงานการเงินของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติสำหรับปีสิ้นสุดวันที่ 30 กันยายน 2566 ที่แสดงเปรียบเทียบตรวจสอบโดยผู้สอบบัญชีอื่น ซึ่งแสดงความเห็นอย่างไม่มีเงื่อนไขตามรายงานลงวันที่ 21 ธันวาคม 2566

ข้อมูลอื่น

ผู้บริหารเป็นผู้รับผิดชอบต่อข้อมูลอื่น ข้อมูลอื่นประกอบด้วยข้อมูลซึ่งรวมอยู่ในรายงานประจำปีไม่รวมถึงรายงานการเงินและรายงานของผู้สอบบัญชีที่อยู่ในรายงานนั้น ซึ่งคาดว่ารายงานประจำปีจะถูกจัดเตรียมให้ข้าพเจ้าภายหลังวันที่ในรายงานของผู้สอบบัญชีนี้

ความเห็นของข้าพเจ้าต่อรายงานการเงินไม่ครอบคลุมถึงข้อมูลอื่นและข้าพเจ้าไม่ได้ให้ความเชื่อมั่นต่อข้อมูลอื่น

ความรับผิดชอบของข้าพเจ้าที่เกี่ยวข้องกับการตรวจสอบรายงานการเงินคือ การอ่านและพิจารณาว่าข้อมูลอื่นมีความขัดแย้งที่มีสาระสำคัญกับรายงานการเงินหรือกับความรู้ที่ได้รับจากการตรวจสอบของข้าพเจ้า หรือปรากฏว่าข้อมูลอื่นมีการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญหรือไม่

เมื่อข้าพเจ้าได้อ่านรายงานประจำปี หากข้าพเจ้าสรุปได้ว่าการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญ ข้าพเจ้าต้องสื่อสารเรื่องดังกล่าวกับผู้มีหน้าที่ในการกำกับดูแล เพื่อให้ผู้มีหน้าที่ในการกำกับดูแลดำเนินการแก้ไขข้อมูลที่แสดงขัดต่อข้อเท็จจริง

ความรับผิดชอบของผู้บริหารและผู้มีหน้าที่ในการกำกับดูแลต่อรายงานการเงิน

ผู้บริหารมีหน้าที่รับผิดชอบในการจัดทำและนำเสนอรายงานการเงินเหล่านี้โดยถูกต้องตามที่ควรตามมาตรฐานการบัญชีภาครัฐและนโยบายการบัญชีภาครัฐที่กระทรวงการคลังกำหนด และรับผิดชอบเกี่ยวกับการควบคุมภายในที่ผู้บริหารพิจารณาว่าจำเป็นเพื่อให้สามารถจัดทำรายงานการเงินที่ปราศจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญไม่ว่าจะเกิดจากการทุจริตหรือข้อผิดพลาด

ในการจัดทำรายงานการเงิน ผู้บริหารรับผิดชอบในการประเมินความสามารถของหน่วยงานในการดำเนินงานต่อเนื่อง เปิดเผยเรื่อง ที่เกี่ยวกับการดำเนินงานต่อเนื่องตามความเหมาะสม และการใช้เกณฑ์การบัญชีสำหรับการดำเนินงานต่อเนื่อง เว้นแต่มีข้อกำหนดในกฎหมาย หรือเป็นนโยบายรัฐบาลที่จะเลิกหน่วยงาน หรือหยุดดำเนินงานหรือไม่สามารถดำเนินงานต่อเนื่องต่อไปได้

ผู้มีหน้าที่ในการกำกับดูแลมีหน้าที่ในการกำกับดูแลกระบวนการในการจัดทำรายงานทางการเงินของหน่วยงาน

ความรับผิดชอบของผู้สอบบัญชีต่อการตรวจสอบรายงานการเงิน

การตรวจสอบของข้าพเจ้ามีวัตถุประสงค์เพื่อให้ได้ความเชื่อมั่นอย่างสมเหตุสมผลว่ารายงานการเงินโดยรวมปราศจากการแสดงข้อมูลที่ ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญหรือไม่ ไม่ว่าจะเป็นจากการทุจริตหรือข้อผิดพลาด และเสนอรายงานของผู้สอบบัญชีซึ่งรวม ความเห็นของข้าพเจ้าอยู่ด้วย ความเชื่อมั่นอย่างสมเหตุสมผลคือความเชื่อมั่นในระดับสูงแต่ไม่ได้เป็นการรับประกันว่าการปฏิบัติงาน ตรวจสอบตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินและมาตรฐานการสอบบัญชีจะสามารถตรวจพบข้อมูลที่ขัดต่อข้อเท็จจริง อันเป็นสาระสำคัญที่มีอยู่ได้เสมอไป ข้อมูลที่ขัดต่อข้อเท็จจริงอาจเกิดจากการทุจริตหรือข้อผิดพลาดและถือว่ามีสาระสำคัญเมื่อการดำเนินการ อย่างสมเหตุสมผลว่ารายการที่ขัดต่อข้อเท็จจริงแต่ละรายการหรือทุกรายการรวมกันจะมีผลต่อการตัดสินใจทางเศรษฐกิจของผู้ใช้ รายงานการเงินจากการใช้รายงานการเงินเหล่านี้

ในการตรวจสอบของข้าพเจ้าตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินและมาตรฐานการสอบบัญชี ข้าพเจ้าได้ใช้ดุลยพินิจ และการสังเกตและสงสัยซึ่งผู้ประกอบวิชาชีพตลอดการตรวจสอบ การปฏิบัติงานของข้าพเจ้ารวมถึง

- ระบุและประเมินความเสี่ยงจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญในรายงานการเงิน ไม่ว่าจะเป็นจากการทุจริตหรือ ข้อผิดพลาด ออกแบบและปฏิบัติตามวิธีการตรวจสอบเพื่อตอบสนองต่อความเสี่ยงเหล่านั้น และได้หลักฐานการสอบบัญชี ที่เพียงพอและเหมาะสมเพื่อเป็นเกณฑ์ในการแสดงความเห็นของข้าพเจ้า ความเสี่ยงที่ไม่พบข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระ สำคัญซึ่งเป็นผลมาจากการทุจริตจะสูงกว่าความเสี่ยงที่เกิดจากข้อผิดพลาด เนื่องจากการทุจริตอาจเกี่ยวกับการสมรู้ร่วมคิด การปลอมแปลงเอกสารหลักฐาน การตั้งใจละเว้นการแสดงผลข้อมูล การแสดงผลข้อมูลที่ไม่ตรงตามข้อเท็จจริงหรือการแทรกแซง การควบคุมภายใน
- ทำความเข้าใจในระบบการควบคุมภายในที่เกี่ยวข้องกับการตรวจสอบ เพื่อออกแบบวิธีการตรวจสอบที่เหมาะสมกับสถานการณ์ แต่ไม่ใช่เพื่อวัตถุประสงค์ในการแสดงความเห็นต่อความมีประสิทธิภาพของการควบคุมภายในของหน่วยงาน
- ประเมินความเหมาะสมของนโยบายการบัญชีที่ผู้บริหารใช้และความสมเหตุสมผลของประมาณการทางบัญชีและการเปิดเผยข้อมูล ที่เกี่ยวข้องซึ่งจัดทำขึ้นโดยผู้บริหาร
- สรุปร่วมกับความเหมาะสมของการใช้เกณฑ์การบัญชีสำหรับการดำเนินงานต่อเนื่องของผู้บริหารและจากหลักฐานการสอบบัญชี ที่ได้รับ สรุปว่ามีความไม่แน่นอนที่มีสาระสำคัญเกี่ยวกับเหตุการณ์ หรือสถานการณ์ที่อาจเป็นเหตุให้เกิดข้อสงสัยอย่างมีนัยสำคัญ ต่อความสามารถของหน่วยงานในการดำเนินงานต่อเนื่องหรือไม่ ถ้าข้าพเจ้าได้ข้อสรุปว่ามีความไม่แน่นอนที่มีสาระสำคัญ ข้าพเจ้า ต้องกล่าวไว้ในรายงานของผู้สอบบัญชีของข้าพเจ้าโดยให้ข้อสังเกตถึงการเปิดเผยข้อมูลในรายงานการเงินที่เกี่ยวข้อง หรือ ถ้าการเปิดเผยข้อมูลดังกล่าวไม่เพียงพอ ความเห็นของข้าพเจ้าจะเปลี่ยนแปลงไป ข้อสรุปของข้าพเจ้าขึ้นอยู่กับหลักฐานการสอบ บัญชีที่ได้รับจนถึงวันที่ในรายงานของผู้สอบบัญชีของข้าพเจ้า อย่างไรก็ตาม เหตุการณ์หรือสถานการณ์ในอนาคตอาจเป็นเหตุ ให้หน่วยงานต้องหยุดการดำเนินงานต่อเนื่อง
- ประเมินการนำเสนอโครงสร้างและเนื้อหาของรายงานการเงินโดยรวม รวมถึงการเปิดเผยข้อมูลว่ารายงานการเงินแสดงรายการ และเหตุการณ์ในรูปแบบที่ทำให้มีการนำเสนอข้อมูลโดยถูกต้องตามที่ควรหรือไม่

ข้าพเจ้าได้สื่อสารกับผู้มีหน้าที่ในการกำกับดูแลในเรื่องต่าง ๆ ที่สำคัญ ซึ่งรวมถึงขอบเขตและช่วงเวลาของการตรวจสอบ ตามที่ได้อ้างแผนไว้ ประเด็นที่มีนัยสำคัญที่พบจากการตรวจสอบรวมถึงข้อบกพร่องที่มีนัยสำคัญในระบบการควบคุมภายในหากข้าพเจ้า ได้พบในระหว่างการตรวจสอบของข้าพเจ้า

ผู้สอบบัญชีที่รับผิดชอบงานสอบบัญชีและนำเสนอรายงานฉบับนี้คือ นายสุวัฒน์ มณีกนกสกุล



(นายสุวัฒน์ มณีกนกสกุล)

ผู้สอบบัญชีรับอนุญาต ทะเบียนเลขที่ 8134

บริษัท สอบบัญชีธรรมนิติ จำกัด

กรุงเทพมหานคร

วันที่ 9 ธันวาคม 2567

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
งบแสดงฐานะการเงิน ณ วันที่ 30 กันยายน 2567

	หมายเหตุ	หน่วย:บาท	
		2567	2566
สินทรัพย์			
สินทรัพย์หมุนเวียน			
เงินสดและรายการเทียบเท่าเงินสด	4	352,397,458.80	182,511,805.46
ลูกหนี้อื่นระยะสั้น	5	18,296,555.87	313,863.68
วัสดุคงเหลือ	6	1,192,435.73	1,171,904.62
รวมสินทรัพย์หมุนเวียน		371,886,450.40	183,997,573.76
สินทรัพย์ไม่หมุนเวียน			
ที่ดิน อาคารและอุปกรณ์ - สุทธิ	7	130,730,634.34	163,257,094.21
สินทรัพย์ไม่มีตัวตน - สุทธิ	8	129,802,427.80	8,268,418.10
รวมสินทรัพย์ไม่หมุนเวียน		260,533,062.14	171,525,512.31
รวมสินทรัพย์		632,419,512.54	355,523,086.07
หนี้สินและสินทรัพย์สุทธิ/ส่วนทุน			
หนี้สิน			
หนี้สินหมุนเวียน			
เจ้าหนี้เงินโอนและรายการอุดหนุนระยะสั้น	9	113,172,874.00	47,795,343.50
เจ้าหนี้อื่นระยะสั้น	10	32,218,764.79	36,002,674.56
เงินรับฝากระยะสั้น	11	7,793,258.63	6,059,923.90
รวมหนี้สินหมุนเวียน		153,184,897.42	89,857,941.96
รวมหนี้สิน		153,184,897.42	89,857,941.96
สินทรัพย์สุทธิ/ส่วนทุน			
ทุน			
รายได้สูงกว่าค่าใช้จ่ายสะสม	13	479,234,615.12	265,665,144.11
รวมสินทรัพย์สุทธิ/ส่วนทุน		479,234,615.12	265,665,144.11
รวมหนี้สินและสินทรัพย์สุทธิ/ส่วนทุน		632,419,512.54	355,523,086.07

ขอรับรองว่าเป็นรายการอันถูกต้องและเป็นจริง


 (นายปรเมศวร์ กุมารบุญ)
 ผู้อำนวยการฝ่ายงบประมาณและกลยุทธ์องค์กร
 รักษาการในตำแหน่ง
 ผู้อำนวยการสำนักงานการเงินและกลยุทธ์องค์กร

พลอากาศตรี 
 (อมร ชมเชย)
 เลขาธิการคณะกรรมการ
 การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หมายเหตุประกอบงบการเงินเป็นส่วนหนึ่งของรายงานการเงินนี้

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
งบแสดงผลการดำเนินงานทางการเงิน สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2567

	หมายเหตุ	หน่วย:บาท	
		2567	2566
รายได้			
รายได้จากงบประมาณ	14	497,067,800.00	318,796,793.00
รายได้จากการอุดหนุนจากหน่วยงานภาครัฐ	15	111,218,486.00	114,148,324.00
รายได้จากการอุดหนุนอื่นและบริจาค		-	599,094.53
รวมรายได้		608,286,286.00	433,544,211.53
ค่าใช้จ่าย			
ค่าใช้จ่ายบุคลากร	16	68,062,811.92	47,725,498.67
ค่าตอบแทน	17	1,599,800.00	301,522.58
ค่าใช้สอย	18	238,453,523.28	211,274,177.58
ค่าวัสดุ	19	9,459,317.81	4,322,711.04
ค่าสาธารณูปโภค	20	736,289.25	787,639.24
ค่าเสื่อมราคาและค่าตัดจำหน่าย	21	96,515,925.57	19,036,765.02
รวมค่าใช้จ่าย		414,827,667.83	283,448,314.13
รายได้สูงกว่าค่าใช้จ่ายสุทธิ		193,458,618.17	150,095,897.40

ขอรับรองว่าเป็นรายการอันถูกต้องและเป็นจริง



(นายปรเมศวร์ กุมารบุญ)

ผู้อำนวยการฝ่ายงบประมาณและกลยุทธ์องค์กร

รักษาการในตำแหน่ง

ผู้อำนวยการสำนักการเงินและกลยุทธ์องค์กร

พลอากาศตรี



(อมร ชมเชย)

เลขาธิการคณะกรรมการ

การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หมายเหตุประกอบงบการเงินเป็นส่วนหนึ่งของรายงานการเงินนี้

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
งบแสดงการเปลี่ยนแปลงสินทรัพย์สุทธิ/ส่วนทุน สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2567

หมายเหตุ	ทุน	หน่วย:บาท	
		รายได้สูงกว่า	รวมสินทรัพย์สุทธิ
		ค่าใช้จ่ายสะสม	ส่วนทุน
ยอดคงเหลือ ณ วันที่ 30 กันยายน 2565 - ตามที่รายงานไว้เดิม	-	114,589,915.77	114,589,915.77
ผลสะสมจากการแก้ไขข้อผิดพลาดปีก่อน	13	979,330.94	979,330.94
ยอดคงเหลือ ณ วันที่ 30 กันยายน 2565 - หลังการปรับปรุง	-	115,569,246.71	115,569,246.71
การเปลี่ยนแปลงสินทรัพย์สุทธิ/ส่วนทุน สำหรับปี 2566			
รายได้สูงกว่าค่าใช้จ่ายสำหรับปี	-	150,095,897.40	150,095,897.40
ยอดคงเหลือ ณ วันที่ 30 กันยายน 2566	-	265,665,144.11	265,665,144.11

หมายเหตุ	ทุน	หน่วย:บาท	
		รายได้สูงกว่า	รวมสินทรัพย์สุทธิ
		ค่าใช้จ่ายสะสม	ส่วนทุน
ยอดคงเหลือ ณ วันที่ 1 ตุลาคม 2566 - ตามที่รายงานไว้เดิม	-	265,665,144.11	265,665,144.11
ผลสะสมจากการแก้ไขข้อผิดพลาดปีก่อน	13	20,110,852.84	20,110,852.84
ยอดคงเหลือ ณ วันที่ 1 ตุลาคม 2566 - หลังการปรับปรุง	-	285,775,996.95	285,775,996.95
การเปลี่ยนแปลงสินทรัพย์สุทธิ/ส่วนทุน สำหรับปี 2567			
รายได้สูงกว่าค่าใช้จ่ายสำหรับปี	-	193,458,618.17	193,458,618.17
ยอดคงเหลือ ณ วันที่ 30 กันยายน 2567	-	479,234,615.12	479,234,615.12

ขอรับรองว่าเป็นรายการอันถูกต้องและเป็นจริง


 (นายปรเมศวร์ กุมารบุญ)
 ผู้อำนวยการฝ่ายงบประมาณและกลยุทธ์องค์กร
 รักษาการในตำแหน่ง
 ผู้อำนวยการสำนักการเงินและกลยุทธ์องค์กร

พลอากาศตรี 
 (อมร ชมเชย)
 เลขาธิการคณะกรรมการ
 การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หมายเหตุประกอบงบการเงินเป็นส่วนหนึ่งของรายงานการเงินนี้



การประเมินผล การดำเนินงาน

PERFORMANCE EVALUATION

การประเมินผลการดำเนินงาน

PERFORMANCE EVALUATION

ผลการประเมินองค์การมหาชน ประจำปีงบประมาณ พ.ศ. 2567
โดยบุคคลภายนอก (บริษัท วินทูเกเตอร์ จำกัด)
The Evaluation of the Public Organization for the Fiscal Year 2024
by an External Entity (Win Together Co.,Ltd.)

องค์ประกอบที่ 1

การประเมินประสิทธิภาพ
ประสิทธิผลของการดำเนินงาน
(Performance Perspective)

ร้อยละ **70**

ตัวชี้วัด

ได้ร้อยละ

1.1 ร้อยละหน่วยงานที่ ThaiCERT สนับสนุน
ปฏิบัติการทางไซเบอร์ได้ตามกำหนดเวลา (ร้อยละ 20) **20**

1.2 ร้อยละเฉลี่ยถ่วงน้ำหนักของการให้บริการ
รับเรื่องแจ้งเหตุภัยคุกคามทางไซเบอร์ของ
ระบบ Help Desk ได้ตามมาตรฐาน
ระยะเวลาการรับเรื่อง (ร้อยละ 15) **15**

1.3 ความสำเร็จในการดำเนินกิจกรรม
การพัฒนาหลักสูตรและส่งเสริมการศึกษา
ด้านความมั่นคงปลอดภัยไซเบอร์ร่วมกับ
สถานศึกษาในประเทศไทย (ร้อยละ 15) **15**

1.4 ความสำเร็จในการจัดทำแผนเผชิญเหตุ
ด้านไซเบอร์ของหน่วยงานของรัฐและ
หน่วยงานโครงสร้างพื้นฐานสำคัญ
ทางสารสนเทศ (ร้อยละ 10) **10**

1.5 ความสำเร็จในการจัดการฝึกและทดสอบ
แผนเผชิญเหตุในกรณีเกิดเหตุภัยคุกคาม
ทางไซเบอร์ในระดับวิกฤติ (ร้อยละ 5) **5**

1.6 ร้อยละของประชาชนหรือบุคลากรของ
หน่วยงานเป้าหมายที่ทำแบบทดสอบและ
เข้าร่วมกิจกรรมสร้างความตระหนักรู้
เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
(ร้อยละ 5) **5**

องค์ประกอบที่ 2

การประเมินศักยภาพ
การดำเนินงานเพื่อบรรลุเป้าหมาย
(Potential Perspective)

ร้อยละ **30**

ตัวชี้วัด

ได้ร้อยละ

2.1 การพัฒนาระบบบัญชีข้อมูล
(Data Catalog) เพื่อนำไปสู่การเปิดเผย
ข้อมูลภาครัฐ (Open Data) (ร้อยละ 10) **10**

2.2 การประเมินสถานะของหน่วยงานภาครัฐ
ในการเป็นระบบราชการ 4.0 (PMQA 4.0)
(ร้อยละ 10) **10**

2.3 การควบคุมดูแลกิจการของ
คณะกรรมการองค์การมหาชน
(ร้อยละ 10) **8.60**

ผลการประเมิน
จากบุคคลภายนอก
รวมคะแนน
ทั้ง 2 องค์ประกอบ ได้

ร้อยละ **98.60**



The external evaluation, combining both
assessment components, resulted in a
total score of 98.60 points.



ปัญหา อุปสรรค และข้อเสนอแนะ & แผนการดำเนินงาน ปี 2568

**ISSUES, CHALLENGES, AND RECOMMENDATIONS &
2025 OPERATIONAL PLAN**

ปัญหา อุปสรรค และข้อเสนอแนะ

ISSUES, CHALLENGES, AND RECOMMENDATIONS



ปัญหาและอุปสรรค Issues and Challenges

1

การขับเคลื่อนนโยบายและแผนปฏิบัติการ Driving Cybersecurity Policies and Plans

- หน่วยงานบางส่วน ขาดความรู้และความเข้าใจในนโยบาย
Lack of understanding among agencies
- ไม่สามารถปรับแผนงานให้สอดคล้องกับแผนปฏิบัติการได้
Inability to align internal projects with the plans

2

ประชาชนยังตกเป็นเหยื่อภัยคุกคามไซเบอร์ Public Vulnerability to Cyber Threats

- ทักษะด้านความมั่นคงปลอดภัยไซเบอร์ยังไม่ครอบคลุมทุกภาคส่วน
Cybersecurity skills remain underdeveloped across sectors

3

ระบบของหน่วยงานยังมีช่องโหว่และไม่ปลอดภัย Security Vulnerabilities in Agency Systems

- ซอฟต์แวร์ล้าสมัย รหัสผ่านอ่อนแอ บุคลากรขาดทักษะ
Outdated software, weak passwords, lack of expertise

4

การบังคับใช้ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ฯ ยังมีปัญหา และอุปสรรคอยู่หลายประการ เช่น Challenges in Enforcing the Cybersecurity Act

- กฎหมายไม่ชัดเจน
Unclear legislation
- บทลงโทษไม่เหมาะสม
Inappropriate penalties
- ความหลากหลายของภัยคุกคามทางไซเบอร์
Diversity of cyber threats
- เทคโนโลยีที่เปลี่ยนแปลงไปในปัจจุบัน
Rapidly evolving technology



ข้อเสนอแนะ Recommendations

ควรขับเคลื่อนผ่านทุกภาคส่วน

Drive implementation across all sectors

- ประสานงานกับ Regulator, หน่วยงาน CII และหน่วยงานของรัฐให้เข้มข้นขึ้น
Coordinate with regulators, organizations of critical information infrastructure, and government agencies
- พลิกดันให้ดำเนินการผ่านการประเมินรางวัล Prime Minister Award
Promote compliance through the Prime Minister Award evaluation process

เพิ่มความตระหนักรู้และยกระดับทักษะ

Raise awareness and enhance skills

- สร้างความตระหนักรู้ให้ประชาชนและยกระดับทักษะผู้ปฏิบัติงานเพื่อดูแลประชาชน
Educate the public and train practitioners continuously
- ร่วมมือกับภาคการศึกษาและเอกชนในการพัฒนาบุคลากร
Collaborate with education and private sectors to develop experts

พัฒนาระบบและเพิ่มมาตรฐานความปลอดภัย

Improve system security and standards

- ทดสอบช่องโหว่ สร้างความตระหนักรู้เรื่องการอัปเดตซอฟต์แวร์ และการใช้รหัสผ่านที่มั่นคงปลอดภัย
Test for vulnerabilities, update software, use strong passwords
- เสริมสร้างผู้เชี่ยวชาญและกำหนดนโยบายสิทธิ์อย่างเข้มงวด
Build expertise and enforce strict access control policies

เร่งปรับปรุงกฎหมายและขอบเขตการบังคับใช้

Amend and expand enforcement scope

- ทบทวนพระราชบัญญัติและกฎหมายที่เกี่ยวข้อง
Review and update the Cybersecurity Act and related laws
- ปรับปรุงให้เหมาะสมกับสถานการณ์และเทคโนโลยีปัจจุบัน
Ensure they align with current risks and technologies

แผนการดำเนินงาน ในปีงบประมาณ พ.ศ. 2568

OPERATIONAL PLAN FOR FISCAL YEAR 2025

ในปี 2568 กลยุทธ์ที่ดัดแปลงดำเนินการเร่งด่วนภายใต้
Team Thailand for Cybersecurity สามารถแบ่งออกเป็น 5 ด้าน ดังนี้

ด้านที่ 1

การขับเคลื่อนและบูรณาการ
หน่วยงานที่เกี่ยวข้องให้สอดคล้อง
กับนโยบายและแผนปฏิบัติการ
ว่าด้วยการรักษาความมั่นคง
ปลอดภัยไซเบอร์
(พ.ศ. 2565-2570)

ด้านที่ 2

การเสริมสร้างและพัฒนา
ขีดความสามารถของบุคลากร
องค์ความรู้ และเทคโนโลยี สอดคล้อง
ต่อยุทธศาสตร์ที่ 1 สร้างขีดความสามารถ
ในการรักษาความมั่นคงปลอดภัยไซเบอร์
ของประเทศ (บุคลากร องค์ความรู้
และเทคโนโลยี) (Capacity)

ด้านที่ 3

การเสริมสร้างความร่วมมือระหว่าง
หน่วยงาน สร้างเครือข่ายความร่วมมือระหว่าง
หน่วยงานภาครัฐ ภาคเอกชน และองค์กร
ระหว่างประเทศเพื่อเตรียมความพร้อมในการ
รับมือทางไซเบอร์สอดคล้องต่อยุทธศาสตร์ที่ 2
บูรณาการความร่วมมือเพื่อเตรียมความพร้อม
ในการรับมือทางไซเบอร์และฟื้นคืนสู่
สภาพปกติได้ (Partnership)

ด้านที่ 4

การส่งเสริมความพร้อมในการฟื้นคืน
ระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
และระบบบริการภาครัฐให้กลับสู่สภาพปกติได้
อย่างรวดเร็ว ปลอดภัยและทันเวลา สอดคล้อง
ต่อยุทธศาสตร์ที่ 3 สร้างบริการภาครัฐและ
โครงสร้างพื้นฐานสำคัญทางสารสนเทศ
ให้มีความมั่นคงปลอดภัยไซเบอร์
และฟื้นคืนสู่สภาพปกติได้
(Resilience)

ด้านที่ 5

การสร้างศักยภาพของหน่วยงาน
ระดับชาติและหน่วยงานระดับภาคส่วน
(Sector) ให้มีคุณภาพและมาตรฐาน
สอดคล้องต่อยุทธศาสตร์ที่ 4
สร้างศักยภาพของหน่วยงานระดับชาติ
ให้มีคุณภาพและมาตรฐาน
(Standard)



สามารถสแกน QR Code เพื่ออ่านแผนปฏิบัติการประจำปีงบประมาณ พ.ศ. 2568 เพิ่มเติมได้

Scan the QR Code for detailed information on the **Fiscal Year 2025 Action Plan**.

Operational Plan for Fiscal Year 2025

In FY2025, addressing urgent needs under the “**Team Thailand for Cybersecurity**” strategy is divided into five key focus areas:

1. Policy Alignment and Integration

Driving and integrating relevant agencies to align with the Cybersecurity Policy and Action Plan (2022-2027).

2. Capacity Building

Enhancing and developing personnel, knowledge, and technology capabilities align with Strategy 1: Building the Nation's Cybersecurity Capabilities (Workforce, Knowledge, and Technology).

3. Partnership Development

Strengthening collaboration and networks among government agencies, private sectors, and international organizations to enhance cyber preparedness, consistent with Strategy 2: Fostering Partnerships for Cyber Incident Response and Resilience.

4. Resilience Enhancement

Promoting readiness to restore critical information infrastructure and public services to normalcy quickly, safely, and promptly, aligned with Strategy 3: Enhancing Cybersecurity Resilience for Public Services and Critical Information Infrastructure.

5. Standardization and Quality Improvement

Enhancing the capabilities of national and sectoral agencies to meet quality and international standards, as outlined in Strategy 4: Enhancing the Capacity and Standards of National Agencies.

บทสรุปส่งท้าย

CLOSING SUMMARY

ในปี พ.ศ. 2567 ที่ผ่านมา สกมช. ได้ขับเคลื่อนการรักษาความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของประเทศไทยด้วยหลักแนวคิด **Proactive Protection** ซึ่งเป็นการป้องกันก่อนเกิดเหตุซึ่งเปรียบได้กับการล้อมคอกก่อนวัวหาย และแนวคิด **Total Defense** ซึ่งเป็นการเสริมความแข็งแกร่งให้ทุกหน่วยงานพร้อมป้องกัน รับมือ และลดความเสี่ยงอย่างมีประสิทธิภาพ ส่งผลให้ประเทศไทยมีการยกระดับความมั่นคงปลอดภัยไซเบอร์อย่างเห็นได้ชัด ดังที่ได้เห็นผลงานสำคัญต่าง ๆ ที่เกิดขึ้น อาทิ

- ▶ การประเมินความมั่นคงปลอดภัยไซเบอร์ตามดัชนีความมั่นคงปลอดภัยไซเบอร์ระดับโลก (GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) ได้คะแนน 99.22 จาก 100 คะแนนเต็ม ซึ่งจัดอยู่ในอันดับ 7 จาก 194 ประเทศทั่วโลก
- ▶ การยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) เป็นสมาชิก FIRST และ AP-CERT ซึ่งเป็นองค์กรสากลระหว่างประเทศในด้านการรับมือ ตอบสนองภัยคุกคามทางไซเบอร์
- ▶ การประกาศยกระดับให้ภัยคุกคามทางไซเบอร์ที่เกิดจากแอปฟูดเงินเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง
- ▶ การขับเคลื่อนและผลักดันประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

ในปี 2568 สกมช. จะเดินหน้าดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของประเทศไทยให้มีประสิทธิภาพ และต่อเนื่อง นอกจากนี้เสริมสร้างความเข้มแข็งของระบบโครงสร้างพื้นฐานทางสารสนเทศและระบบบริการที่สำคัญของประเทศแล้ว ยังเตรียมความพร้อมในการฟื้นคืนระบบให้กลับสู่สภาวะปกติโดยเร็วและมั่นคง จึงจำเป็นอย่างยิ่งที่ต้องดำเนินการตามกลยุทธ์ ซึ่งสามารถแบ่งออกเป็น 5 ด้าน ประกอบด้วย

- ด้านที่ 1** การขับเคลื่อนและบูรณาการหน่วยงานที่เกี่ยวข้องให้สอดคล้องกับนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570)
- ด้านที่ 2** การเสริมสร้างและพัฒนาขีดความสามารถของบุคลากร องค์ความรู้ และเทคโนโลยี
- ด้านที่ 3** การเสริมสร้างความร่วมมือระหว่างหน่วยงาน สร้างเครือข่ายความร่วมมือระหว่างหน่วยงานภาครัฐ ภาคเอกชน และองค์กรระหว่างประเทศเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์
- ด้านที่ 4** การส่งเสริมความพร้อมในการฟื้นคืนระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศและระบบบริการภาครัฐในกลับสู่สภาวะปกติได้อย่างรวดเร็ว ปลอดภัยและทันเวลา
- ด้านที่ 5** การสร้างศักยภาพของหน่วยงานระดับชาติและหน่วยงานระดับภาคส่วน (Sector) ให้มีคุณภาพและมาตรฐาน

Team Thailand for Cybersecurity



การส่งเสริมและสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์ ด้วยการยกระดับ สกมช. ให้เป็นองค์กรสมรรถนะสูง เป็นศูนย์กลางขับเคลื่อนความมั่นคงปลอดภัยไซเบอร์ของประเทศ สร้างความเชื่อมั่นให้กับทุกภาคส่วนในการรักษาความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งบูรณาการและยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน Regulator หน่วยงาน CII หน่วยงานของรัฐ หน่วยงานภาคเอกชน และหน่วยงานภาคประชาสังคม ด้วยการสร้าง **Team Thailand for Cybersecurity** อย่างเข้มแข็งและยั่งยืน

In 2024, the National Cyber Security Agency (NCSA) has driven Thailand's cybersecurity initiatives using two key approaches: Proactive Protection, which emphasizes prevention akin to “locking the barn before the horse escapes,” and Total Defense, which strengthens all agencies to prevent, respond to, and mitigate risks effectively. These strategies have significantly elevated the nation's cybersecurity landscape, as demonstrated by key achievements, including:

- ▶ Achieving a score of **99.22 out of 100** in the **Global Cybersecurity Index (GCI)** by the International Telecommunication Union (ITU), ranking **7th among 194** countries worldwide.
- ▶ Elevating **ThaiCERT** to membership in **FIRST** and **AP-CERT**, international organizations for cybersecurity incident response.
- ▶ Declaring **cyber threats from mobile banking trojan applications** as 'Incident at a Critical Level'
- ▶ Promoting and implementing the **Notification of the National Cyber Security Committee (NCSC) on Cybersecurity Standards for Cloud Systems, B.E. 2567 (2024)**.

In 2025, the NCSA will continue advancing Thailand's cybersecurity efforts efficiently and consistently. This includes strengthening the resilience of the nation's critical information infrastructure and essential services to restore operations swiftly and securely. To achieve these goals, the agency will implement its FY2025 operational plan through five strategic areas:

1. Driving and integrating relevant agencies to align with the **Cybersecurity Policy and Action Plan (2022-2027)**.
2. **Building the Nation's Cybersecurity Capabilities** (Workforce, Knowledge, and Technology).
3. **Fostering Partnerships** for Cyber Incident Response and Resilience.
4. **Enhancing Cybersecurity Resilience** for Public Services and Critical Information Infrastructure.
5. **Enhancing the Capacity and Standards** of National Agencies.

To support these efforts, the NCSA aims to become a **high-performance organization** central to national cybersecurity. By fostering collaboration across regulators, organizations of critical information infrastructure, government agencies, private sectors, and civil society, the NCSA seeks to build a strong and sustainable Team Thailand for Cybersecurity, ensuring confidence and resilience in the face of evolving cyber challenges.



ภาคผนวก

APPENDIX

คำศัพท์ทางไซเบอร์

คำศัพท์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

ภาษาอังกฤษ	ความหมาย/คำจำกัดความ
Advanced Persistent Threat (APT)	การโจมตีทางไซเบอร์ประเภทนี้เป็นการโจมตีที่มีความซับซ้อนและมุ่งเน้นเป้าหมายเฉพาะ โดยดำเนินการโดยกลุ่มผู้โจมตีที่มีศักยภาพสูงและมีทรัพยากรเพียงพอ เช่น รัฐบาล หน่วยงานข่าวกรอง หรือองค์กรขนาดใหญ่ ทั้งนี้มีเป้าหมายเพื่อการเข้าถึงข้อมูลสำคัญหรือสร้างความเสียหายต่อเป้าหมายที่กำหนดไว้อย่างเฉพาะเจาะจง
Botnet	เครือข่ายของคอมพิวเตอร์หรืออุปกรณ์ที่ถูกควบคุมโดยมัลแวร์ (Malware) และถูกนำมาใช้โดยผู้ไม่ประสงค์ดี (แฮกเกอร์) โดยที่เจ้าของอุปกรณ์ไม่รู้ตัว อุปกรณ์ที่ติดมัลแวร์และกลายเป็นส่วนหนึ่งของ Botnet เรียกว่า “บ็อต” หรือ “ซอมบี้”
Command and Control Server (C&C Server หรือ C2 Server)	เซิร์ฟเวอร์ที่ใช้ในการควบคุมและสั่งการระบบคอมพิวเตอร์หรืออุปกรณ์ที่ถูกโจมตี (โดยทั่วไปจะหมายถึง botnet หรือ เครื่องคอมพิวเตอร์ที่ถูกแฮก) ในบริบทของการโจมตีทางไซเบอร์ C2 Server จะทำหน้าที่เป็นศูนย์กลางที่แฮกเกอร์ใช้ในการส่งคำสั่งไปยังเครื่องที่ถูกควบคุม หรือ bot ที่เชื่อมต่อกับ C2 Server และรับคำสั่งในการทำกิจกรรมต่าง ๆ เช่น การส่งสแปม, การโจมตีแบบ DDoS, การขโมยข้อมูล หรือการกระจายมัลแวร์
Credential Leak	การรั่วไหลของข้อมูลที่สำคัญ เช่น ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) หรือข้อมูลรับรองอื่น ๆ เช่น API keys, tokens หรือข้อมูลสำหรับการยืนยันตัวตน รั่วไหลออกไปจากระบบที่ควรปลอดภัยและเป็นความลับ
Data Breach	การละเมิดข้อมูลที่สำคัญ เช่น ข้อมูลส่วนบุคคล ข้อมูลทางการเงิน ข้อมูลองค์กร หรือข้อมูลที่มีความลับ ถูกเข้าถึง เปิดเผย หรือถูกขโมยโดยไม่ได้รับอนุญาตจากเจ้าของข้อมูลหรือผู้ที่มีอำนาจในการควบคุมข้อมูลนั้น ๆ
Distributed Denial of Service (DDoS)	การโจมตีเครือข่ายหรือระบบด้วยการส่งคำขอจำนวนมากจากหลายแหล่งไปยังเป้าหมายพร้อมกัน จนทำให้ระบบหรือบริการไม่สามารถตอบสนองต่อคำขอที่ถูกต้องจากผู้ใช้งานปกติได้ ส่งผลให้ระบบล่มหรือทำงานช้าลงอย่างมาก
Fake Website	เว็บไซต์ที่ถูกสร้างขึ้นเพื่อเลียนแบบหรือแอบอ้างว่าเป็นเว็บไซต์จริง โดยมีวัตถุประสงค์ในการหลอกลวงผู้ใช้งานในรูปแบบต่าง ๆ เช่น การขโมยข้อมูลส่วนบุคคล การฉ้อโกงทางการเงิน หรือการแพร่กระจายซอฟต์แวร์ที่เป็นอันตราย (Malware)



ภาษาอังกฤษ	ความหมาย/คำจำกัดความ
Fraud	การกระทำที่มีเจตนาหลอกลวงเพื่อแสวงหาผลประโยชน์โดยมิชอบ อาทิ เงิน ทรัพย์สิน หรือข้อมูล โดยการฉ้อโกงดังกล่าวสามารถเกิดขึ้นได้ในหลากหลายรูปแบบและบริบท อาทิ ธุรกิจ การเงิน หรือการทำการธุรกรรมผ่านช่องทางออนไลน์
Two Factor Authentication (2FA)	การยืนยันตัวตนแบบสองปัจจัย คือ กระบวนการรักษาความปลอดภัยที่ใช้การตรวจสอบตัวตนของผู้ใช้ด้วยสองขั้นตอน โดยอาศัย สองปัจจัยที่แตกต่างกัน เพื่อยืนยันว่าผู้ใช้เป็นเจ้าของบัญชีหรือสิทธิ์การเข้าถึงนั้นจริง
Malware	Malicious Software หรือ ซอฟต์แวร์ที่เป็นอันตราย หมายถึงโปรแกรมหรือซอฟต์แวร์ที่ถูกพัฒนาขึ้นโดยมีวัตถุประสงค์ไม่สุจริต เพื่อก่อให้เกิดความเสียหาย แทรกแซงการทำงาน หรือกระทำการส่งละเมิดต่อข้อมูลในระบบคอมพิวเตอร์ อุปกรณ์ หรือเครือข่ายของผู้ใช้งานโดยไม่ได้รับอนุญาต
Misconfiguration	ความผิดพลาดหรือช่องโหว่ที่เกิดขึ้นจากการกำหนดค่าระบบ แอปพลิเคชัน เครือข่าย หรือโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่ไม่ถูกต้อง หรือขาดความปลอดภัย อันส่งผลให้ระบบมีความเสี่ยงต่อการถูกโจมตีหรือทำงานผิดปกติ
Multi Factor Authentication (MFA)	การยืนยันตัวตนหลายปัจจัย คือ กระบวนการรักษาความปลอดภัยที่ใช้มากกว่าหนึ่งปัจจัยในการยืนยันตัวตนของผู้ใช้งาน เพื่อเพิ่มความปลอดภัยและลดความเสี่ยงจากการเข้าถึงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต
Penetration Test	การทดสอบเจาะระบบ หมายถึง กระบวนการทดสอบและประเมินความปลอดภัยของระบบคอมพิวเตอร์ เครือข่าย หรือแอปพลิเคชัน โดยการจำลองการโจมตีจากแฮกเกอร์ที่ได้รับอนุญาต (หรือที่เรียกว่า White Hat Hacker) เพื่อค้นหาช่องโหว่ที่อาจถูกนำไปใช้ในการโจมตีจริง การทดสอบเจาะระบบมีวัตถุประสงค์ในการประเมินความเสี่ยงและการป้องกันภัยคุกคามที่อาจเกิดขึ้นในอนาคต
Ransomware	มัลแวร์ประเภทหนึ่งที่ถูกออกแบบมาเพื่อเข้ารหัสข้อมูลในระบบคอมพิวเตอร์หรือเครือข่ายของผู้ใช้งาน จากนั้นจะมีการเรียกร้องค่าไถ่จากเจ้าของข้อมูล เพื่อแลกกับการปลดล็อกข้อมูลหรือระบบที่ถูกเข้ารหัส โดยแฮกเกอร์มักขู่ว่าจะลบข้อมูลหรือไม่อนุญาตให้ผู้ใช้งานเข้าถึงข้อมูล หากไม่จ่ายเงินค่าไถ่ตามที่กำหนด
Social Engineering	เทคนิคหรือกลวิธีที่ถูกใช้โดยผู้ไม่ประสงค์ดีหรือแฮกเกอร์ในการหลอกลวงหรือชักจูงให้บุคคลหรือองค์กรเปิดเผยข้อมูลที่สำคัญ เช่น รหัสผ่าน ข้อมูลส่วนบุคคล หรือข้อมูลทางการเงิน โดยใช้การหลอกลวงทางจิตวิทยา โดยไม่จำเป็นต้องพึ่งพาช่องโหว่ทางเทคนิคหรือการเจาะระบบ

ภาษาอังกฤษ	ความหมาย/คำจำกัดความ
Supply Chain Attack	การโจมตีที่มุ่งเป้าไปที่ส่วนหนึ่งของห่วงโซ่อุปทานขององค์กร เช่น ผู้จัดหาสินค้าหรือบริการ ซอฟต์แวร์ หรือผู้ให้บริการภายนอก โดยแฮกเกอร์จะเจาะระบบของผู้ให้บริการหรือผู้ผลิตภายนอก เพื่อใช้ช่องโหว่ที่พบในการเข้าถึงระบบหรือข้อมูลขององค์กรที่เกี่ยวข้อง ซึ่งอาจส่งผลให้ข้อมูลถูกขโมย ถูกทำลาย หรือเกิดความเสียหายต่อระบบขององค์กร
Spyware	ซอฟต์แวร์ที่ถูกออกแบบมาเพื่อแอบติดตาม เก็บข้อมูล หรือสอดแนมกิจกรรมของผู้ใช้โดยไม่ได้รับอนุญาต ซอฟต์แวร์ประเภทนี้มักทำงานโดยไม่ให้ผู้ใช้สังเกตเห็น และข้อมูลที่เก็บได้อาจถูกนำไปใช้ในทางที่ไม่เหมาะสม เช่น การขโมยข้อมูลส่วนตัว ข้อมูลทางการเงิน หรือการสอดแนมพฤติกรรมการใช้งานอินเทอร์เน็ต
Spoofing	การปลอมแปลงหรือหลอกลวงข้อมูลเพื่อทำให้ดูเหมือนเป็นแหล่งที่เชื่อถือได้หรือเป็นสิ่งที่ไม่ได้เป็นจริง โดยปกติแล้วการ spoofing จะทำกับข้อมูลที่เกี่ยวกับการสื่อสารผ่านเครือข่ายคอมพิวเตอร์ เช่น การปลอมแปลงที่อยู่ IP, อีเมล หรือเว็บไซต์ เพื่อหลอกลวงผู้ใช้ให้ทำการกระทำที่ไม่ปลอดภัย
Website Defacement	การโจมตีที่ทำให้เนื้อหาบนเว็บไซต์ถูกแก้ไขหรือดัดแปลงโดยผู้โจมตี เพื่อแสดงข้อความ รูปภาพ หรือเนื้อหาที่ไม่เหมาะสม มีวัตถุประสงค์ในการแสดงจุดยืนทางการเมือง การประท้วง หรือการทำลายชื่อเสียงขององค์กรที่เป็นเจ้าของเว็บไซต์
Website Phishing	การสร้างเว็บไซต์ปลอมที่เลียนแบบเว็บไซต์จริง โดยมีวัตถุประสงค์เพื่อหลอกลวงผู้ใช้งานให้เปิดเผยข้อมูลส่วนตัว เช่น รหัสผ่าน ข้อมูลบัตรเครดิต หรือข้อมูลทางการเงิน โดยมักจะใช้การออกแบบที่คล้ายคลึงกับเว็บไซต์ที่ผู้ใช้งานคุ้นเคยและไว้วางใจ เพื่อให้ผู้ใช้งานหลงเชื่อและกรอกข้อมูลสำคัญลงในเว็บไซต์ปลอมดังกล่าว
Vulnerability	ช่องโหว่หรือจุดอ่อนในระบบคอมพิวเตอร์ ซอฟต์แวร์ ฮาร์ดแวร์ หรือโครงสร้างพื้นฐานทางไอที ซึ่งสามารถถูกแฮกเกอร์หรือผู้ไม่ประสงค์ดีใช้เป็นช่องทางในการโจมตีเพื่อเข้าถึงข้อมูลหรือทำลาย ความมั่นคงของระบบนั้น ๆ ช่องโหว่เหล่านี้อาจเกิดขึ้นจากข้อผิดพลาดในการออกแบบ การพัฒนา หรือการตั้งค่าระบบที่ไม่ปลอดภัย
Virtual Private Network (VPN)	เทคโนโลยีที่สร้างการเชื่อมต่อที่มั่นคงปลอดภัยและเป็นส่วนตัวระหว่างผู้ใช้งานและเครือข่ายอินเทอร์เน็ต โดยใช้การเข้ารหัสข้อมูลที่ส่งผ่านการเชื่อมต่อออนไลน์ ซึ่งช่วยป้องกันการดักรับข้อมูลและการโจมตีจากผู้ไม่ประสงค์ดี



TEAM THAILAND



FOR CYBERSECURITY



POLICY TEAM



LEGAL TEAM



INFO-TECH TEAM



CII TEAM



ADMIN TEAM



ACADEMIC TEAM



THAICERT TEAM



RESEARCH TEAM



FINANCE & STRATEGY TEAM



AUDIT TEAM

รายชื่อคณะกรรมการทำงาน

คณะกรรมการกำกับติดตามการดำเนินงานการจัดทำรายงานประจำปี (Annual Report) ปีงบประมาณ พ.ศ. 2567 (Steering Group)

1. เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	ประธานกรรมการ
2. รองเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	รองประธานกรรมการ
3. ผู้เชี่ยวชาญด้านการจัดการองค์การ	ที่ปรึกษา
4. ผู้ช่วยเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	กรรมการ
5. ผู้ทรงคุณวุฒิพิเศษ	กรรมการ
6. ผู้อำนวยการสำนัก/ศูนย์ฯ	กรรมการ
7. ผู้อำนวยการฝ่ายตรวจสอบภายใน	กรรมการ
8. ผู้อำนวยการฝ่ายการคุ้มครองข้อมูลส่วนบุคคล	กรรมการ
9. ผู้อำนวยการฝ่ายพัฒนาองค์กร	กรรมการ
10. ผู้อำนวยการฝ่ายบริหารความเสี่ยง	กรรมการ
11. ผู้อำนวยการสำนักนโยบายยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์	กรรมการและเลขานุการ 1
12. ผู้อำนวยการสำนักบริหารกลาง	กรรมการและเลขานุการ 2
13. นางพัชรีชา ไกรแสงศรี	กรรมการและผู้ช่วยเลขานุการ
14. พันโท ญาณินทร์ สุพันธ์โพธารมณ์	กรรมการและผู้ช่วยเลขานุการ

คณะกรรมการจัดทำรายงานประจำปี (Annual Report) ปีงบประมาณ พ.ศ. 2567 (Working Group)

1. นางชไมพร พงศ์พยุหะ	หัวหน้าคณะกรรมการ
2. นายเอกพงษ์ กิตติวิทยารัตน์	รองหัวหน้าคณะกรรมการ
3. นางสาวสุวรรณี ขุนทองปาน	คณะกรรมการ
4. นางสาวบัณฑิตย์ พุ่มกุมาร	คณะกรรมการ
5. นางสาวกมลพรรณ คงไข	คณะกรรมการ
6. นางสาวยุภาภรณ์ กุ่มโม่ง	คณะกรรมการ
7. นายทักษิณ บุญรอด	คณะกรรมการ
8. นายพงศ์ชินทร์ สกุลรัตนศักดิ์	คณะกรรมการ
9. นางสาววัชรภรณ์ จิตรสง่า	คณะกรรมการ
10. นายศุภณัฐ รัตนวราหะ	คณะกรรมการ
11. นางสาวพรพรรณ มั่นช่วยวงศ์	คณะกรรมการ
12. นายทศพล กลิ่นหอม	คณะกรรมการ
13. นางสาวกนกวรรณ พรศุภปัทมา	คณะกรรมการ
14. นายดนัยวิทย์ ชาญสมร	คณะกรรมการ
15. นางสาวพรวิภา สระทองขำ	คณะกรรมการ
16. นายอดิสร พิมลรัตน์	คณะกรรมการ
17. ว่าที่ร้อยตรีหญิง กัญจนภรณ์ ประไพ	คณะกรรมการ
18. นายทรงวุฒิ ทวีแสง	คณะกรรมการ
19. นายภาณุพงศ์ ม้วนทอง	คณะกรรมการ
20. นางสาวพัฒนภรณ์ แสงศิริชัย	คณะกรรมการ





In Loving Memory of MATTIKA J.

คุณมัตติกา จงพิริยะอนันต์ คือหนึ่งในกำลังสำคัญที่ร่วมสร้างและบุกเบิก สกมช.
ให้เป็นหน่วยงานที่มั่นคงแข็งแกร่งเช่นในวันนี้
การจากไปของคุณมัตติกา นับเป็นความสูญเสียที่ยิ่งใหญ่ ทั้งในด้านการทำงาน
และมิตรภาพที่เราได้ร่วมแบ่งปันกันมา ด้วยการอุทิศตนเพื่อหน้าที่การงานอย่างเต็มที่
ในฐานะเพื่อนร่วมทางที่ซื่อสัตย์ จริงใจ และเปี่ยมด้วยน้ำใจ
ด้วยความทุ่มเททั้งในเวลางานและนอกเวลาเสมอ
แม้วันนี้เธอจะไม่ได้อยู่กับเราแล้ว แต่เรานั้นเชื่อว่าเธอได้พักอยู่ในอ้อมกอดแห่งความรัก
และความเมตตาของพระเจ้า และพบกับความสงบสุขในดินแดนแห่งสันติสุขของพระองค์

ความดี ความมุ่งมั่น และแบบอย่างที่คุณมัตติกาได้ฝากไว้
คือแรงบันดาลใจในการใช้ชีวิตและทำงานของพวกเรา
เพื่อองค์กรและประเทศชาติต่อไป

ด้วยความระลึกถึงอย่างสุดซึ้ง
เลขาฯ และพี่ ๆ น้อง ๆ สกมช.





รายงานประจำปี 2567

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

จัดทำและเผยแพร่โดย

**สำนักงานคณะกรรมการการรักษา
ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สภามช.)**



120 หมู่ 3 อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ
80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210



โทรศัพท์ 02 142 6888 โทรสาร 02 143 7593



Email: saraban@ncsa.or.th



DOWNLOAD

พิมพ์ครั้งที่ 1 จำนวน 1,000 เล่ม

กุมภาพันธ์ 2568

พิมพ์ที่ บริษัท พี ดับบลิว พรินติ้ง จำกัด

ISBN 978-616-94218-2-5

