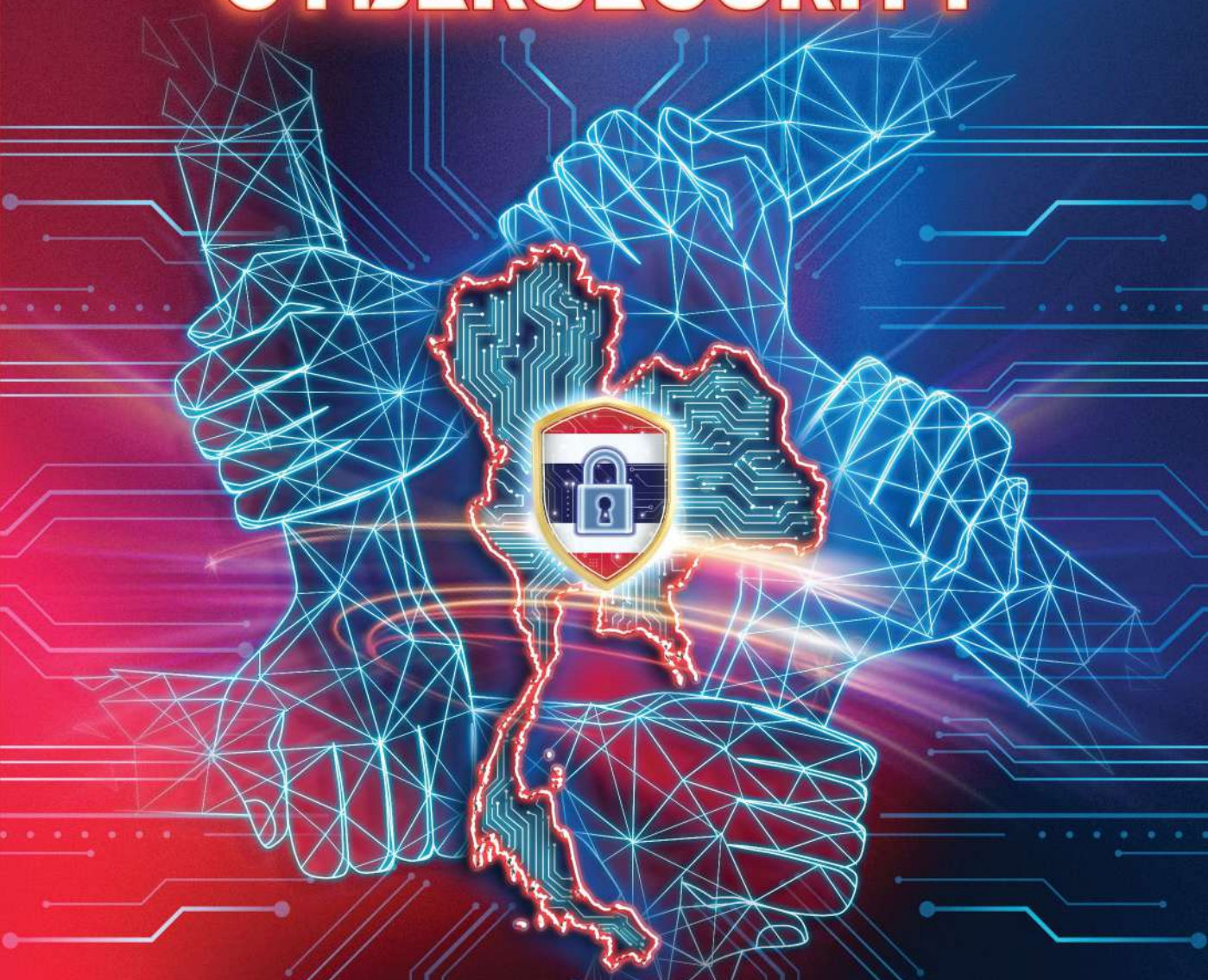
TEAM THAILAND FOR CYBERSECURITY



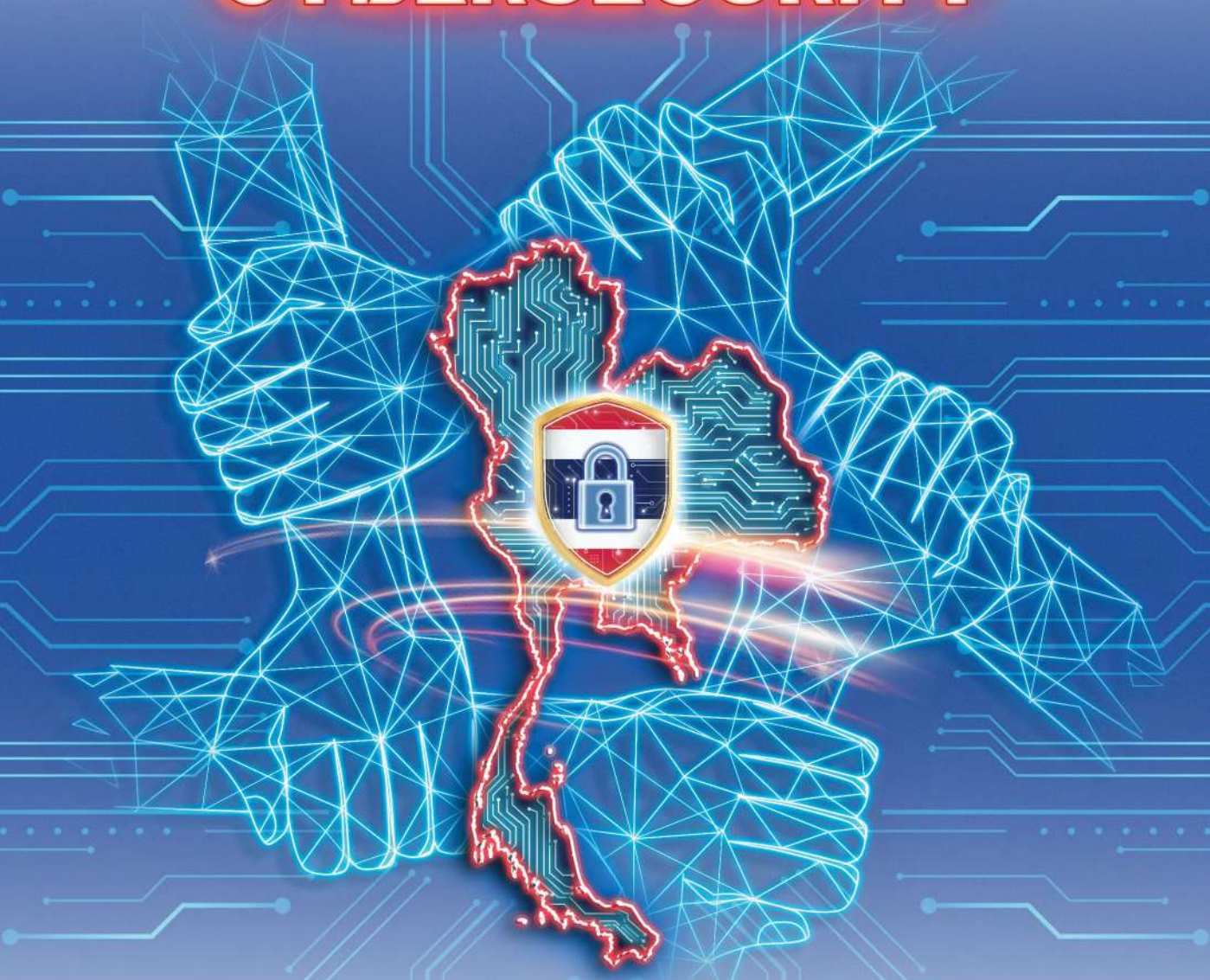
รายงานประจำปี 2568

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

NATIONAL CYBER SECURITY AGENCY

ANNUAL REPORT 2025

TEAM THAILAND
FOR
CYBERSECURITY



รายงานประจำปี 2568

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

NATIONAL CYBER SECURITY AGENCY

ANNUAL REPORT 2025

น้อมรำลึกในพระมหากรุณาธิคุณ

สมเด็จพระนางเจ้าสิริกิติ์ พระบรมราชินีนาถ พระบรมราชชนนีพันปีหลวง

In Remembrance of Her Majesty's Boundless Royal Grace Her Majesty Queen Sirikit The Queen Mother

ข้าพระพุทธเจ้า คณะผู้บริหาร พนักงาน และเจ้าหน้าที่
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)
With most profound respect and gratitude,
The Executives, Staff, and Officials of The National Cyber Security Agency (NCSA)


พิธีบำเพ็ญกุศลถวายพระราชกุศลแด่สมเด็จพระนางเจ้าสิริกิติ์
พระบรมราชินีนาถ ทรงบรมราชอนุสรณ์ปีหลวง และพิธีแสดงความอาลัย

ผลงานเด่นประจำปี 2568 ของ สกมช.

กิจกรรมสำคัญระดับชาติและระดับนานาชาติ
Key National and International Initiatives

PM Awards 2025 รางวัลที่มอบให้หน่วยงานไทย เพื่อยกระดับความมั่นคงปลอดภัยไซเบอร์ มีองค์กรสมัครเข้าร่วมกว่า 200 หน่วยงาน ผ่านการประเมินตามมาตรฐานสากล และ**ได้รับรางวัลรวม 173 หน่วยงาน**

Awards were presented to Thai organizations for enhancing national cybersecurity. More than 200 organizations were assessed against international standards, with 173 receiving awards.

Thailand's National Cyber Exercise 2025

ฝึกซ้อมรับมือภัยคุกคามไซเบอร์ระดับชาติ
หน่วยงานเข้าร่วมการฝึก: 333 หน่วย ผู้เข้าร่วม 1,615 คน
ผลการประเมินความพึงพอใจ 91.20% **(ระดับดีมาก)**

A national-level cyber threat response exercise involved 333 organizations and 1,615 participants, achieving a 91.20% satisfaction rating **(Very Good)**.

Thailand Cybersecurity Product and Service Awards 2024

จัดประกวดผลิตภัณฑ์และบริการด้านความมั่นคงปลอดภัยไซเบอร์
มีผู้สมัครเข้าร่วม 23 ราย
และได้รับรางวัล 9 ราย

A competition recognizing cybersecurity products and services attracted 23 applicants, with 9 award recipients.

รับฟังความคิดเห็นปรับปรุง พ.ร.บ. ไซเบอร์ พ.ศ. 2562

ให้ทันสมัย ยืดหยุ่น และเสริมประสิทธิภาพการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์
มีผู้เข้าร่วม รวมกว่า 2,000 คน

A public consultation on the revision of the Cybersecurity Act B.E. 2562 (2019) was undertaken to strengthen its modernity, flexibility, and effectiveness in addressing cyber risks and threats, with over 2,000 participants.

Thailand International Cyber Week 2025

เวทีแลกเปลี่ยนองค์ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ระดับนานาชาติ
มีผู้เข้าร่วมงานกว่า 3,142 คน จาก 46 ประเทศ

An international cybersecurity knowledge-sharing platform with over 3,142 participants from 46 countries.

เตรียมความพร้อมประเมินดัชนี GCI ปี 2569

ยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ
ขับเคลื่อนผ่านกิจกรรมสำคัญ ทั้งการอบรมสร้างความเข้าใจในมาตรฐานการประเมินระดับโลก และการประชุมเพื่อรวบรวมข้อมูล ข้อเท็จจริง และหลักฐานประกอบการประเมิน โดยมีผู้เข้าร่วมกิจกรรมรวมกว่า 300 คน

Preparations for the Global Cybersecurity Index (GCI) 2026 assessment were undertaken to enhance the nation's cybersecurity posture. Key initiatives included training to strengthen understanding of global assessment standards, as well as coordination meetings to gather data, factual information, and supporting evidence for the evaluation process. These activities engaged more than 300 participants.

Cyber SEA Game 2024

ศึกแข่งขัน Capture the Flag ระดับภูมิภาคอาเซียน
ส่งเด็กไทยจากเวที Thailand Cyber Top Talent 2024 เข้าร่วม

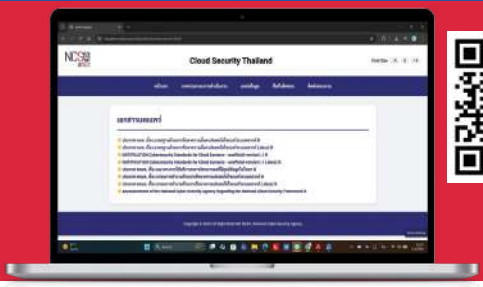
A regional ASEAN Capture the Flag (CTF) competition, with Thailand's representatives selected from Thailand Cyber Top Talent 2024.

สนับสนุน Cyber Hero ประเทศไทย

ส่งไปคว้า เหรียญเงิน งาน WorldSkills ASEAN 2025
Empowering Thailand's Cyber Heroes - Silver Medal Achievement at WorldSkills ASEAN 2025

NCSA HIGHLIGHTS 2025

การขับเคลื่อนมาตรฐาน และ รางวัลเกียรติยศ
Advancing Standards and Distinguished Recognition



เปิด "Cloud Security Thailand" เว็บไซต์กลางด้านความมั่นคงปลอดภัยระบบคลาวด์ พร้อมคลัง "เอกสารมาตรฐานและคู่มือที่เกี่ยวข้อง" เพื่อใช้กำหนดนโยบาย ออกแบบมาตรการควบคุม และยกระดับความมั่นคงปลอดภัยของระบบคลาวด์ในองค์กร ทาง cloudsecurity.ncsa.or.th

Launch of **"Cloud Security Thailand,"** a central cloud security platform providing standards documents and practical guidelines to support policy development, control design, and the strengthening of cloud security across organizations. Available at **cloudsecurity.ncsa.or.th.**

มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

ประกาศ Website Security Standard
มาตรฐานเว็บไซต์ที่มั่นคงปลอดภัย เตรียมพร้อมบังคับใช้ในเดือนกันยายน 2569

The Website Security Standard has been officially issued and is scheduled to take effect in September 2026.

เผยแพร่ AI Security Guidelines
แนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย แนวทางที่ทันสมัยที่สุดในอาเซียน

AI Security Guidelines Launched: Setting the Benchmark for Secure AI Use in ASEAN

สกมช. ผ่านการประเมินองค์กรคุณธรรม ในระดับคุณธรรมต้นแบบ
ประจำปีงบประมาณ พ.ศ. 2568

NCSA achieved the **"Moral Role Model"** level in the Moral Organization

สกมช. รับโล่รางวัลเชิดชูเกียรติ "คนดีของสังคม"
เนื่องในโอกาสครบรอบ 25 ปี แห่งการสถาปนา มหาวิทยาลัยนอร์ทกรุงเทพ

NCSA was honored with the **"Good Person of the Society"** Honorary Trophy at the 25th Anniversary of North Bangkok University.

ดร.สุนทร ศิระไพศาล หัวหน้างานวิจัย และรักษาการผู้อำนวยการฝ่ายวิจัยและพัฒนาเครือข่ายวิจัย ได้เข้าเฝ้าฯ รับพระราชทานเกียรติบัตร **รางวัลการวิจัยแห่งชาติ : รางวัลวิทยานิพนธ์** ประจำปีงบประมาณ 2568 จากผลงานเรื่อง **"เฟรมเวิร์กการรับรองความถูกต้องที่มีประสิทธิภาพสำหรับ MapReduce ในสภาพแวดล้อมคลาวด์สาธารณะหลายระบบ"** ซึ่งนับเป็นรางวัลระดับประเทศที่ยกย่องผลงานวิจัยที่มีคุณภาพสูงและมีคุณูปการต่อการพัฒนาประเทศ

Dr. Soontorn Sirapaisan, Lead of the Research Group and Acting Head of the Research and Research Collaboration Section, was granted an audience to receive the **National Research Award: Thesis Award 2025**, in recognition of his outstanding research, *"An Effective and Efficient Authentication Framework for MapReduce in a Multiple Public Cloud Environment."* The award honors excellence in research that delivers meaningful impact on the nation's development.

ผลงานเด่นประจำปี 2568 ของ สกมช.

พัฒนาบุคลากรเชิงรุก สร้างความตระหนักรู้ทุกภาคส่วน

โครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ระยะที่ 2

9 หลักสูตร ผู้เข้าอบรม **14,344** คน
Certificate **1,235** ใบ

Intensive Cybersecurity Capacity Building Program (Phase II)
- 9 specialized training courses
- 14,344 participants trained
- 1,235 certificates issued

NCSA Cyber Clinic

จัดอบรม **6** ครั้ง ยอดผู้เข้าร่วม **993** คน
ยอดรวมผู้เข้าร่วมงาน ปี 2567-ปัจจุบัน **2,186** คน

- 6 training sessions
- 993 participants
- 2,186 cumulative participants trained (2024-present)

Lead Implementer, Lead Auditor

เป้าหมาย **150** คน ยอดผู้เข้าร่วมทั้งสิ้น **998** คน

Target: 150 certified professionals
Achievement: 998 cumulative participants

แพลตฟอร์มเรียนรู้ออนไลน์ NCSA Mooc

ผู้เข้าอบรม **20,638** คน
ได้ประกาศนียบัตรรับรองผ่านหลักสูตร **6,004** คน

- 20,638 learners enrolled on the NCSA Mooc Platform
- 6,004 certificates issued

THNCA E-Learning

ผู้เข้าอบรม **15,378** คน
ได้ประกาศนียบัตรรับรองผ่านหลักสูตร **7,145** คน

- 15,378 learners enrolled on the THNCA E-Learning Platform
- 7,145 certificates issued

การอบรมและทดสอบ Certified in Cybersecurity ของ ISC2

ผู้เข้าร่วมออนไลน์ **11,410** คน
ผู้เข้าอบรมผ่านยูทูบ **1,312** ครั้ง
ผู้ลงทะบียนสอบ CC **3,976** คน
ผู้สอบผ่าน **207** คน

ISC2 Certified in Cybersecurity (CC)
- 11,410 online participants
- 1,312 training sessions
- 3,976 exam registrants
- 207 certified

จัดอบรมร่วมกับศูนย์ AJCCBC

ผู้เข้าอบรมทั้งหมด **1,474** คน

- **1,474** participants trained through joint programs in collaboration with the **AJCCBC**

NCSA HIGHLIGHTS 2025

Proactive Workforce Development and Awareness Building Across All Sectors

NCSA Cybersecurity Knowledge Sharing

จัด **10** ครั้ง
ผู้เข้าร่วม **44,511** คน

- **10 sessions held**
- **44,511 participants**

โครงการอบรมร่วมกับ กอ.รมน.

77 จังหวัด ทั่วประเทศ
ผู้เข้าร่วม **2,339** คน

Training Program in Collaboration with the Internal Security Operations Command (ISOC)
- 77 provinces nationwide
- 2,339 participants

อบรมร่วมกับ Microsoft

สำหรับนักเรียน นักศึกษา บุคลากร และประชาชนทั่วไป
ผู้เข้าร่วม **34,282** คน

In collaboration with Microsoft, serving students, university students, personnel, and the general public
- 34,282 participants

NCSA x NBTC Cyber Top Talent 2025

เฟ้นหาดาวรุ่ง ช้างเผือกไซเบอร์
ผู้เข้าอบรม **3,000** คน
ทีมเข้าร่วมแข่งขัน **110** ทีม
ผู้เข้าร่วมแข่งขันกว่า **300** คน
ทีมเข้ารอบ **16** ทีม

Discovering Rising Stars and Exceptional Cybersecurity Talent
- 3,000 trainees
- 300+ competitors
- 110 teams participated
- 16 finalist teams

NCSA Cybersecurity Knowledge Sharing ร่วมกับ สพฐ. จัด 4 ครั้ง

ผู้เข้าร่วมปี **2568** จำนวน **2,051** คน
ยอดผู้เข้าร่วมทั้งสิ้น **26,132** คน

In collaboration with the **Office of the Basic Education Commission (OBEC)**
- 4 sessions organized
- 2,051 participants in 2025
- 26,132 cumulative participants

อบรมหลักสูตรสำหรับเยาวชนสู่ศูนย์อินเทอร์เน็ตสาธารณะ (USO Net)

ผู้เข้าร่วม **10,645** คน

Training Courses for Youth at Public Internet Centers (USO Net)
- 10,645 participants

กิจกรรมอบรมเผยแพร่ความรู้สำหรับเยาวชนสู่ศูนย์ดิจิทัลชุมชน

ผู้เข้าร่วม **1,877** คน

Training and Knowledge Dissemination Activities for Youth at Community Digital Centers
- 1,877 participants

ไซเบอร์บอร์ดเกม

แจกจ่ายให้หน่วยงานทั่วประเทศ
ปี 2567 จำนวน **437** ชุด
ปี 2568 จำนวน **600** ชุด

Cyber Boardgames Distributed Nationwide
- Year 2024: 437 sets
- Year 2025: 600 sets

กิจกรรมแข่งขัน Thailand Cyber TOP Talent 2025

3,387 คน **1,352** ทีม

Thailand Cyber Top Talent 2025
- Participants: 3,387 persons
- Teams: 1,352 teams

สรุปยอดคนเข้าร่วมงานตามกลุ่มเป้าหมาย Summary of Participants

จำนวนมากกว่า / คน
By Target Groups More than / persons

450,000

NCSA E-LEARNING | MOOC | AIS อุ่นใจ CYBER

จำนวนมากถึง **236,000** คน
Reaching up to 236,000 people

ผลงานเติบโตต่อเนื่องจำนวน
มากกว่า **1.95** ล้านคน
Continuously Growing Impact
More than 1.95 million people

ผลงานเด่นประจำปี 2568 ของ สกมช.

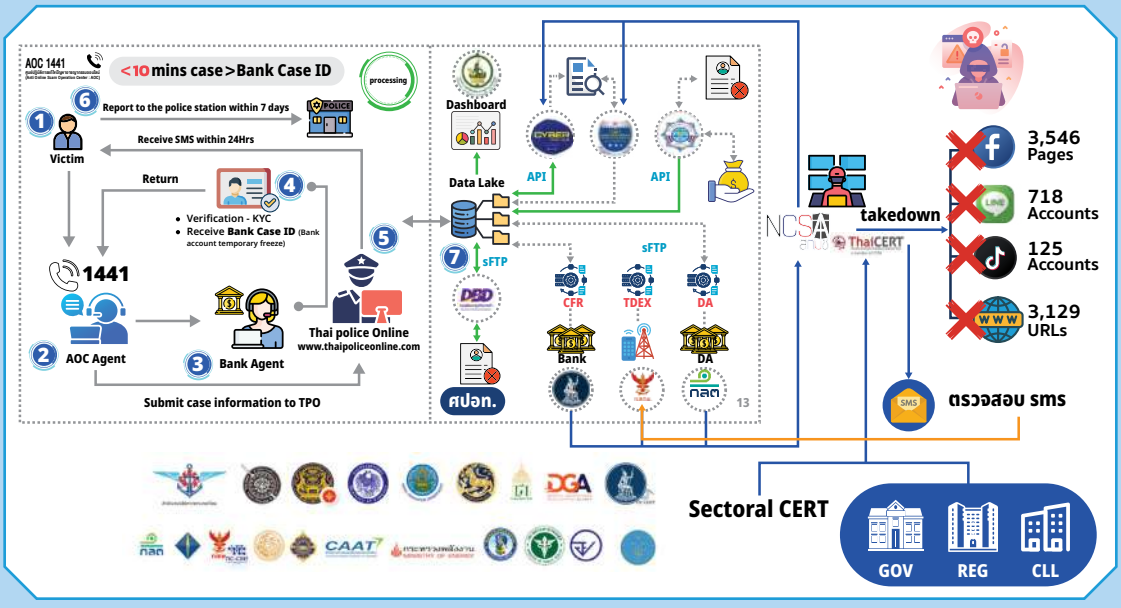
การปราบปรามอาชญากรรมทางเทคโนโลยี

การแก้ไขปัญหาในปัจจุบัน
Current Measures and Progress

ในช่วง 2-3 ปี ที่ผ่านมารัฐบาลไทยได้ดำเนินมาตรการป้องกันและปราบปรามอาชญากรรมทางไซเบอร์อย่างเข้มข้น โดยเฉพาะขบวนการสแกมเมอร์ **สามารถยึดทรัพย์และอายัดเงินจากบัญชีม้าได้กว่า 10,000 ล้านบาท** นอกจากนี้ สกมช. และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ยังได้ร่วมมือกันปิดและนำเว็บไซต์หลอกลวงออกจากระบบ โดยมี**ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT)** เป็นหน่วยงานหลักในการรับแจ้งข้อมูล รวบรวม และประสานการดำเนินการอย่างต่อเนื่อง

Over the past couple of years, the Thai Government has intensified efforts to prevent and suppress cybercrime, particularly online fraud and technology-enabled crimes. Through integrated screening mechanisms, authorities have frozen and seized illicit assets exceeding THB 10 billion.

At the same time, the NCSA, in collaboration with the Ministry of Digital Economy and Society (MDES), has worked with relevant agencies to detect and remove fraudulent websites and online scam platforms. In this regard, the Thailand Computer Emergency Response Team (ThaiCERT) serves as the national focal point for incident reporting, information aggregation, and coordinated response actions.



เร่งขับเคลื่อนมาตรการป้องกันก่อนเกิดเหตุ
Accelerating Proactive Prevention Measures

เตรียมการแก้กฎหมาย : ก่อนเดือนกันยายน 2568 ยกร่างและรับฟังความคิดเห็นการแก้ไข พ.ร.บ. ไซเบอร์ เพื่อขยายอำนาจจัดการภัยคุกคามเชิงรุก และครอบคลุมผู้ให้บริการคลาวด์และศูนย์ข้อมูล

Legal Amendments Preparation: By September 2025, NCSA is advancing public consultations and legislative drafting to strengthen proactive cyber threat management and extend regulatory oversight to Cloud Service Providers and data centers.

ประกาศใช้มาตรฐานขั้นต่ำ : ออกประกาศเรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568 กำหนดมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ โดยจะเริ่มบังคับใช้อย่างเป็นทางการในปี 2569

Minimum Cybersecurity Standards: Issuance of the Website Security Standard, B.E. 2568 (2025), establishing minimum cybersecurity requirements for websites, with official enforcement scheduled for 2026.

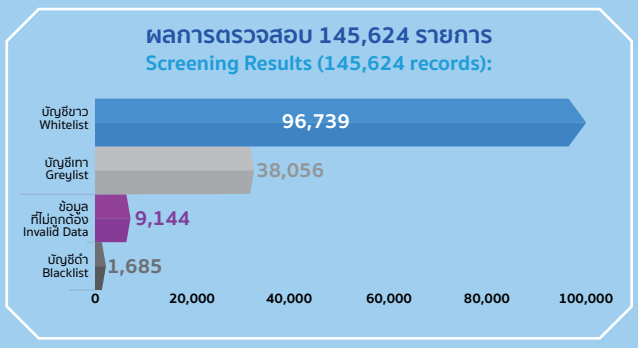
NCSA HIGHLIGHTS 2025

Technology-Enabled Crime Suppression Framework

การจัดการ SMS แนบลิงก์แบบ A2P
A2P SMS Link Governance and Control

ร่วมกับสำนักงาน กสทช. ตรวจสอบลิงก์ใน SMS A2P ก่อนถึงประชาชน เพื่อป้องกัน SMS หลอกลวง และอาชญากรรมไซเบอร์ โดย**ตรวจสอบแล้ว 145,624 รายการ**

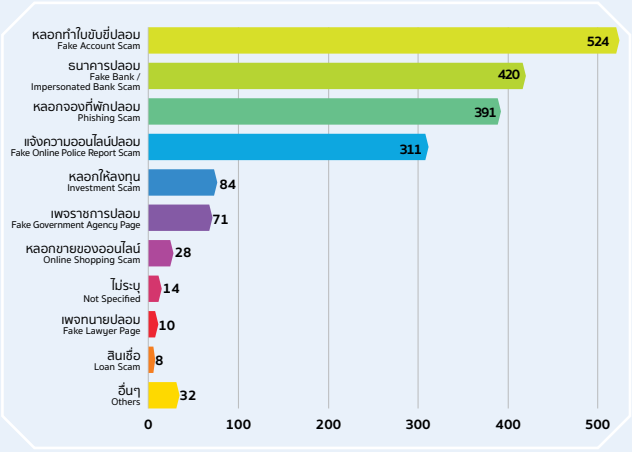
In cooperation with the National Broadcasting and Telecommunications Commission (NBTC), authorities have implemented pre-delivery inspections of A2P SMS messages to safeguard the public from SMS-based scams and cybercrime. To date, 145,624 A2P SMS records have been reviewed, classified, and regulated.



การตรวจสอบเพจที่เข้าข่ายหลอกลวง 1,893 รายการ
Online Scam Platform Monitoring and Enforcement

จากการตรวจสอบ พบมิจฉาชีพใช้แพลตฟอร์มออนไลน์ในการหลอกลวงประชาชน 1,893 รายการ และประสานผู้ให้บริการแพลตฟอร์มออนไลน์ปิดบัญชีปลอม เพื่อลดความเสียหายที่จะเกิดขึ้นกับประชาชน

Investigations have identified **1,893 cases** involving the misuse of online platforms for fraudulent activities targeting the public. Relevant authorities have coordinated with platform service providers to **suspend fraudulent accounts and remove deceptive content,** thereby **reducing potential harm to citizens.**



ครร. เห็นชอบให้การปลอมแปลงหน้าเว็บไซต์เป็นกรณีที่คาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง
CIRC Classifies Website Defacement as a Critical Cybersecurity Threat

คณะกรรมการรับมือภัยคุกคามทางไซเบอร์ในระดับร้ายแรง (ครร.) มีมติเห็นชอบในการประชุมครั้งที่ 1/2568 เมื่อวันที่ 17 กรกฎาคม 2568 ให้กรณีการโจมตีด้วยวิธีการเปลี่ยนแปลงหน้าเว็บไซต์โดยมิชอบ (Web Defacement) ของหน่วยงานในประเทศที่ส่งผลกระทบต่อความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ และความสงบเรียบร้อยของประชาชน เป็นกรณีที่คาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยเฉพาะกรณีที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญของประเทศ พร้อมสั่งการให้ สกมช. ผู้ให้บริการอินเทอร์เน็ต หน่วยงานด้านความมั่นคง และหน่วยงานที่เกี่ยวข้อง บูรณาการความร่วมมือเพื่อรับมือและแก้ไขภัยคุกคามทางไซเบอร์ในลักษณะดังกล่าวอย่างเร่งด่วน

The **Critical Incident Response Committee (CIRC)**, at its Meeting No. 1/2025 held on 17 July 2025, agreed to classify incidents of unauthorized web defacement affecting domestic agencies as cases anticipated to constitute **critical cybersecurity threats**. Such incidents were assessed as having potential impacts on national security, international relations, national defense, and public order-particularly where they involve critical infrastructure. The Committee further instructed the NCSA, internet service providers, security agencies, and other relevant entities to integrate and coordinate their efforts in urgently addressing and mitigating such threats.

ผลงานเด่นประจำปี 2568 ของ สกมช.

เปิดตัวศูนย์รวมผู้เชี่ยวชาญการวิจัย เพื่อความมั่นคงปลอดภัยไซเบอร์แห่งประเทศไทย
Launch of the Thailand Hub of Talents in Cybersecurity Research

HTCR
THAILAND HUB OF TALENTS IN CYBERSECURITY RESEARCH
ศูนย์รวมผู้เชี่ยวชาญการวิจัย เพื่อความมั่นคงปลอดภัยไซเบอร์แห่งประเทศไทย

สกมช. เปิดตัว**ศูนย์รวมผู้เชี่ยวชาญการวิจัยเพื่อความมั่นคงปลอดภัยไซเบอร์แห่งประเทศไทย (ศชวช.)** เมื่อวันพุธที่ 13 สิงหาคม 2568

The NCSA officially launched **the Thailand Hub of Talents in Cybersecurity Research (HTCR) on 13 August 2025.**

เพื่อเป็นศูนย์กลางเชื่อมโยงนักวิจัย ผู้เชี่ยวชาญ และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐ เอกชนและสถาบันการศึกษา

To serve as a national central platform connecting researchers, experts, and relevant agencies from the public, private, and educational sectors.

เพื่อส่งเสริมการสร้างองค์ความรู้ งานวิจัย และนวัตกรรม ที่สอดคล้องยุทธศาสตร์ชาติและความต้องการของประเทศ

To promote the creation of knowledge, research, and innovation that align with national strategic priorities and the country's cybersecurity needs.

เพื่อพัฒนากำลังคนและยกระดับทักษะนักวิจัยให้มีความเชี่ยวชาญเฉพาะทาง สอดคล้องกับเทคโนโลยีใหม่ เช่น AI Security, Quantum, IoT/OT Security และ Data Privacy

To develop and enhance the capacity of researchers with specialized expertise, in line with emerging technologies such as AI Security, Quantum Technology, IoT/OT Security, and Data Privacy.

เพื่อจัดทำฐานข้อมูลกลางด้านการวิจัยและกลไกสนับสนุนทุนวิจัย

To establish a centralized database on cybersecurity research and technologies to support research activities and policy development.

เพื่อเพิ่มประสิทธิภาพการบริหารจัดการข้อมูลและสร้างเครือข่ายความร่วมมือ ขับเคลื่อนการวิจัยสู่การใช้ประโยชน์เชิงนโยบายและเชิงพาณิชย์

To improve the efficiency of research data management and foster collaboration networks, facilitating the translation of research outcomes into policy implementation and practical applications.

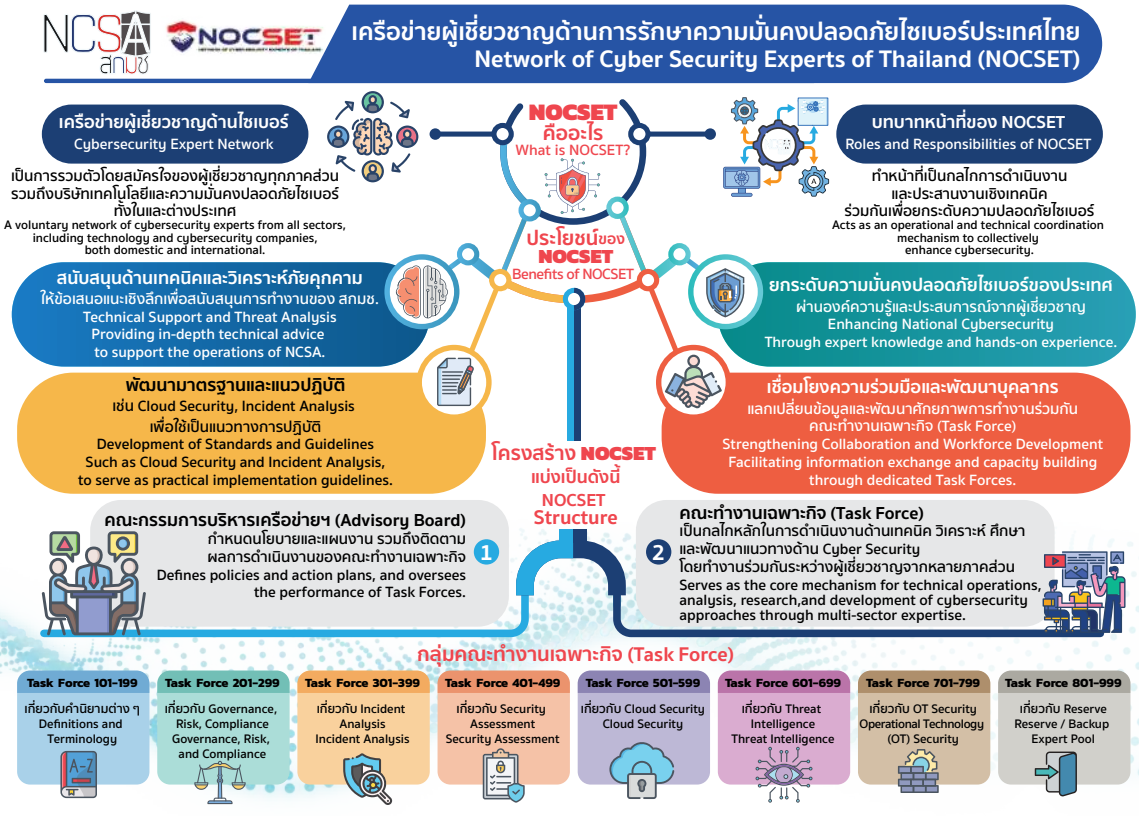
NCSA HIGHLIGHTS 2025

Kick-off เครือข่ายผู้เชี่ยวชาญ เสริมความเข้มแข็งด้านความมั่นคงปลอดภัยไซเบอร์ประเทศไทย

Kick-off of the Expert Network to Strengthen Thailand's Cybersecurity

สกมช. เปิดตัว NOCSET เพื่อขับเคลื่อนการทำงานผ่านเครือข่ายผู้เชี่ยวชาญด้านไซเบอร์จากทุกภาคส่วน ร่วมแลกเปลี่ยนองค์ความรู้ พัฒนามาตรฐาน แนวปฏิบัติ และกลไกการทำงานด้านไซเบอร์ เพื่อยกระดับความมั่นคงปลอดภัยไซเบอร์ของประเทศอย่างเป็นระบบ เมื่อวันที่ 27 สิงหาคม 2568

The NCSA officially launched NOCSET (Network of Cyber Security Experts of Thailand) to drive cybersecurity efforts through a nationwide network of cyber experts from all sectors. The initiative aims to foster knowledge sharing, develop standards, best practices, and operational mechanisms, and enhance coordinated collaboration in order to systematically strengthen Thailand's national cybersecurity posture. The launch took place on 27 August 2025.



สารนายกรัฐมนตรี

MESSAGE FROM THE PRIME MINISTER

ในยุคที่เทคโนโลยีดิจิทัลมีบทบาทสำคัญต่อการดำเนินชีวิต ทำให้เกิดภัยคุกคามรูปแบบต่าง ๆ ที่สร้างความเสียหายต่อชีวิต ทรัพย์สิน และความเป็นอยู่ของประชาชน ตลอดจนสร้างความเสียหายแก่ระบบเศรษฐกิจและความมั่นคงของประเทศ การเสริมสร้าง**ความมั่นคงปลอดภัยไซเบอร์** (Cybersecurity) จึงเป็นภารกิจสำคัญเชิงยุทธศาสตร์ของชาติที่ต้องดำเนินการอย่างเร่งด่วนเพื่อแก้ไขปัญหาที่เกิดจากภัยไซเบอร์ ทั้งปัญหาอาชญากรรมไซเบอร์ (Cybercrime) และ**การหลอกลวงออนไลน์ (Cyber Scam)** เป็นต้น

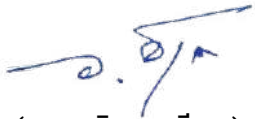
ตลอดระยะเวลาที่ผ่านมา **สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)** ได้ดำเนินภารกิจสำคัญนี้อย่างเข้มแข็ง ช่วยสร้างความมั่นใจให้แก่พี่น้องประชาชน ผมขอชื่นชมคณะผู้บริหารและบุคลากรของ สกมช. ทุกท่านที่มีส่วนสำคัญในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ ทำให้การป้องกันและแก้ไขปัญหาอาชญากรรมทางไซเบอร์เกิดผลสัมฤทธิ์ ซึ่งการจัดทำ**รายงานผลการดำเนินงานประจำปีงบประมาณ พ.ศ. 2568** จะทำให้ทุกภาคส่วนได้รับทราบถึงการดำเนินภารกิจด้านความมั่นคงปลอดภัยไซเบอร์และสื่อสารให้ผู้มีส่วนเกี่ยวข้องได้รับทราบผลการดำเนินการตามแผนงานและมาตรการต่าง ๆ รวมถึงความคืบหน้าเกี่ยวกับสถานการณ์ความมั่นคงปลอดภัยไซเบอร์อันเป็นส่วนหนึ่งของความร่วมมือร่วมใจของทุกคนที่จะสร้างสังคมไทยให้เป็นสังคมแห่งความปลอดภัยอย่างยั่งยืนตลอดไป

ในโอกาสนี้ ผมขอส่งความปรารถนาดีมายังคณะผู้บริหารและบุคลากรของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และผู้มีส่วนเกี่ยวข้องกับการขับเคลื่อนภารกิจการรักษาความมั่นคงปลอดภัยไซเบอร์ของชาติ พร้อมทั้งขออวยพรให้ทุกคนประสบแต่ความสุข ความเจริญ มีกำลังกาย กำลังใจ กำลังสติปัญญาที่เข้มแข็ง เพื่อปฏิบัติหน้าที่ให้สัมฤทธิผลในสิ่งที่มุ่งหมายไว้ทุกประการโดยทั่วกัน

In an era where digital technology plays an increasingly vital role in daily life, a wide range of emerging threats has caused harm to lives, property, and the well-being of the people, while also undermining the national economy and national security. **Strengthening cybersecurity** is therefore a strategic national priority that must be advanced with urgency and determination in order to effectively address the challenges posed by cyber threats, including cybercrime and **online fraud (cyber scams)**, among others.

Over the years, **the National Cyber Security Agency (NCSA)** has carried out its mandate with steadfast commitment and dedication, thereby reinforcing public confidence in the nation's cybersecurity framework. I would like to commend the executives and officials of the NCSA for their significant contributions to safeguarding national cybersecurity and for the tangible progress achieved in the prevention and suppression of cybercrime. **The Annual Report 2025** will enable all sectors to be apprised of the Agency's performance in advancing cybersecurity efforts, and will communicate to relevant stakeholders the outcomes achieved under various plans and measures, as well as developments concerning the national cybersecurity landscape. This reflects the collective commitment and shared responsibility of all parties in fostering a secure, resilient, and sustainable Thai society.

On this occasion, I would like to extend my best wishes to the executives and officials of the NCSA, as well as to all those who contribute to advancing the nation's cybersecurity mission. I sincerely wish you continued success, good health, and strength of spirit, so that you may carry out your duties with integrity and accomplish the objectives entrusted to you in service of the country.



(นายอนุทิน ชาญวีรกูล)
นายกรัฐมนตรี
Mr. Anutin Charnvirakul
Prime Minister

สารรองนายกรัฐมนตรี
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

MESSAGE FROM
THE DEPUTY PRIME MINISTER
Chairman of the National Cyber Security Committee (NCSC)

ภายใต้สถานการณ์ที่ภัยคุกคามไซเบอร์ซับซ้อน รวดเร็ว และส่งผลกระทบในวงกว้าง **คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)** จึงได้ขับเคลื่อนภารกิจด้านความมั่นคงปลอดภัยไซเบอร์มาอย่างต่อเนื่องและทวีความเข้มข้นขึ้น โดยอาศัยรากฐานเชิงนโยบายและมาตรฐานที่ได้วางไว้ตลอดหลายปี ทั้งการดำเนินงานตามแผนระดับชาติ การยกระดับมาตรฐานและมาตรการด้านไซเบอร์ในหลากหลายมิติ และการติดตามความพร้อมของหน่วยงานภาครัฐ หน่วยงานกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงอย่างต่อเนื่อง เพื่อลดผลกระทบที่จะเกิดขึ้นแก่พี่น้องประชาชนและความเสียหายของระบบเศรษฐกิจและความมั่นคงของประเทศ

ในปีงบประมาณ พ.ศ. 2568 กมช. ได้ดำเนินนโยบายที่มีความสำคัญเชิงยุทธศาสตร์ต่อประเทศ ทั้งการจัดทำกรอบแนวทางการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ เพื่อป้องกันการรั่วไหลของข้อมูลส่วนบุคคล อันเป็นปัญหาที่ส่งผลกระทบโดยตรงต่อความเชื่อมั่นของประชาชน การออกประกาศมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ เพื่อยกระดับความน่าเชื่อถือและความมั่นคงปลอดภัยของบริการภาครัฐบนโลกออนไลน์ รวมถึงการผลักดันให้เกิด**แนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย หรือ AI Security Guidelines** เพื่อเตรียมความพร้อมของประเทศต่อความท้าทายด้านเทคโนโลยีสมัยใหม่ ควบคู่กับการขยายความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์กับหน่วยงานพันธมิตรทั้งในประเทศและต่างประเทศอย่างต่อเนื่อง พร้อมทั้งติดตามการปฏิบัติตามกฎหมายด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานต่าง ๆ ในทุกระดับ เพื่อให้ประเทศมีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์และสอดคล้องกับมาตรฐานสากลมากยิ่งขึ้น

บนรากฐานสำคัญที่ได้วางไว้ ในปีต่อไป กมช. ให้ความสำคัญต่อการเร่งปรับกลยุทธ์จาก **“การป้องกัน”** (Prevention) ไปสู่ “การสร้างภูมิคุ้มกัน” (Cyber Immunity) ที่มั่นคงยั่งยืนและครอบคลุมทั้งระบบนิเวศไซเบอร์ของประเทศ โดยมีเป้าหมายสำคัญคือ การผลักดันให้ประชาชนมี **“ภูมิคุ้มกันตนเอง” (Self-Immunity)** สามารถรับรู้เข้าใจ และปฏิบัติตนได้อย่างมั่นคงปลอดภัยในโลกออนไลน์ท่ามกลางภัยไซเบอร์ที่เข้าใกล้ตัวมากยิ่งขึ้น

ในนามประธาน กมช. ผมขอชื่นชมและขอเป็นกำลังใจให้แก่ผู้บริหารและบุคลากร**สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)** ทุกท่านที่ทุ่มเทปฏิบัติภารกิจสำคัญนี้ เพื่อสร้างความมั่นคงปลอดภัยและสร้างความมั่นใจให้แก่พี่น้องประชาชน ให้เกิดขึ้นอย่างเป็นรูปธรรม และหวังเป็นอย่างยิ่งว่า **รายงานผลการดำเนินงานประจำปีงบประมาณ พ.ศ. 2568** ฉบับนี้ จะเป็นประโยชน์ต่อการดำเนินการของทุกภาคส่วน และร่วมกันขับเคลื่อนให้การดำเนินงานรักษาความมั่นคงปลอดภัยไซเบอร์ของชาติ เป็นกลไกสำคัญในการสร้างสังคมและประเทศที่มีความมั่นคงปลอดภัยไซเบอร์ในระดับสากลอย่างยั่งยืนตลอดไป

Amid increasingly complex, rapid, and wide-ranging cyber threats, **the National Cyber Security Committee (NCSC)** has continued to advance and intensify its cybersecurity mandate in a sustained and systematic manner. Building upon the strong policy foundations and standards established over the years, the NCSC has driven implementation in accordance with national plans, strengthened cybersecurity standards and measures across multiple dimensions, and closely monitored the preparedness of government agencies, regulators, and critical information infrastructure entities. These efforts are undertaken to mitigate potential impacts on the public and to safeguard the national economy and national security from potential harm.

In FY 2025, the NCSC implemented key national policies and strategies, including the development of a comprehensive cybersecurity framework for government agencies to prevent personal data breaches-an issue that directly affects public trust; the issuance of Website Security Standards to enhance the credibility and security of online public services; and the promotion of secure artificial intelligence practices through the introduction of **AI Security Guidelines**, aimed at strengthening national preparedness for the challenges posed by emerging technologies. At the same time, the NCSC expanded cybersecurity cooperation with domestic and international partners, while closely monitoring compliance with cybersecurity laws across agencies at all levels. These efforts are intended to enhance the country's overall cybersecurity readiness and to ensure greater alignment with international standards.

Building upon the strong foundations already established, in the coming year the NCSC will prioritize accelerating the strategic shift from **"Prevention"** to the development of robust and sustainable "Cyber Immunity" across the nation's entire cyber ecosystem. A key objective is to promote **"Self-Immunity"** among citizens, enabling them to recognize, understand, and navigate the online environment in a secure and responsible manner, amid cyber threats that are increasingly pervasive and closer to everyday life.

In my capacity as the Chairman of the NCSC, I wish to commend and extend my encouragement to the executives and officials of the NCSA for their dedication in carrying out this important mission to strengthen national cybersecurity and to build tangible public confidence. I sincerely hope that this **Annual Report 2025** will prove beneficial to all sectors in advancing their respective efforts and in collectively driving forward the nation's cybersecurity mission. Such efforts constitute a vital mechanism in fostering a secure and resilient society and in strengthening Thailand's cybersecurity standing at the international level on a sustainable basis.

(นายพิพัฒน์ รัชกิจประการ)
Mr. Phiphat Ratchakitprakarn
รองนายกรัฐมนตรี
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)
Deputy Prime Minister
Chairman of the National Cyber Security Committee (NCSC)

คำกล่าวของรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)
และประธานกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)

QUOTE FROM THE MINISTER OF DIGITAL ECONOMY AND SOCIETY

Chairman of the Cybersecurity Regulating Committee (CRC)
and Chairman of the Committee Managing the National Cyber Security Agency (CMSA)

“ **สกมช. มีบทบาทสำคัญในการเชื่อมโยงการทำงานระหว่างภาครัฐ ภาคเอกชน และประชาชน** เพื่อให้ประเทศไทยมีความพร้อมในการรับมือกับ**ภัยคุกคามทางไซเบอร์ที่ซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว** โดยเฉพาะในยุคที่**เทคโนโลยีปัญญาประดิษฐ์ (AI) ถูกนำมาใช้ทั้งในเชิงสร้างสรรค์และในลักษณะที่อาจก่อให้เกิดความเสี่ยง**

รัฐบาลให้ความสำคัญกับ**การยกระดับศักยภาพบุคลากรและโครงสร้างพื้นฐานด้านไซเบอร์** ควบคู่กับ**การส่งเสริมความร่วมมือกับพันธมิตรระหว่างประเทศ** เพื่อผลักดันประเทศไทยให้ก้าวสู่**มาตรฐานสากลด้านความมั่นคงปลอดภัยไซเบอร์**

นอกจากนี้ เพื่อให้ประชาชนสามารถใช้ชีวิตในโลกดิจิทัลได้อย่าง**มั่นใจและปลอดภัย** รัฐบาลจึงให้ความสำคัญกับ**การป้องกันและปราบปรามอาชญากรรมไซเบอร์ในทุกมิติ** ทั้งกลุ่ม**สแกมเมอร์ที่หลอกลวงประชาชน**และ**กลุ่มแฮกเกอร์ที่มุ่งโจมตีโครงสร้างพื้นฐานของประเทศ** ซึ่งถือเป็น**วาระแห่งชาติที่ต้องเร่งดำเนินการ**

ทั้งนี้ การดำเนินงานของ สกมช. ในปีงบประมาณหน้า จะมุ่งเน้น**การพัฒนาเชิงรุกด้านการเฝ้าระวัง การป้องกัน และการรับมือภัยไซเบอร์อย่างมีประสิทธิภาพ**

The National Cyber Security Agency (NCSA) plays a pivotal role in strengthening coordination across the public sector, the private sector, and society at large to ensure that Thailand remains well prepared to address increasingly complex and rapidly evolving cyber threats. This is particularly significant in an era where Artificial Intelligence (AI) is being deployed both as a driver of innovation and in ways that may present new risks.

The Government places high priority on enhancing human capability and reinforcing national cyber infrastructure, while deepening cooperation with international partners to advance Thailand's cybersecurity framework in line with internationally recognized standards.

Moreover, to ensure that people can participate in the digital economy with confidence and security, the Government remains firmly committed to the comprehensive prevention and suppression of cybercrime in all its forms - from scam networks targeting the public to malicious actors seeking to compromise the nation's critical infrastructure. This has been designated as a national agenda requiring sustained and decisive action.

In the forthcoming fiscal year, the NCSA will intensify its proactive efforts, with a focus on strengthening capabilities in cyber monitoring, prevention, and effective incident response. ”

นายไชยชนก ชิดชอบ
รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ในฐานะประธานกรรมการบริหารสำนักงาน
คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)
เป็นประธานการประชุม กบส. ครั้งที่ 7/2568 (30 ตุลาคม 2568)

Mr. Chaichanok Chidchob
Minister of Digital Economy and Society,
Chairman of the Committee Managing
the National Cyber Security Agency (CMSA),
presided at the CMSA Meeting No. 7/2025
held on **30 October 2025.**

สารเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

กรรมการและเลขานุการ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)
คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)
และคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (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)

ตลอด**ปีงบประมาณ พ.ศ. 2568** ที่ผ่านมา **สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)** ได้ดำเนินภารกิจภายใต้แนวคิด **"Team Thailand for Cybersecurity"** ซึ่งเป็นคำมั่นสัญญาที่ สกมช. ได้ให้ไว้ในรายงานฉบับปีก่อน ซึ่งแนวคิดนี้ได้นำมาสู่การปฏิบัติจริงและกลายเป็นหัวใจสำคัญของการผสานพลังจากทุกภาคส่วนให้กับประเทศอย่างเป็นรูปธรรม

ในระดับโลก สถานการณ์ภัยคุกคามทวีความรุนแรงขึ้นอย่างต่อเนื่อง ตาม**ผลสำรวจความเสี่ยงของ World Economic Forum (WEF) พ.ศ. 2568** ชี้ให้เห็นว่าข้อมูลเท็จและการบิดเบือนข้อมูล (Misinformation and Disinformation) กลายเป็นความเสี่ยงอันดับหนึ่งของโลกในระยะสั้น ขณะที่ภัยคุกคามจากการจารกรรมและความขัดแย้งทางไซเบอร์ยังคงเป็นความเสี่ยงสำคัญทั้งในระยะสั้นและระยะยาวซึ่งล้วนส่งผลกระทบต่อประเทศไทย นอกเหนือจากอาชญากรรมออนไลน์ที่สร้างความเดือดร้อนแก่ประชาชน ซึ่งจำเป็นต้องอาศัย**ความร่วมมือแบบบูรณาการ** มิใช่การทำงานเฉพาะหน่วยงานใดหน่วยงานหนึ่ง

ด้วยเหตุนี้ **"Team Thailand"** จึงมิใช่เพียงแนวคิด แต่เป็น **"การลงมือทำ"** ตลอดปีที่ผ่านมา สกมช. ได้มุ่งเน้นการประสานความร่วมมือใน **"สงครามกับสแกมเมอร์"** อันเป็นวาระแห่งชาติ ผ่านการปฏิบัติการเชิงรุกในการจำกัดช่องทางหลอกลวง ปิดกั้นบัญชีและเพจต้องสงสัยจำนวนมาก รวมถึงการยกระดับ**การแบ่งปันข้อมูลภัยคุกคามผ่านระบบ MISP** ซึ่งมีการแลกเปลี่ยน Indicators of Compromise (IOCs) จำนวนมาก เพื่อให้ทุกหน่วยงานสามารถตรวจจับและรับมือภัยคุกคามได้อย่างทันท่วงที ขณะเดียวกัน สกมช. ยังได้เสริมความร่วมมือทั้งในและต่างประเทศผ่านการลงนามบันทึกข้อตกลงร่วมหลายฉบับ สร้างโครงข่ายพันธมิตรที่ช่วยยกระดับขีดความสามารถของประเทศในภาพรวม

ภายใต้บริบทภัยไซเบอร์ที่เปลี่ยนแปลงรวดเร็ว สกมช. ได้มุ่งสร้างรากฐานสำคัญสำหรับความมั่นคงดิจิทัลในอนาคต ผ่านการพัฒนามาตรฐาน แนวปฏิบัติ และกลไกกำกับดูแลที่จำเป็น โดยได้เผยแพร่ "แนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย (AI Security Guidelines)" ฉบับแรกของประเทศ พร้อมเดินหน้าเตรียมออกมาตรฐานใหม่ที่สำคัญ อาทิ **แนวทางความมั่นคงปลอดภัยของระบบอุตสาหกรรม (Operational Technology: OT) และมาตรฐานด้านความมั่นคงปลอดภัยของอุปกรณ์ IoT** ซึ่งจะเป็นรากฐานในปี พ.ศ. 2569

นอกจากนี้ สกมช. ยังได้จัดฝึกซ้อมรับมือภัยไซเบอร์ระดับชาติ **“Thailand’s National Cyber Exercise 2025 (NCX)”** เพื่อพัฒนาความพร้อมของหน่วยงานรัฐและภาคส่วนต่าง ๆ อย่างต่อเนื่อง พร้อมผลักดันศูนย์ความร่วมมืออาเซียน-ญี่ปุ่นเพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ **(ASEAN-Japan Cybersecurity Capacity Building Centre: AJCCBC)** ให้ก้าวสู่บทบาทศูนย์กลางพัฒนาศักยภาพไซเบอร์ของภูมิภาคอาเซียนอย่างเต็มรูปแบบ

ผลลัพธ์ของการทำงานร่วมกันของ **“Team Thailand”** ในปีที่ผ่านมา ได้สะท้อนอย่างชัดเจน ผ่านความก้าวหน้าเชิงประจักษ์ของประเทศ ตลอดจนการเสริมความเข้มแข็งภายในของ สกมช. เอง ซึ่งได้**คะแนนประเมินคุณธรรมและความโปร่งใส (ITA) สูงขึ้น** และมีผลการประเมินองค์การมหาชนอยู่ในระดับสูง แสดงให้เห็นถึงการบริหารจัดการองค์กรที่มีประสิทธิภาพ โปร่งใส และมีธรรมาภิบาล

ในนามของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ผมขอขอบคุณหน่วยงานกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภาครัฐ ภาคเอกชน ภาคประชาสังคม ตลอดจนบุคลากรของ สกมช. ทุกท่าน ที่ได้ร่วมกันขับเคลื่อนภารกิจนี้อย่างสุดกำลัง และในปี พ.ศ. 2569 สกมช. จะยังคงมุ่งมั่นที่จะยกระดับความพร้อมของประเทศในการสร้างพื้นที่ไซเบอร์ที่ **“ปลอดภัย มั่นคง และน่าเชื่อถือ (Safe, Secure, and Trusted Cyberspace for Thailand)”** เพื่อประโยชน์สูงสุดของประชาชนและประเทศชาติอย่างแท้จริง

Throughout **FY 2025, the National Cyber Security Agency (NCSA)** has carried out its mandate under the guiding concept of **“Team Thailand for Cybersecurity,”** a commitment articulated in the previous Annual Report. This concept has since been translated into concrete action and has become a central pillar in mobilizing and integrating the collective efforts of all sectors in a tangible and coordinated manner for the benefit of the nation.

At the global level, the threat landscape continues to intensify. According to the **World Economic Forum (WEF) Global Risks Report 2025**, misinformation and disinformation have emerged as the world’s most significant short-term risk. Meanwhile, cyber espionage and cyber conflict remain critical risks in both the short and long term. These developments inevitably have implications for Thailand, in addition to the growing impact of online crime on the public. It is therefore imperative to adopt an integrated and **collaborative approach**, rather than relying on the efforts of any single agency alone.

Accordingly, **“Team Thailand”** is not merely a concept, but a commitment translated into concrete action. Throughout the past year, the NCSA has prioritized coordinated efforts in the national **“War Against Scammers,”** undertaking proactive operations to restrict fraudulent channels and to suspend a significant number of suspicious accounts and pages. At the same time, the NCSA has strengthened the sharing of threat intelligence through the MISP platform, facilitating extensive exchanges of Indicators of Compromise (IOCs) to enable all relevant agencies to detect and respond to threats in a timely manner. Concurrently, the NCSA has continued to enhance cooperation both domestically and internationally, signing multiple Memoranda of Understanding and building a robust network of partners to elevate the nation’s overall cybersecurity capabilities.

Against the backdrop of a rapidly evolving cyber threat environment, the NCSA has focused on laying essential foundations for the nation’s future digital security. This has been pursued through the development of necessary standards, guidelines, and governance mechanisms. Notably, the NCSA issued the country’s first “AI Security Guidelines” to promote the secure use of artificial intelligence. In parallel, preparations are underway for the introduction of key new standards, including Cybersecurity Guidelines for **Operational Technology (OT)** Systems and Security Standards for IoT Devices, which will serve as foundational frameworks for 2026.

In addition, the NCSA conducted the national-level exercise, Thailand’s National Cyber Exercise 2025 (NCX), to continuously strengthen the preparedness of government agencies and relevant sectors. At the same time, the NCSA has advanced the development of the **ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC),** with the aim of elevating it into a fully-fledged regional hub for cybersecurity capacity development in ASEAN.

The outcomes of the collective efforts under “Team Thailand” over the past year have been clearly reflected in the country’s tangible progress, as well as in the strengthened institutional capacity of the NCSA itself. The NCSA achieved a higher score in the **Integrity and Transparency Assessment (ITA)** and received strong results in external organizational evaluations, demonstrating effective management, transparency, and governance.

On behalf of the NCSA, I wish to express my sincere appreciation to the regulators, critical information infrastructure entities, public sector, private sector, civil society, and all NCSA officials for their unwavering commitment in advancing this mission. In 2026, the NCSA will remain firmly dedicated to enhancing the nation’s readiness in fostering a **“Safe, Secure, and Trusted Cyberspace for Thailand,”** for the utmost benefit of the people and the country as a whole.

พลอากาศตรี (อมร ชมเชย)
Air Vice Marshal Amorn Chomchoey
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กรรมการและเลขานุการ
Secretary-General of the National Cyber Security Committee (NCSC)

มุมมองผู้บริหารต่ออนาคต สกมช.

EXECUTIVE PERSPECTIVES ON THE FUTURE OF THE NCSA

"ความร่วมมือกับต่างประเทศเป็นสิ่งที่จำเป็น เนื่องจากภัยคุกคามในอนาคตจะมีมากขึ้น ความรู้จากบทเรียนที่เกิดขึ้นจากต่างประเทศ จะเป็นประโยชน์ต่อการเตรียมพร้อมรับมือของประเทศไทย ในอนาคต สกมช. จึงต้องมีบทบาทในการกำกับดูแลผู้ให้บริการและองค์กรต่าง ๆ มากขึ้น

International cooperation remains indispensable, as cyber threats are expected to continue intensifying. Lessons learned from incidents abroad provide valuable insights that strengthen Thailand's preparedness for the future. Accordingly, the NCSA must play an increasingly pivotal role in overseeing service providers and relevant organizations to ensure a resilient and secure digital ecosystem."

นายปกรณ์ ธรรมโรจน์
Mr. Pakorn Tummaroad
Expert Committee on Legal Affairs

กรรมการผู้ทรงคุณวุฒิ ด้านกฎหมาย
คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์
Expert Committee on Legal Affairs, Committee Managing the National Cyber Security Agency

"ความท้าทายสำคัญคือความคาดหวังของคนจำนวนมาก ในอนาคตเราต้องการดูแลภาคเอกชนมากขึ้น สกมช. ได้สร้างความร่วมมือและประโยชน์ให้กับพันธมิตรในลักษณะ win win หากมีการบูรณาการ มีการเชื่อมต่อและประสานงานมากกว่านี้ จะเป็นประโยชน์มาก

One of the most pressing challenges is meeting the rising expectations of the public. Looking ahead, we must further strengthen engagement with the private sector. The NCSA has cultivated meaningful, mutually beneficial partnerships, and through deeper integration and closer coordination, these collaborative efforts will deliver even greater and more sustainable outcomes."

พลอากาศตรี อมร ชมเชย
Air Vice Marshal Amorn Chomchoey

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
Secretary-General of the National Cyber Security Committee

"ในโลกที่ภัยไซเบอร์ซับซ้อนและเปลี่ยนแปลงตลอดเวลา ความร่วมมือจากทุกภาคส่วน รัฐ เอกชน องค์กร สถาบันการศึกษา และประชาชน คือกุญแจสำคัญในการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ โดยมี สกมช. เป็นศูนย์กลางในการขับเคลื่อนและประสานพลัง เพื่อใช้ทรัพยากรของประเทศอย่างมีประสิทธิภาพสูงสุด สร้างเกราะป้องกันที่แข็งแกร่ง และวางรากฐานสู่อนาคตดิจิทัลที่ปลอดภัย

In a world of increasingly complex and rapidly evolving cyber threats, collaboration across government, the private sector, academia, and the public is indispensable. The NCSA serves as the central driving force in uniting and coordinating national capabilities, optimizing the use of resources, strengthening our defenses, and laying a strong foundation for a secure digital future."

พลตรี ธีรวุฒิ วิทยากรณ์
Major General Teerawut Wittayakorn

รองเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
Deputy Secretary-General of the National Cyber Security Committee

“การขับเคลื่อนของ สกมช. ไม่เพียงแต่เน้นให้ Regulator หน่วยงาน CII และหน่วยงานรัฐมีความแข็งแกร่งด้านโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แต่ยังต้องขับเคลื่อนและสร้างความเข้มแข็งให้กับ Ecosystem ใน Cybersecurity Landscape ประเทศไทยด้วย และ Ecosystem สำคัญที่ สกมช. ต้องดำเนินการขับเคลื่อนไปพร้อม ๆ กัน คือ ผู้ประกอบการ เพื่อให้เกิดการวิจัยและพัฒนาผลิตภัณฑ์ เทคโนโลยี และการบริการ ความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะอย่างยิ่งผู้ประกอบการไทย จำเป็นต้องได้รับการส่งเสริมสนับสนุนให้มีศักยภาพที่สามารถแข่งขันได้กับต่างประเทศ เพื่อลดการขาดดุลของเศรษฐกิจดิจิทัลไทย ผ่านการจัดทำนโยบาย ยุทธศาสตร์และแผนไซเบอร์ที่ทันสมัย เพื่อให้ประเทศไทยมี Ecosystem ที่พร้อมรับมือภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในปัจจุบันและภัยคุกคามทางไซเบอร์รูปแบบใหม่ที่คาดว่าจะเกิดขึ้นในอนาคต

The NCSA's mission extends beyond strengthening regulators, CIIs, and government agencies. We must elevate Thailand's entire cybersecurity ecosystem. A vital component of this ecosystem is the private sector - spanning cybersecurity research and development, technology, innovation, and services. Thai enterprises must be empowered to compete internationally, thereby helping to reduce the digital trade deficit. With modern policies, forward-looking strategies, and adaptive cyber plans, Thailand can build a resilient ecosystem capable of addressing both current and emerging cyber threats.”

ผู้ช่วยศาสตราจารย์ ดร.วราภรณ์ พรหมวิกร
Assistant Professor Dr.Waraporn Promwikorn
ผู้ช่วยเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
Assistant Secretary-General of the National Cyber Security Committee

“เรายังขาดอำนาจบังคับใช้กฎหมาย หากมีการปรับแก้แล้ว จะช่วยให้การดำเนินงานดีขึ้นมาก การเป็นองค์การมหาชนช่วยให้จ่ายเงินเดือนสูงกว่าราชการได้ แต่บุคลากรต้องมีอุดมการณ์เพื่อประเทศชาติมากกว่าค่าตอบแทน

Our enforcement authority remains limited; strengthening it would significantly enhance the effectiveness of our operations. As a public organization, we are able to offer competitive compensation compared with the civil service; however, our officials must ultimately be guided by commitment and a sense of duty to the nation, rather than by financial considerations alone.”

นางกิ่งนภา บางชวด
Mrs. Kingnapa Bangchuad
ผู้ช่วยเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
Assistant Secretary-General of the National Cyber Security Committee

“ตลอดหลายปีที่ผ่านมา สกมช. มีข้อจำกัดอย่างมากในเรื่องบุคลากรและงบประมาณ อย่างไรก็ตาม เราไม่ได้ย่อท้อ หรือใช้เป็นข้ออ้างในการทำงานไม่สำเร็จ กลับเป็นแรงผลักดันให้เราทำงานหนักมากขึ้น โดยเฉพาะการสร้างความร่วมมือกับหน่วยงานทั้งภาครัฐและเอกชน เพื่อผลักดันงานสำคัญในการสร้างการเปลี่ยนแปลงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ ซึ่งจะส่งผลดีต่อเศรษฐกิจ สังคม ความมั่นคง และประชาชน อย่างเป็นรูปธรรม

Over the past several years, the NCSA has faced considerable constraints in both manpower and budget. Nevertheless, these limitations have never been regarded as obstacles. Instead, they have strengthened our resolve to work more effectively, particularly by deepening collaboration with government and private-sector partners to advance critical national cybersecurity priorities. These sustained efforts have laid a firm foundation for meaningful and lasting transformation, delivering tangible benefits to Thailand's economy, society, national security, and the well-being of its people.”

พลอากาศตรี จเด็ด คูหะก้องกิจ
Air Vice Marshal Jadet Khuhakongkit
ผู้ช่วยเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
Assistant Secretary-General of the National Cyber Security Committee

สารบัญ CONTENT

1 ORGANIZATIONAL STRUCTURE OVERVIEW

เกี่ยวกับองค์กร

ประวัติความเป็นมา
HISTORY

สกมช. เกิดขึ้นจากความจำเป็นเร่งด่วนในการรับมือภัยคุกคามไซเบอร์ที่รุนแรงขึ้นและส่งผลต่อความมั่นคงของชาติ เหตุการณ์ทั้งในประเทศและต่างประเทศสะท้อนให้เห็นว่ารัฐต้องมีหน่วยงานกลางด้านความมั่นคงไซเบอร์อย่างเป็นระบบ จึงนำไปสู่การตราพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อสร้างกลไกด้านการป้องกัน รับมือ และประสานงานระดับชาติ

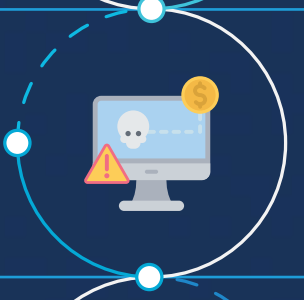
The establishment of the **National Cyber Security Agency (NCSA)** arose from the urgent need to address increasingly severe cyber threats that have had direct impacts on national security. Cyber incidents, both domestic and international, highlighted the necessity for a centralized national authority responsible for cybersecurity in a systematic manner. This led to the enactment of the **Cybersecurity Act, B.E. 2562 (2019)**, which aimed to create a national mechanism for prevention, response, and coordination.

บทเรียนสำคัญจากภัยคุกคามทางไซเบอร์
Key Lessons from Cyber Threats

เหตุโจมตีเอสโตเนีย (2550) : **การโจมตีด้วย DDos** ครั้งใหญ่ ทำให้ระบบคอมพิวเตอร์ของประเทศและบริการทางการเงินหยุดชะงัก ไม่สามารถให้บริการได้หลายสัปดาห์

Estonia Cyber Attacks (2007)
Large-scale **DDoS attacks** targeted Estonia, rendering nationwide computer systems and financial services unavailable. Essential services were disrupted for several weeks, demonstrating the significant impact of cyberattacks on national infrastructure.

กรณี WannaCry (2560) : **มัลแวร์แบบ Ransomware** เข้ารหัสข้อมูลและเรียกค่าไถ่ โดยใช้**ช่องโหว่ EternalBlue** บน Windows โจมตี 150 ประเทศ เน้นย้ำความสำคัญของการอัปเดตระบบและการสำรองข้อมูล

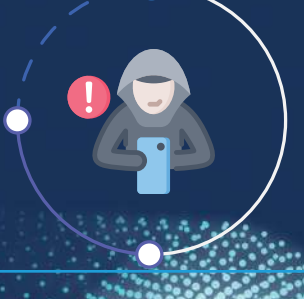


WannaCry Incident (2017)
The **WannaCry ransomware** exploited the **EternalBlue vulnerability** in Microsoft Windows systems, encrypting data and demanding ransom payments. The attack affected more than **150 countries**, underscoring the critical importance of timely system patching and data backup.

Stuxnet 2553 : มัลแวร์แบบ WORM ที่ใช้**ช่องโหว่ Zero-Day** เจาะระบบ **SCADA/PLC** เชื่อกันว่าเป็นต้นเหตุที่สร้างความเสียหายให้กับโครงการนิวเคลียร์ของอิหร่าน และถูกมองว่าเป็น**อาวุธดิจิทัล**ตัวแรกของโลก

Stuxnet (2010)
Stuxnet was a worm-type malware that exploited **zero-day vulnerabilities** to infiltrate **SCADA/PLC systems**. It is widely believed to have caused damage to Iran's nuclear facilities and is regarded as the world's first known **digital weapon**.

ประเทศไทย : เหตุการณ์โจมตีระบบการให้บริการที่สำคัญต่าง ๆ ภายในประเทศไทย ส่งผลให้เกิดการรั่วไหลของข้อมูลส่วนบุคคล และเป็นต้นตอของอาชญากรรมทางไซเบอร์ การหลอกลวงผ่านสื่อสังคมออนไลน์



Thailand
Cyberattacks on critical service systems in Thailand have led to personal data breaches and served as the starting point for various forms of cybercrime, including online fraud on social media platforms.

การยกระดับความมั่นคงปลอดภัยไซเบอร์
CYBERSECURITY ADVANCEMENTS

ปี 2562 2019

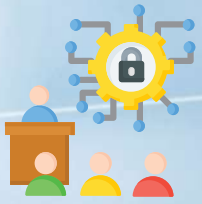
- ตรากฎหมายพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
  Enactment of the Cybersecurity Act B.E. 2562 (2019)

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 และหน่วยงาน 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 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 ครร. และการฝึกซ้อมเตรียมรับมือภัยคุกคามทางไซเบอร์ระดับประเทศในระดับร้ายแรงและวิกฤต
  Establishment of the CIRC and preparation for managing severe and critical national cyber threats

ปี 2567 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
- ยกระดับภัยคุกคามจากแอปดูดเงินเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง
  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
- การจัดตั้ง Sectoral CERT ครบทุก Sector
  Establishment of Sectoral CERTs across all sectors

ปี 2568 2025

- จัดตั้งศูนย์รวมผู้เชี่ยวชาญการวิจัยเพื่อความมั่นคงปลอดภัยไซเบอร์แห่งประเทศไทย (ศชวช.)
  Establishment of the national hub of cybersecurity research experts (Thailand Hub of Talents in Cybersecurity Research - HTCR)
- ออกประกาศเรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568 กำหนดมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์
  Issuance of the Website Security Standard, B.E. 2568 (2025) establishing minimum cybersecurity requirements for websites

ค่านิยมองค์กร

NCSA DNA

NATIONAL :
เป็นองค์กรระดับชาติมีหน้าที่ขับเคลื่อนและสร้างความมั่นคงปลอดภัยไซเบอร์ของประเทศ และเป็นศูนย์กลางความร่วมมือหน่วยงานภาครัฐและเอกชนทั้งภายในและต่างประเทศ

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.

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 CIIs to impress and exceed expectations.

STRONG/SYNERGY :
ต้องเข้มแข็งด้วยความสามัคคีผนึกกำลังในการปฏิบัติหน้าที่

Showing strength and synergy to fulfill responsibilities.

AGILITY :
ต้องมีความคล่องตัวพร้อมรับมือทุกความเปลี่ยนแปลงและทุกความท้าทาย

Operating with agility, adapting to changes and challenges.

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
Mr. Prasert Jantararuangtong
Deputy Prime Minister

กรรมการโดยตำแหน่ง
Committees by Position

พลเอก ณัฐพล นาคพาณิชย์
รัฐมนตรีว่าการกระทรวงกลาโหม
General Nattapon Nakpanich
Minister of Defence

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

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

พลตำรวจเอก กิตติ์รัฐ พันธุ์เพ็ชร์
ผู้บัญชาการตำรวจแห่งชาติ
Police General Kittirat Phanphet
Commissioner General,
Royal Thai Police

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

นายฉัตรชัย บางชวด
เลขาธิการสภาความมั่นคงแห่งชาติ
Mr. Chatchai Bangchuad
Secretary-General,
National Security Council

กรรมการและเลขานุการ
Committee member and Secretary

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

คณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

NATIONAL CYBER SECURITY COMMITTEE (NCSC)

กรรมการผู้ทรงคุณวุฒิ
Honorary Committees

ดร.ปริญญา หอมเอนก
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
Dr.Prinya Hom-anek
Expert Committee on Cyber Security

ดร.ไพบูลย์ อมรภิญโญเกียรติ
ด้านกฎหมาย
Dr.Paiboon Aamonpinyokeat
Expert Committee on Legal Affairs

พลเอก มโน นุชเกษม
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
General Mano Nuchkasem
Expert Committee on Information Technology and Communications

นายวิเชฐ ตันติวานิช
ด้านการเงิน
Mr. Vichate Tantiwanich
Expert Committee on Finance

พันตำรวจเอก ญาณพล ยั่งยืน
ด้านวิศวกรรมศาสตร์
Police Colonel Yanpol Yungyuen
Expert Committee on Engineering

นายแพทย์บดินทร์ ทรัพย์สมบูรณ์
ด้านสาธารณสุข
Dr.Bordin Sapsomboon
Expert Committee on Public Health

รองศาสตราจารย์ ดร.ปณิธาน วัฒนายากร
ด้านความสัมพันธ์ระหว่างประเทศ
Associate Professor Dr.Panitan Wattanayagorn
Expert Committee on International Relations

ประธานกรรมการ
Chairman

นายประเสริฐ จันทรรวงทอง
รองนายกรัฐมนตรีและรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
Mr. Prasert Jantararuangtong
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

นายอรรษิษฐ์ สัมพันธรัตน์
ปลัดกระทรวงมหาดไทย
Mr. Unsit Sampuntharat
Permanent Secretary,
Ministry of Interior

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

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

ศาสตราจารย์พิเศษ
วิศิษฏ์ วิศิษฏ์สรอรรถ
ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
Adjunct Professor
Wisit Wisitsora-At
Permanent Secretary, Ministry
of Digital Economy and Society

พลตำรวจเอก กิตติ์รัฐ พันธุ์เพ็ชร์
ผู้บัญชาการตำรวจแห่งชาติ
Police General Kittirat Phanphet
Commissioner General,
Royal Thai Police

นายประเสริฐ สินสุขประเสริฐ
ปลัดกระทรวงพลังงาน
Mr. Prasert Sinsukprasert
Permanent Secretary,
Ministry of Energy

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

นายฉัตรชัย บางชวด
เลขาธิการสภาความมั่นคงแห่งชาติ
Mr. Chatchai Bangchuad
Secretary-General,
National Security Council

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

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

กรรมการผู้ทรงคุณวุฒิ
Honorary Committees

พลตำรวจโท มนเทียร พันธ์อิ่ม
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
Police Lieutenant General
Montien Pun-im
Expert Committee on Cyber Security

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

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

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

นายวิทัย รัตนากร
ผู้ว่าการธนาคารแห่งประเทศไทย
Mr. Vitai Ratanakorn
Governor of the Bank of Thailand

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

นายไตรรัตน์ วิริยะศิริกุล
รองเลขาธิการ รักษาการแทนเลขาธิการ
คณะกรรมการกิจการกระจายเสียง
กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
Mr. Trairat Viriyasirikul
Deputy Secretary General,
Acting Secretary General, The Office of the National Broadcasting and Telecommunications Commission of Thailand

กรรมการและเลขานุการ
Committee member and Secretary

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

ประธานกรรมการ
Chairman

นายประเสริฐ จันทรรวงทอง
รองนายกรัฐมนตรีและรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
Mr. Prasert Jantararuangtong
Deputy Prime Minister
& Minister of Digital Economy and Society

กรรมการโดยตำแหน่ง
Committees by Position

ศาสตราจารย์พิเศษ
วิศิษฏ์ วิศิษฏ์สรอรรถ
ปลัดกระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม
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

นางแพตริเซีย มงคลวนิช
อธิบดีกรมบัญชีกลาง
Mrs. Patricia Mongkhonvanit
Comptroller - General,
The Comptroller
General's Department

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

กรรมการและเลขานุการ
Committee member and Secretary

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

คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)

COMMITTEE MANAGING THE NATIONAL CYBER SECURITY AGENCY (CMSA)

กรรมการผู้ทรงคุณวุฒิ
Honorary Committees

ดร.ชัยชนะ มิตรพันธ์
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
Dr. Chaichana Mitrpant
Expert Committee on Cyber Security

รองศาสตราจารย์ ดร.จอมพงศ์ มงคลวนิช
ด้านสังคมศาสตร์
Assoc. Prof. Dr. Jomphong Mongkhonvanit
Expert Committee on Social Sciences

รองศาสตราจารย์ สุรศักดิ์ สงวนพงษ์
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
Assoc. Prof. Surasak Sanguanpong
Expert Committee on Information Technology and Communication

นายปกรณ์ ธรรมโรจน์
ด้านกฎหมาย
Mr. Pakorn Tummaroad
Expert Committee on Legal Affairs

นายสมหมาย ลักขณานุรักษ์
ด้านเศรษฐศาสตร์
Mr. Sommai Lakananurak
Expert Committee on Economics

ดร.ลดาวัลย์ กระแสร์ชล
ด้านบริหารธุรกิจ
Dr. Ladawan Krasaechol
Expert Committee on Organizational Administration

การเข้าร่วมประชุมของ กบส. ประจำปีงบประมาณ 2568

PARTICIPATION IN THE MEETINGS OF THE CMSA FOR FISCAL YEAR 2025

ครั้งที่ Meeting No.	ผู้เข้าร่วม Participants	ผู้ไม่เข้าร่วม Absentees	ร้อยละของผู้เข้าร่วม Participation Rate (%)
7/2567	12	0	100
1/2568	12	0	100
2/2568	12	0	100
3/2568	11	1	91.66
4/2568	11	1	91.66
5/2568	11	1	91.66
6/2568	10	1	90.90
ร้อยละของจำนวนการประชุมมีกรรมการเข้าประชุม ร้อยละ 80 ขึ้นไป Percentage of committee members' meeting attendance: At least 80 percent			**ร้อยละ 100 100 percent**

หมายเหตุ :
Notes:

1. ประกาศแต่งตั้งกรรมการผู้ทรงคุณวุฒิใน กบส. เมื่อวันที่ 24 กุมภาพันธ์ 2568
   The appointment of qualified CMSA committee members was announced on 24 February 2025.
2. กรอบการประเมินองค์การมหาชน กำหนดให้ ร้อยละ 90 ของการประชุม กบส. ในรอบ 1 ปี จะต้องมีองค์ประชุม ไม่น้อยกว่าร้อยละ 80 ขึ้นไป หรือคิดเป็น 10 คนขึ้นไป
   According to the Public Organization Act, committee members are required to attend at least 90 percent of CMSA meetings within one year. Attendance of not less than 80 percent or absence of no more than 10 percent is considered compliant.
3. การประชุมคณะกรรมการในรอบ 1 ปี ต้องมีการประชุมไม่น้อยกว่า 1 ครั้ง ที่ไม่มีฝ่ายบริหาร (เลขาธิการฯ) ร่วมประชุมด้วย
   In one year, the committee must hold at least one meeting, excluding meetings in which only the Secretariat (Secretary-General) is present.


NCS

คณะกรรมการและคณะอนุกรรมการ
COMMITTEES AND SUBCOMMITTEES APPOINTED

คณะกรรมการตรวจสอบภายใน

1. รองศาสตราจารย์ ดร.จอมพงศ์ มงคลวนิช	ประธานกรรมการ
2. รองศาสตราจารย์ ดร.เสาวณีย์ ไทยรุ่งโรจน์	กรรมการ
3. นางพิลาสลักษณ์ ยุคเกษมวงศ์	กรรมการ
4. นางสาววศินี ธรรมศิริ	กรรมการ
5. ผู้อำนวยการฝ่ายตรวจสอบภายใน	เลขานุการ

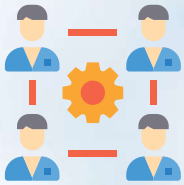
คณะอนุกรรมการด้านกฎหมาย (กกม.)

1. นายปกาศิต เหลืองทอง	ประธานอนุกรรมการ
2. พลตำรวจโท มนเทียร พันธ์อิ่ม	อนุกรรมการ
3. รองศาสตราจารย์ ดร.อติวงศ์ สุชาโต	อนุกรรมการ
4. ศาสตราจารย์ ดร.ยศชนัน วงศ์สวัสดิ์	อนุกรรมการ
5. นายภูรีพัชร์ แสงแก้ว	อนุกรรมการ
6. นายชาญชัย งามวิถี	อนุกรรมการ
7. พันเอก สุขธนา พงษ์มา	อนุกรรมการ
8. นางสาววิชชุกาญจน์ พัฒนพันธ์ชัย ผู้แทนสำนักงานคณะกรรมการกฤษฎีกา	อนุกรรมการ
9. นางสาวดรุณี พิกุลทอง ผู้อำนวยการสำนักกฎหมาย สกมช.	อนุกรรมการและเลขานุการ
10. นายอดิศร พิมลรัตน์ เจ้าหน้าที่กลุ่มวิชาชีพเฉพาะ ด้านกฎหมาย สกมช.	อนุกรรมการและผู้ช่วยเลขานุการ

คณะอนุกรรมการด้านกฎหมาย (กบส.)

1. นายปกรณ์ ธรรมโรจน์	ประธานอนุกรรมการ
2. นายรักไท เทพปัญญา ผู้แทนสำนักงานคณะกรรมการกฤษฎีกา	อนุกรรมการ
3. นายดามพ์ สุคนธทรัพย์	อนุกรรมการ
4. นายวรรณวิทย์ อาขุนุตร	อนุกรรมการ
5. นายสิโรตม์ รัตนามหัทธนะ	อนุกรรมการ
6. นางสาวดรุณี พิกุลทอง ผู้อำนวยการสำนักกฎหมาย สกมช.	อนุกรรมการและเลขานุการ
7. นายอดิศร พิมลรัตน์ เจ้าหน้าที่กลุ่มวิชาชีพเฉพาะ ด้านกฎหมาย สกมช.	อนุกรรมการและผู้ช่วยเลขานุการ

คณะอนุกรรมการด้านการบริหารงานบุคคล



1. นางลดาวัลย์ กระแสร์ชล	ประธานอนุกรรมการ
2. นางพัชรียา กุลานุช	อนุกรรมการ
3. นางสาวนภัส ศิริวรางกูร	อนุกรรมการ
4. ผู้แทนสำนักงาน ก.พ.ร.	อนุกรรมการ
5. นางมุทิตา เลิศลักษณาพร	อนุกรรมการ
6. พันตำรวจเอก ปัญญา สิงห์ไชย	อนุกรรมการและเลขานุการ
7. นายสุทธิวัฒน์ โตสมบุญ	อนุกรรมการและผู้ช่วยเลขานุการ

คณะอนุกรรมการด้านยุทธศาสตร์องค์กร

1. ศาสตราจารย์พิเศษวิศิษฏ์ วิศิษฏ์สรอรรถ	ประธานอนุกรรมการ
2. รองศาสตราจารย์สุรศักดิ์ สงวนพงษ์	อนุกรรมการ
3. นายชัยชนะ มิตรพันธ์	อนุกรรมการ
4. นายสมหมาย ลักขณานุรักษ์	อนุกรรมการ
5. พลอากาศตรี อมร ชมเชย เลขาธิการ กมช.	อนุกรรมการ
6. ผู้แทนกรมบัญชีกลาง	อนุกรรมการ
7. ผู้แทนสำนักงบประมาณ	อนุกรรมการ
8. พนักงานที่เลขาธิการ กมช. มอบหมาย	อนุกรรมการและเลขานุการ
9. พนักงานที่เลขาธิการ กมช. มอบหมาย	อนุกรรมการและผู้ช่วยเลขานุการ
10. พนักงานที่เลขาธิการ กมช. มอบหมาย	อนุกรรมการและผู้ช่วยเลขานุการ

คณะอนุกรรมการประเมินผลการปฏิบัติงานของเลขาธิการ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

1. ศาสตราจารย์พิเศษวิศิษฏ์ วิศิษฏ์สรอรรถ	ประธานอนุกรรมการ
2. นางสาวจิตตา กิตติเสถียรนนท์	อนุกรรมการ
3. นายชัยชนะ มิตรพันธ์	อนุกรรมการ
4. ผู้ช่วยศาสตราจารย์ ดร.วราภรณ์ พรหมวิกร	เลขานุการ
5. พันโท ญาณินทร์ สุรพันธ์ไพโรจน์	ผู้ช่วยเลขานุการ 1
6. นายสุทธิวัฒน์ โตสมบุญ	ผู้ช่วยเลขานุการ 2

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

2 **นางกิ่งนภา บางชวด**
ผู้ช่วยเลขาธิการ 2
Mrs. Kingnapa Bangchuad
Assistant Secretary-General 2

3 **พลอากาศตรี จเด็ด คูหะก้องกิจ**
ผู้ช่วยเลขาธิการ 3
AVM Jadet Khuhakongkit
Assistant Secretary-General 3

4 **นาวาเอกหญิง ศิริเนตร รักษ์วงศ์**
ผู้ทรงคุณวุฒิพิเศษ 1
Capt. Sirinate Rugvong WRTN
Senior Advisor 2

5 **นายจิรศักดิ์ วิชัยกุล**
ผู้ทรงคุณวุฒิพิเศษ 2
Mr. Chirasak Vishaigool
Senior Advisor 2

ผู้อำนวยการสำนัก
NCSA DIRECTORS

1 **พันตำรวจเอก ปัญญา สิงห์ไชย**
ผู้อำนวยการสำนักบริหารกลาง
Pol. Col. Panya Singhachai
Director of Central Administration Office

2 **นายภาณุพงษ์ ธนูทอง**
รักษาการผู้อำนวยการ
สำนักเทคโนโลยีสารสนเทศ
Mr. Panupong Thanutong
Acting Director of Information Technology Office

3 **พลอากาศตรี เฉลิมชัย วงษ์เกตุ**
ผู้อำนวยการศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์
AVM Chalermchai Wonggate
Director of Cyber Security Research Center

4 **พลอากาศตรี ธวัชชัย มากพานิช**
ผู้อำนวยการสำนักนโยบายยุทธศาสตร์
การรักษาความมั่นคงปลอดภัยไซเบอร์
AVM Tawatchai Makphanit
Director of Cyber Security Policy
and Strategy Office

5 **พันโท ปณต แสงทับทิม**
ผู้อำนวยการสำนักการเงินและกลยุทธ์องค์กร
Lt. Col. Panot Saengthapthim
Director of Finance and Strategy Office

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

7 พันตำรวจโท นรินทร์ เพชรทอง
รักษาการผู้อำนวยการ
สำนักบริหารโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
Pol. Lt. Col. Narin Phetthong
Acting Director of Critical Information Infrastructure Management Office

8 พันตรี ปวิช บูรพาชลทิศน์
รักษาการผู้อำนวยการสำนักวิชาการ
ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
Maj. Pawich Burapachonlatid
Acting Director of National Cyber Security Academy Office

9 นางสาวสายชล แซ่ลี้
ผู้อำนวยการสำนักประสานงาน
และรักษาการผู้อำนวยการสำนักปฏิบัติการ
Ms. Saichon Saelee
Director of Coordination Office, Acting Director of Cyber Operation Office

ผู้เชี่ยวชาญพิเศษ
SPECAIL EXPERTS

1 **นางพัชญ์ชิชา ไกรแสงศรี**
ผู้เชี่ยวชาญพิเศษ สำนักบริหารกลาง
Mrs. Phatchicha Kraisangsri
Special Expert, Central Administration Office

2 **นางชไมพร พงศ์พยุหะ**
ผู้เชี่ยวชาญพิเศษ
สำนักนโยบายยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์
Mrs. Chamaiporn Pongpayuha
Special Expert, Cyber Security Policy and Strategy Office

3 **นางอสิดา สุขสว่าง**
ผู้เชี่ยวชาญพิเศษ รักษาการผู้อำนวยการ
ฝ่ายยุทธศาสตร์ความร่วมมือระหว่างประเทศ
สำนักนโยบายยุทธศาสตร์การรักษา
ความมั่นคงปลอดภัยไซเบอร์
Mrs. Asida Suksawang
Special Expert, Acting Director
of International Affairs Division,
Cyber Security Policy and Strategy Office

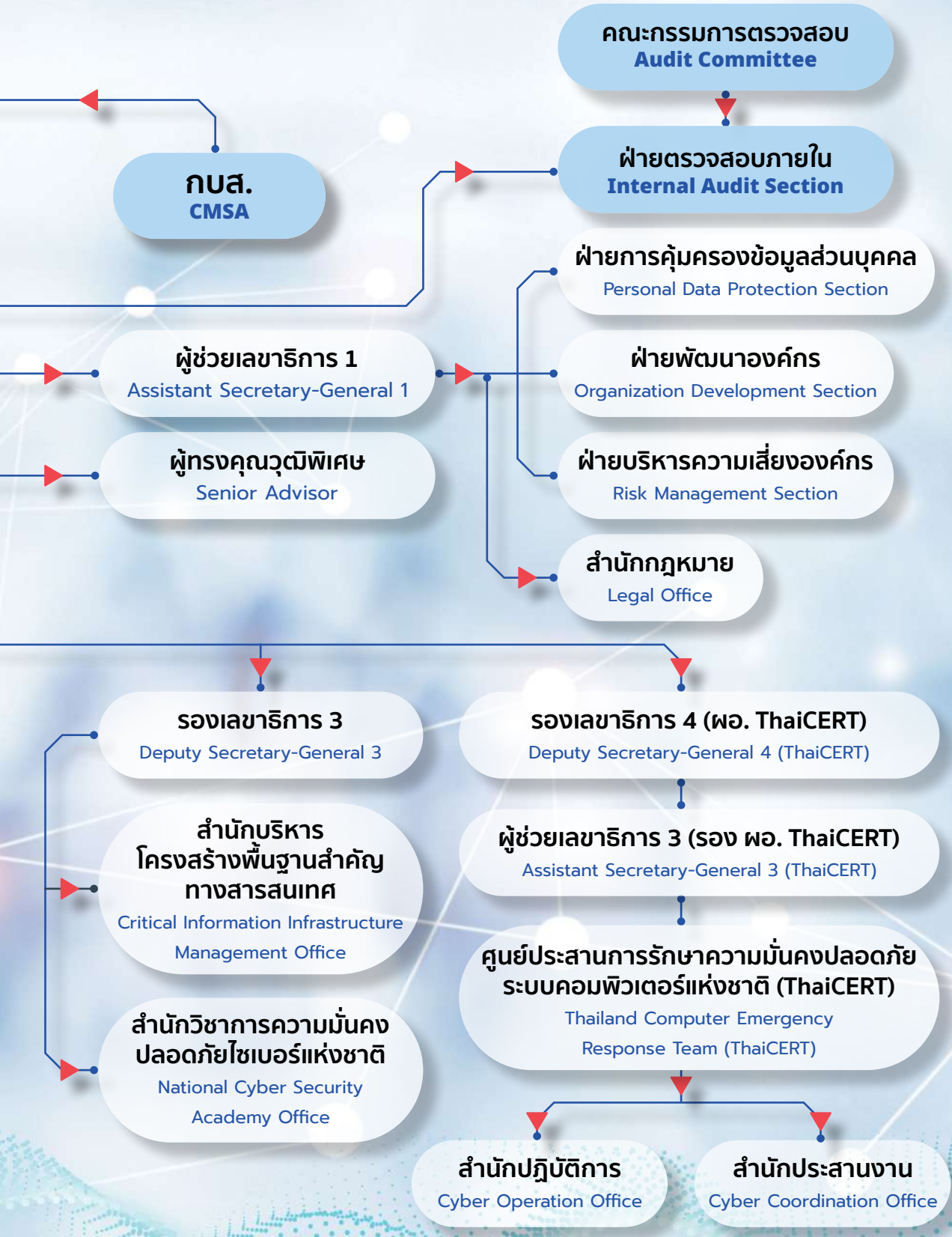
4 พันตำรวจโท นรินทร์ เพชรทอง
ผู้เชี่ยวชาญพิเศษ สำนักประสานงาน
Pol. Lt. Col. Narin Phetthong
Special Expert, Coordination Office

5 นาวาอากาศเอก เนติภัทร ภัทรกุลชัย
ผู้เชี่ยวชาญพิเศษ สำนักประสานงาน
Grp. Capt. Netipat Pattarakulchai
Special Expert, Coordination Office

6 พันตรี ปวิช บูรพาชลทิศน์
ผู้เชี่ยวชาญพิเศษ
สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
Major Pawich Burapachontit
Special Expert, National Cyber Security Academy

7 นาวาโท ศักติพงษ์ สิบหมื่นเปี่ยม
ผู้เชี่ยวชาญพิเศษ สำนักปฏิบัติการ
Cdr. Saktipong Sibmuenpiam
Special Expert, Operations Office

โครงสร้างองค์กร
CHART OF ORGANIZATION


คณะกรรมการตรวจสอบ
Audit Committee
กบส.
CMSA
ฝ่ายตรวจสอบภายใน
Internal Audit Section
ฝ่ายการคุ้มครองข้อมูลส่วนบุคคล
Personal Data Protection Section
ผู้ช่วยเลขาธิการ 1
Assistant Secretary-General 1
ฝ่ายพัฒนาองค์กร
Organization Development Section
ผู้ทรงคุณวุฒิพิเศษ
Senior Advisor
ฝ่ายบริหารความเสี่ยงองค์กร
Risk Management Section
สำนักกฎหมาย
Legal Office
รองเลขาธิการ 3
Deputy Secretary-General 3
รองเลขาธิการ 4 (ผอ. ThaiCERT)
Deputy Secretary-General 4 (ThaiCERT)
สำนักบริหารโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
Critical Information Infrastructure Management Office
ผู้ช่วยเลขาธิการ 3 (รอง ผอ. ThaiCERT)
Assistant Secretary-General 3 (ThaiCERT)
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT)
Thailand Computer Emergency Response Team (ThaiCERT)
สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
National Cyber Security Academy Office
สำนักปฏิบัติการ
Cyber Operation Office
สำนักประสานงาน
Cyber Coordination Office

2 TEAM THAILAND FOR CYBERSECURITY

ผลการดำเนินงาน

วิสัยทัศน์และพันธกิจ
VISION AND MISSION

วิสัยทัศน์ VISION

เป็นผู้นำในการขับเคลื่อนในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศที่มีประสิทธิภาพ พร้อมตอบสนองต่อภัยคุกคามไซเบอร์ทุกมิติ

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

พันธกิจ MISSION

1. เสนอแนะและขับเคลื่อนนโยบายแผนยุทธศาสตร์และปรับปรุงกฎหมาย ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งศึกษาวิจัยกำหนดแนวทาง มาตรฐาน มาตรการที่เกี่ยวข้องให้สอดคล้องกับสถานการณ์ทั้งในปัจจุบันและอนาคต
   Recommend and implement strategic policies and plans to improve cybersecurity and laws, and conduct research to establish standard guidelines and relevant measures aligned with current and future conditions.

2. กำกับ ดูแล เฝ้าระวัง ติดตาม วิเคราะห์ ประมวลผล แจ้งเตือน และปฏิบัติการเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์
   Regulate, monitor, analyze, process, and notify, while conducting operations to prevent, respond to, and mitigate risks arising from cyber threats.

3. เป็นศูนย์กลางในการประสานความร่วมมือ รวมทั้งส่งเสริม 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. เผยแพร่ความรู้ ความเข้าใจ และสนับสนุนการพัฒนาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
   Disseminate knowledge, foster understanding, and support the development of cybersecurity personnel.

ทีมประเทศไทยเพื่อความมั่นคงปลอดภัยไซเบอร์
TEAM THAILAND FOR CYBERSECURITY

ในโลกดิจิทัลที่ภัยคุกคามไซเบอร์ทวีความซับซ้อนและข้ามพรมแดน การสร้างความมั่นคงปลอดภัยไซเบอร์ไม่อาจสำเร็จได้ด้วยการดำเนินงานของหน่วยงานใดหน่วยงานหนึ่งเพียงลำพัง หากแต่ต้องเกิดจากการผนึกกำลังร่วมกัน เป็น **“Team Thailand”** ที่หลอมรวมพลัง ความเชี่ยวชาญ และทรัพยากรของทุกภาคส่วน ให้ประเทศไทยสามารถป้องกัน รับมือ และฟื้นตัวจากภัยคุกคามไซเบอร์ได้อย่างรวดเร็ว

In a digital era where cyber threats are increasingly complex and transboundary, strengthening cybersecurity cannot be achieved by any single agency alone. It requires collaboration across all sectors, known as **“Team Thailand,”** which brings together collective strength, expertise, and resources from every sector to enable Thailand to **prevent, respond to, and recover from cyber threats swiftly and effectively.**

TEAM THAILAND FOR CYBERSECURITY

เป้าหมาย
Objectives

ยกระดับความปลอดภัยไซเบอร์ของชาติ
Enhance national cybersecurity.

ลดความเสี่ยงข้อมูลรั่วไหล & การโจมตี
Reduce the risks of data breaches and cyberattacks.

เสริมสร้างระบบนิเวศความปลอดภัยไซเบอร์
Strengthen the cybersecurity ecosystem.

มุ่งรับมือภัยไซเบอร์ทุกรูปแบบ
Comprehensive Response to All Forms of Cyber Threats

ทุกฝ่ายประสานความร่วมมือเพื่อรับมือภัยไซเบอร์ที่ซับซ้อนและรุนแรง เช่น การโจมตีทางเทคนิค ข้อมูลรั่วไหล และข้อมูลเท็จ

All stakeholders collaborate to respond to **complex and severe cyber threats**, such as technical cyberattacks, data breaches, and misinformation and disinformation.

องค์ประกอบ
Key Stakeholders

ภาครัฐ
Public sector

ภาคเอกชน
Private sector

ภาคการศึกษา
Education sector

ผู้เชี่ยวชาญ
Experts

นักวิจัย
Researchers

ประชาชน
General public

ดำเนินผ่านกิจกรรม/โครงการต่าง ๆ เช่น
Implementation Through Activities / Programs Such As

กิจกรรมแข่งขัน
เฟ้นหาดาวรุ่ง
สร้างนักไซเบอร์มืออาชีพ
Cybersecurity competitions to identify rising stars and develop professional cybersecurity talent

กิจกรรมฝึกอบรม
และสร้างความตระหนักรู้
ให้คนไทยในทุกภาคส่วน
Training and awareness-building activities to enhance cybersecurity awareness among people in all sectors across Thailand

กลยุทธ์ 5 ด้าน ขับเคลื่อนแนวคิด “TEAM THAILAND FOR CYBERSECURITY”

Five Strategic Pillars Driving the “TEAM THAILAND FOR CYBERSECURITY”

ในปีงบประมาณ พ.ศ. 2568 นี้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เดินหน้าขับเคลื่อนภารกิจภายใต้แนวคิด **“Team Thailand for Cybersecurity”** ผ่านกลยุทธ์ 5 ด้านหลัก

1

การขับเคลื่อนและบูรณาการหน่วยงานที่เกี่ยวข้อง
ให้สอดคล้องกับนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565-2570

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

2

การเสริมสร้างและพัฒนาขีดความสามารถของบุคลากร องค์ความรู้ และเทคโนโลยี สอดคล้องต่อยุทธศาสตร์ที่ 1 สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Capacity)

Capacity Building
Enhancing and developing the capacities of personnel knowledge, and technology in alignment with Strategy 1: Building the Nation’s Cybersecurity Capabilities (Workforce, Knowledge, and Technology).

3

การเสริมสร้างความร่วมมือระหว่างหน่วยงาน
สร้างเครือข่ายความร่วมมือระหว่างหน่วยงานภาครัฐ ภาคเอกชน และองค์กรระหว่างประเทศ เพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์ สอดคล้องต่อยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)

Partnership Development
Strengthening collaboration and networks among government agencies, private sectors, and international organizations to enhance cyber preparedness, in alignment with Strategy 2: Fostwering Partnerships for Cyber Incident Response and Resilience.

In Fiscal Year 2025, the NCSA continued to advance its mandate under the **"Team Thailand for Cybersecurity"** approach through 5 core strategic pillars.

4

การส่งเสริมความพร้อมในการฟื้นคืน
ระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศและระบบบริการภาครัฐ ให้กลับสู่สภาพปกติได้อย่างรวดเร็ว ปลอดภัย และทันเวลา สอดคล้องต่อยุทธศาสตร์ที่ 3 สร้างบริการภาครัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Resilience)

Resilience Enhancement
Promoting preparedness to ensure the rapid, secure, and timely recovery of critical information infrastructure and government service systems to normal operations, in alignment with Strategy 3: Strengthening the Cybersecurity and Resilience of Government Services and Critical Information Infrastructure (Resilience).

5

การสร้างศักยภาพของหน่วยงานระดับชาติและหน่วยงานระดับภาคส่วน (Sector) ให้มีคุณภาพและมาตรฐาน สอดคล้องต่อยุทธศาสตร์ที่ 4 สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน (Standard)

Standardization and Quality Improvement
Enhancing the capabilities of national and sectoral agencies to meet quality and international standards, in alignment with Strategy 4: Enhancing the Capacity and Standards of National Agencies.

ภาพรวมสถานการณ์ภัยคุกคามไซเบอร์ปี 2568
OVERVIEW OF CYBER THREAT LANDSCAPE IN 2025

ประเทศไทยอยู่ในช่วงของการ **“เปลี่ยนผ่านดิจิทัล”** อย่างเต็มรูปแบบ โดยเร่งนำระบบคลาวด์ การทำงานทางไกล (Remote Work) และการใช้อินเทอร์เน็ตในทุกสิ่ง (Internet of Things:IoT) เข้ามาใช้ในภาครัฐและเอกชนอย่างกว้างขวาง การเปลี่ยนผ่านดังกล่าวช่วยขับเคลื่อนเศรษฐกิจดิจิทัลและเพิ่มประสิทธิภาพการดำเนินงานขององค์กร แต่ขณะเดียวกันก็ทำให้ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศขยายตัวมากขึ้น โดยในปี 2568 แนวโน้มการโจมตีไซเบอร์มีความซับซ้อนขึ้นอย่างมีนัยสำคัญเมื่อเทียบกับปีก่อนหน้า

Thailand is undergoing a full-scale digital transformation, with the accelerated adoption of cloud computing, remote work, and the Internet of Things (IoT) across both the public and private sectors. This transformation has driven the growth of the digital economy and enhanced organizational efficiency. However, it has also significantly expanded the nation’s cybersecurity risk landscape.

In Fiscal Year 2025, cyberattack trends became notably more complex compared to the previous year.

ภัยคุกคามไซเบอร์ ปี 2568
Cyber Threats in 2025

การโจมตีด้วยปัญญาประดิษฐ์และจิตวิทยาทางสังคม

อาชญากรไซเบอร์มีแนวโน้มใช้ **Generative AI** สร้าง **ข้อความ อีเมล เสียง และวิดีโอ** Deepfake ที่สมจริง ทำให้เหยื่อหลงเชื่อและถูกหลอกได้ง่ายขึ้น การโจมตีรูปแบบนี้จะถูกนำไปใช้ปลอมตัวเป็นผู้บริหารหรือบุคคลสำคัญ เพื่อหลอกให้เปิดเผยข้อมูลหรือโอนเงิน คาดว่าการใช้ AI เสริมพลังการโจมตีทางจิตวิทยาสังคม จะกลายเป็นเครื่องมือหลักของอาชญากรในอนาคต ดังนั้น จึงต้องเร่งพัฒนา**เครื่องมือตรวจจับเนื้อหาที่สร้างด้วย AI** และเพิ่มความตระหนักรู้ให้บุคลากรในการรับมือภัยคุกคามในรูปแบบนี้

AI-Driven and Social Engineering Attacks

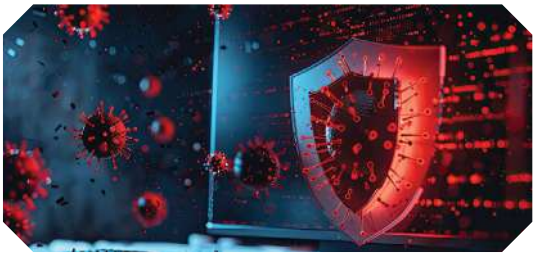
Cybercriminals are increasingly leveraging **generative AI** to produce highly realistic **text, emails, audio**, and deepfake videos, making victims more susceptible to deception. Such attacks are often used to impersonate senior executives or high-profile individuals in order to induce victims to disclose sensitive information or transfer funds. The use of AI to amplify social engineering attacks is expected to become a primary tool of cybercriminals in the future. Consequently, there is an urgent need to accelerate the development of **AI-generated content detection tools** and to enhance personnel awareness and preparedness to effectively address this emerging threat.

ความตึงเครียดทางภูมิรัฐศาสตร์

ทวีความรุนแรงและส่งผลโดยตรงต่อความมั่นคงปลอดภัยทางไซเบอร์ โดยผู้โจมตีที่ได้รับการสนับสนุนจากรัฐมุ่งบ่อนทำลาย**เศรษฐกิจ โครงสร้างพื้นฐานสำคัญ** และ**เสถียรภาพ**ของประเทศคู่แข่ง ผ่านการโจมตีระบบสารสนเทศ การขโมยข้อมูลลับ และการปั่นข้อมูลเท็จให้สังคมแตกแยก ส่งผลให้ประเทศต่าง ๆ ต้องเร่ง**ปรับยุทธศาสตร์ความมั่นคงไซเบอร์**ให้ทันกับพฤติกรรมของรัฐมหาอำนาจในยุคใหม่ รวมถึงการโจมตีทางไซเบอร์ที่ไม่สามารถหาแหล่งที่มาของการโจมตีอย่างเห็นได้ชัด

Geopolitical Tensions

Escalating geopolitical tensions have intensified and directly impacted cybersecurity. State-sponsored threat actors increasingly seek to undermine the **economies, critical infrastructure**, and **national stability** of rival countries through cyberattacks on information systems, the theft of sensitive data, and the dissemination of disinformation to sow societal division. As a result, countries are compelled to rapidly adapt their **cybersecurity strategies** to keep pace with the evolving behavior of major powers in the modern era, including cyber oerations where the source of an attack cannot be clearly or conclusively attributed.



มัลแวร์ยังเป็นภัยคุกคามหลักในอนาคต

มัลแวร์มีแนวโน้มพัฒนาให้ซับซ้อนและตรวจจับได้ยากขึ้น โดยเฉพาะ Ransomware และ Trojan ที่แฝงมากับอีเมลหรือไฟล์ออนไลน์ มุ่งขโมยข้อมูลหรือเรียกค่าไถ่แนบเนียนกว่าเดิม องค์กรจึงต้องเสริม**การป้องกัน การตรวจจับ และการตอบสนองให้รวดเร็วและมีประสิทธิภาพมากขึ้น**

Malware Remains a Primary Threat

Malware is expected to remain a major cybersecurity threat in the future, with increasing sophistication and greater difficulty of detection. In particular, ransomware and trojans embedded in emails or online files are becoming more covert, targeting data theft and extortion with greater subtlety. Organizations must therefore strengthen their **prevention, detection, and response capabilities to ensure faster and more effective cybersecurity incident management.**

การโจมตีผ่านช่องโหว่ซอฟต์แวร์ล้าสมัย

ในปี 2568 ผู้ไม่หวังดีมุ่งโจมตีช่องโหว่ของซอฟต์แวร์ที่ไม่ได้อัปเดตหรือถูกละเลยมากขึ้น โดยเฉพาะระบบเวอร์ชันเก่าที่ขาดกระบวนการอัปเดตซอฟต์แวร์และ**ระบบปฏิบัติการความปลอดภัย (Patch Management)** ทำให้องค์กรตกเป็นเป้าได้ง่าย จึงจำเป็นต้องมีการตรวจสอบช่องโหว่อย่างสม่ำเสมอ

Attacks Exploiting Outdated Software Vulnerabilities

In 2025, malicious actors increasingly targeted vulnerabilities in outdated or neglected software, particularly legacy systems lacking effective software and **operating system patch management**. This has made organizations more susceptible to cyberattacks, underscoring the need for regular vulnerability assessments and timely patching.

ข้อมูลยืนยันตัวตนรั่วไหล
Credential Leaks

การรั่วไหลของข้อมูลยืนยันตัวตน หรือ **"Credential Leaks"** เช่น ชื่อผู้ใช้งาน รหัสผ่าน และรหัสข้อมูลดิจิทัลในการเข้าถึงระบบ (Access Token) เป็นอีกภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบอย่างต่อเนื่อง แพร่หลาย และกลายเป็นช่องทางสำคัญที่ผู้ไม่หวังดีใช้เจาะระบบขององค์กรในปีที่ผ่านมา

ยิ่งในประเทศไทย ถือว่าประสบปัญหาการรั่วไหลของข้อมูลยืนยันตัวตนในวงกว้าง โดยตรวจพบข้อมูลรั่วไหลกว่า **200 ล้านบัญชี** ซึ่งส่งผลกระทบโดยตรงต่อหน่วยงานภาครัฐและเอกชน จากเหตุการณ์นี้ ได้มีการแจ้งเตือนไปยังหน่วยงานที่ได้รับผลกระทบรวม **5,875 หน่วยงาน**

The leakage of authentication credentials, or **"credential leaks,"** including usernames, passwords, and digital access tokens, remains a persistent and widespread cybersecurity threat. Such leaks have become a major attack vector exploited by malicious actors to compromise organizational systems over the past year.

In Thailand, credential leaks have occurred on a large scale, with more than **200 million compromised** accounts identified. This has had a direct impact on both public and private sector organizations. In response, alerts were issued to a total of **5,875 affected organizations.**

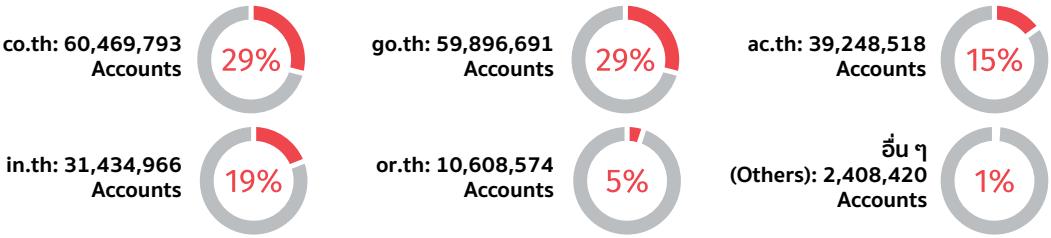
จำนวนไฟล์ข้อมูล Username และ Password รั่วไหลทั้งหมด 6,301 ไฟล์
Total Number of Leaked Username and Password Files: 6,301 Files

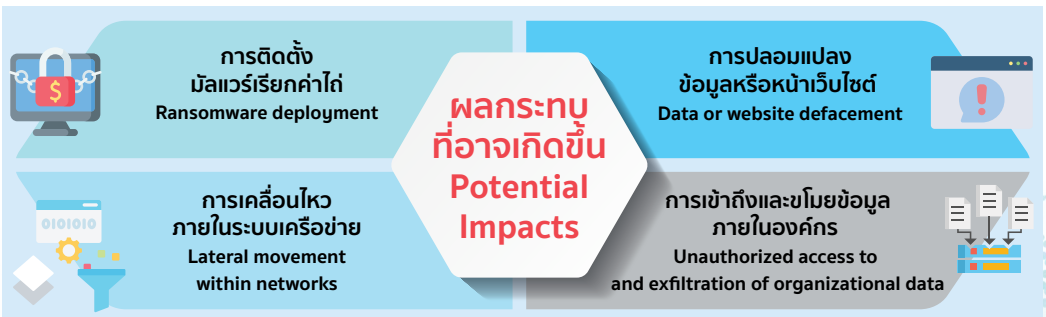
จำนวน Username และ Password ทั่วโลกทั้งหมด
Total leaked usernames and passwords worldwide:
43,436,415,464 Accounts

จำนวน Username และ Password ตามโดเมน .th ทั้งหมด
Total leaked usernames and passwords under the .th domain:
204,066,962 Accounts

ThaiCERT ได้ออกประกาศแจ้งเตือนต่อหน่วยงานที่ได้รับผลกระทบ
Organizations notified by ThaiCERT due to the impact:
5,875 หน่วยงาน

จำนวนไฟล์ข้อมูลรั่วไหล Username และ Password
Distribution of Leaked Username and Password Data





ที่มา : ThaiCERT
ข้อมูลเดือนตุลาคม 2567-30 กันยายน 2568
Source: ThaiCERT
Data period: October 2024-30 September 2025

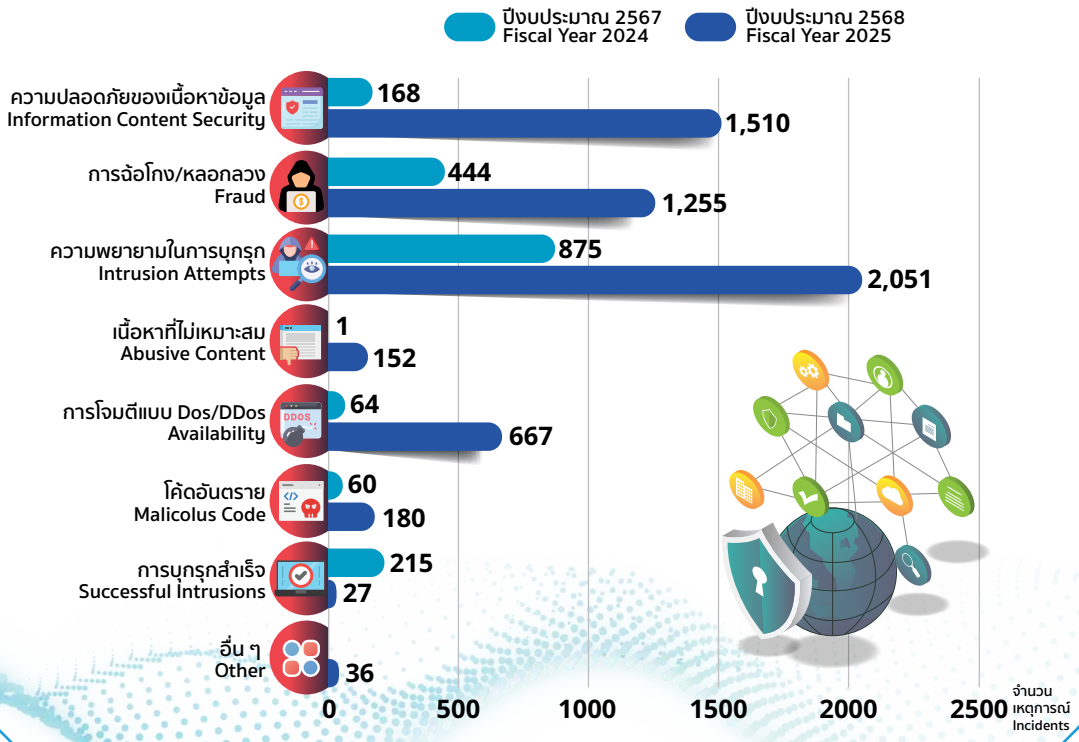
สถิติภัยคุกคามทางไซเบอร์
Cyber Threat Statistics

จากการติดตามและเฝ้าระวังภัยคุกคามทางไซเบอร์ในรอบปี 2568 พบว่าเหตุการณ์ภัยคุกคามมีแนวโน้มเพิ่มขึ้นอย่างชัดเจน ทั้งด้านความปลอดภัยของข้อมูล การฉ้อโกง และโดยเฉพาะความพยายามบุกรุกระบบที่สะท้อนว่าผู้ไม่ประสงค์ดีเพิ่มความพยายามในการเจาะระบบ แม้ยังไม่สามารถบุกรุกสำเร็จ แต่แสดงถึงการปรับใช้เทคนิคที่ซับซ้อนยิ่งขึ้น จึงควรให้ความสำคัญกับการป้องกันเชิงรุก การเฝ้าระวังอย่างต่อเนื่อง และการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ในทุกระดับ

Based on continuous monitoring and surveillance of cyber threats throughout fiscal year 2025, it was found that cyber threat incidents have shown a clear upward trend. This increase spans multiple dimensions, including data security risks, fraud, and particularly attempts to compromise systems.

These findings indicate that malicious actors are intensifying their efforts to breach systems. Although many attacks have not been fully successful, they demonstrate the adoption of increasingly sophisticated techniques. This underscores the importance of prioritizing proactive prevention measures, continuous monitoring, and the enhancement of cybersecurity awareness at all levels.

สถิติภัยคุกคามทางไซเบอร์ (เปรียบเทียบปี 2567-2568)
Cyber Threat Statistics (Comparison between 2024-2025)



รูปแบบภัยคุกคามทางไซเบอร์ที่พบมากที่สุด
Most Common Types of Cyber Threats

การโจมตีหน้าเว็บไซต์
เพื่อเข้าไปแก้ไขเนื้อหาเว็บเพจ ให้ปรากฏเป็นข้อความ รูปภาพ หรือประกาศที่ไม่ได้รับอนุญาต

Website Defacement Attacks
Attacks targeting websites with the intent to alter web page content to display unauthorized text, images, or announcements.

การรั่วไหลของข้อมูลยืนยันตัวตน
เหตุการณ์ที่ข้อมูลรับรองการเข้าสู่ระบบของผู้ใช้ เช่น ชื่อผู้ใช้ รหัสผ่าน และรหัสข้อมูลดิจิทัลในการเข้าถึงระบบถูกเปิดเผยหรือรั่วไหลสู่บุคคลที่ไม่ได้รับอนุญาต

Credential Leaks
Incidents in which user authentication credentials-such as usernames, passwords, and digital access tokens-are exposed or leaked to unauthorized parties.

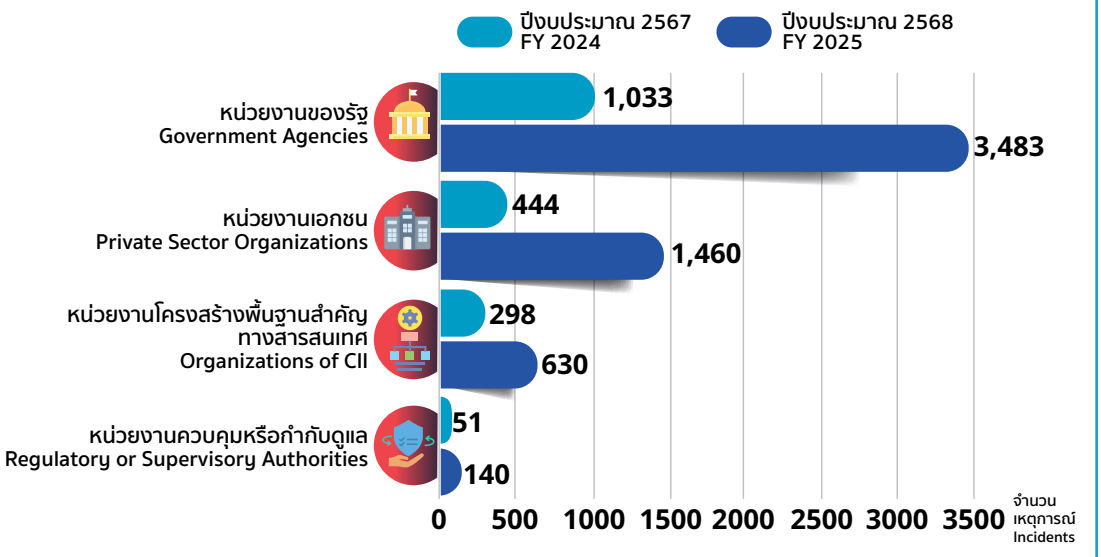
การโจมตีแบบ DDoS
โดยใช้คอมพิวเตอร์จำนวนมากส่งคำร้องขอปริมาณสูงเข้ามายังเว็บไซต์หรือระบบ จนระบบไม่สามารถรองรับได้ ทำให้เกิดการหยุดให้บริการ หรือทำงานช้าลง

Distributed Denial-of-Service (DDoS) Attacks
Attacks in which a large number of computers generate an overwhelming volume of requests to a website or system, exceeding its capacity and causing service disruption or performance degradation.

การละเมิดข้อมูลส่วนบุคคล
ข้อมูลที่เป็นความลับหรือข้อมูลสำคัญขององค์กรหรือบุคคล ถูกเข้าถึง เปิดเผย หรือถูกนำออกไปโดยไม่ได้รับอนุญาต ไม่ว่าจะจากการถูกโจมตีทางไซเบอร์ ความผิดพลาดของมนุษย์ หรือระบบที่มีช่องโหว่

Data Breach
Incidents in which confidential or sensitive information of organizations or individuals is accessed, disclosed, or exfiltrated without authorization, whether due to cyberattacks, human error, or system vulnerabilities.

สถิติภัยคุกคามทางไซเบอร์ที่พบกับหน่วยงาน (เปรียบเทียบปี 2567-2568)
Cyber Threat Statistics Affecting Organizations (Comparison between FY 2024-2025)



ข้อมูลการตรวจพบภัยคุกคามทางไซเบอร์ ชี้ให้เห็นว่ามีหน่วยงานที่ได้รับผลกระทบเพิ่มขึ้นเป็นจำนวนมาก ครอบคลุมทั้งหน่วยงานของรัฐ องค์กรภาคเอกชน หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานกำกับดูแล สถานการณ์ดังกล่าวสะท้อนว่าภัยคุกคามมีการขยายตัวและกระจายสู่ทุกภาคส่วน โดยเฉพาะหน่วยงานรัฐและเอกชนซึ่งเป็นเป้าหมายหลักของผู้ไม่ประสงค์ดี แนวโน้มนี้ตอกย้ำความจำเป็นเร่งด่วนในการดำเนินการ ดังนี้

Cyber threat detection data indicate a significant increase in the number of affected organizations, encompassing government agencies, private sector organizations, critical information infrastructure entities, and regulatory bodies. This situation reflects the expanding and increasingly widespread nature of cyber threats across all sectors, with public and private organizations in particular becoming primary targets of malicious actors. This trend underscores the urgent need to undertake the following actions:

เสริมสร้างมาตรการป้องกันและตรวจจับภัยคุกคามเชิงรุก
Strengthen proactive prevention and detection measures against cyber threats.

พัฒนาศักยภาพบุคลากร ด้านความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์
Enhance personnel capacity and cybersecurity awareness at all levels.

จัดทำแผนตอบสนองและรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพ เพื่อยกระดับความมั่นคงปลอดภัยไซเบอร์ของประเทศอย่างยั่งยืน
Develop effective incident response and cyber threat management plans to improve national cybersecurity resilience in a sustainable manner.

สกมช. กับบทบาทผู้นำทีมประเทศไทย
NCSA TEAM THAILAND CYBER LEADERSHIP

สกมช. ในฐานะหน่วยงานหลักด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ทำหน้าที่เป็น **“ผู้นำทีมประเทศไทย”** ในการขับเคลื่อนการป้องกันและรับมือภัยคุกคามทางไซเบอร์อย่างเป็นระบบ เชื่อมโยงความร่วมมือระหว่างภาครัฐ เอกชน และภาคประชาชน เพื่อเสริมสร้างขีดความสามารถของประเทศทั้งเชิงนโยบาย มาตรฐาน และการปฏิบัติการ พร้อมยกระดับบทบาทไทยบนเวทีความมั่นคงไซเบอร์ระดับภูมิภาคและนานาชาติอย่างเต็มภาคภูมิ

As the national authority for cybersecurity, the NCSA serves as the **“Team Thailand Cyber Leader”** in systematically driving the prevention of and response to cyber threats. The NCSA connects and coordinates collaboration among the public sector, private sector, and the public to strengthen national capabilities across policy, standards, and operational dimensions, while elevating Thailand’s role and standing in regional and international cybersecurity arenas with confidence and distinction.

ความร่วมมือกับ Sectoral CERT
Collaboration with Sectoral CERTs

ส่งเสริมและสนับสนุนการจัดตั้ง**ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT)** ในภาคส่วนต่าง ๆ

NCSA promotes and supports the establishment of **Sectoral Computer Emergency Response Teams (Sectoral CERTs)** across various sectors, serving as **coordinating centers for cybersecurity incident response** within **Critical Information Infrastructure (CII) organizations.**

เป้าหมายของการจัดตั้ง Sectoral CERT
Objectives of Establishing Sectoral CERTs

- เสริมขีดความสามารถในแต่ละภาคส่วนให้สามารถรับมือกับภัยไซเบอร์ได้รวดเร็วและมีประสิทธิภาพ
  Enhance sector-specific cybersecurity capabilities to enable **rapid and effective response** to cyber threats.
- สร้างกลไกความร่วมมือแบบ PPP ให้ภาครัฐและเอกชนแลกเปลี่ยนข้อมูลและแนวปฏิบัติร่วมกัน
  Establish Public-Private Partnership (PPP) mechanisms, enabling government agencies and private entities to **exchange threat information and share best practices.**
- ยกระดับการแบ่งปันข้อมูลภัยคุกคาม สร้างความปลอดภัยระดับประเทศที่เชื่อมโยงถึงกัน
  Strengthen national-level threat intelligence sharing, fostering an **interconnected and resilient cybersecurity ecosystem.**
- พัฒนาศักยภาพบุคลากรด้านไซเบอร์ในแต่ละภาคส่วนผ่านการอบรม การฝึกซ้อมจำลองสถานการณ์ และการพัฒนาองค์ความรู้
  Develop cybersecurity workforce capacity in each sector **through training programs, cyber exercises, scenario-based simulations, and continuous knowledge development.**

สนับสนุนการจัดตั้ง SECTORAL CERT
Support for the Establishment of Sectoral CERTs

CAAT

สำนักดิจิทัลกรุงเทพมหานคร
BMA Digital Office

ENERGY CERT

สพฐ.
Office of the Basic Education Commission (OBEC)

MOF CSIRT

TCM CERT

จัดตั้งไปแล้ว 15 แห่ง / 15 Sectoral CERTs established
อยู่ระหว่างการจัดตั้ง 10 แห่ง / 10 Sectoral CERTs currently under establishment

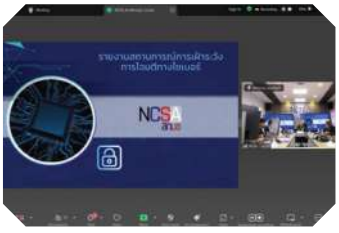
ประชุมประชาคมไซเบอร์ TH-CERT Community
Cybersecurity Community Meeting - TH-CERT Community

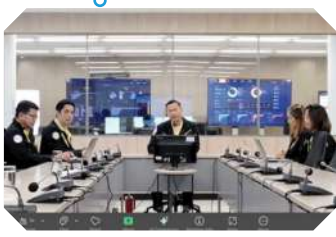
จัดกิจกรรม **“การประชุมประชาคมไซเบอร์ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ทุกภาคส่วน (TH-CERT Community)”** เพื่อแลกเปลี่ยนข้อมูลและประสบการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ติดตามสถานการณ์ภัยคุกคาม แบ่งปันข้อมูลเชิงลึกด้านภัยคุกคาม และนำเสนอแนวทางการรับมือภัยไซเบอร์ที่มีความซับซ้อนมากขึ้น การประชุมนี้ มุ่งเสริมสร้างความร่วมมือระหว่างทุกภาคส่วน ยกระดับความพร้อมของประเทศในการป้องกันและตอบสนองต่อเหตุการณ์อย่างมีประสิทธิภาพ และส่งเสริมการสร้างภูมิคุ้มกันทางดิจิทัลของประเทศไทยอย่างยั่งยืน

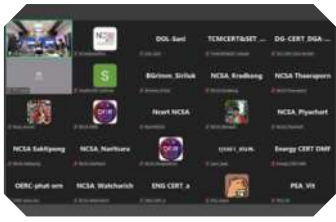
The **TH-CERT Community Meeting** was organized as a forum for the **Computer Security Incident Response Teams (CSIRTs)** to exchange information and share experiences related to cybersecurity operations. The meeting focused on **monitoring the cyber threat landscape, sharing threat intelligence,** and **discussing response approaches to cyber incidents** with increasing complexity.

The objective of the meeting was to **strengthen collaboration among all sectors,** enhance **national readiness in cyber incident prevention and response,** and promote **effective coordination.** This initiative also contributes to fostering **a resilient digital society** and ensuring **sustainable cybersecurity for Thailand.**

ร่วมมือกับ CERT ทุกภาคส่วน เฝ้าระวังภัยคุกคาม จากสถานการณ์ไม่ปกติ ในด้านข่าวกรองทางไซเบอร์
Collaboration with CERTs Across All Sectors to Monitor and Respond to Cyber Threats







จัดตั้งศูนย์ปฏิบัติการ**เฝ้าระวัง**และรับมือภัยคุกคามทางไซเบอร์ทุกวัน ตลอด **24 ชั่วโมง** ทำหน้าที่ติดตาม วิเคราะห์ แจ้งเตือน และตอบสนองต่อเหตุการณ์ฉุกเฉินอย่างทันท่วงที พร้อมสร้างเครือข่ายความร่วมมือกับหน่วยงานความมั่นคง ทั้งภาครัฐและเอกชน เพื่อแลกเปลี่ยนข้อมูลและแนวทางปฏิบัติร่วมกัน

Established a 24/7 Cyber Threat Monitoring and Response Operations Center responsible for continuously monitoring, analyzing, alerting, and responding to cyber incidents in a timely manner. The Center also builds collaborative networks with security agencies across both the public and private sectors to facilitate information sharing and the exchange of best practices.

เฝ้าระวังจากสถานการณ์ความความขัดแย้งทางภูมิรัฐศาสตร์ ระหว่างวันที่ 28 พฤษภาคม-9 กันยายน 2568 ได้ดำเนินการ**แจ้งเตือนภัย รวม 1,076 เหตุการณ์**

Cybersecurity Monitoring Amid Geopolitical Tensions **During the period from 28 May to 9 September 2025,** a total of **1,076 cybersecurity alerts** were issued.

แพลตฟอร์มรับและแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์
Cyber Threat Information Sharing Platform

พัฒนาแพลตฟอร์มรับและแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์ ผ่าน Malware Information Sharing Platform (MISP) ครอบคลุมหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยมี**หน่วยงานทั้งในและต่างประเทศเชื่อมต่อระบบ 223 หน่วยงาน**

ระบบเชื่อมต่ออัตโนมัติเพื่อแลกเปลี่ยนข้อมูลภัยคุกคามเชิงเทคนิค สนับสนุนการป้องกันภัยเชิงรุก (Proactive Protection) ทั้งยังออกแบบให้รองรับการขยายการเชื่อมต่อในอนาคต พร้อมกลไกคัดกรองและการสร้างความเชื่อมั่นในการแลกเปลี่ยนข้อมูล โดยใช้มาตรฐานสากล **"Traffic Light Protocol"** มาควบคุมการแลกเปลี่ยนข้อมูลระหว่างกัน

Developed a cyber threat information receiving and sharing platform through the Malware Information Sharing Platform (MISP), covering critical information infrastructure entities, with a total of **223 domestic and international organizations connected to the system.**

The **platform features automated** connectivity for the exchange of technical threat intelligence, supporting proactive protection measures. It is also designed to be scalable for future expansion, with built-in screening mechanisms and trust-building controls for information sharing, utilizing the international standard **Traffic Light Protocol (TLP)** to govern data exchange among participating organizations.

สกมช. ได้แชร์ indicator of compromise (IOCs)
รวมทั้งพัฒนาขีดความสามารถของบุคลากรอย่างต่อเนื่อง

- **255,110** เหตุการณ์
- **62,719,476** ประเภทของตัวบ่งชี้
- อบรมเชิงปฏิบัติการการใช้งานระบบ MISP
- อบรมหลักสูตรการวิเคราะห์ข่าวกรองภัยคุกคามทางไซเบอร์
- สัมมนาเชิงปฏิบัติการและกิจกรรมกลุ่มสัมพันธ์เชิงวิชาการด้านความมั่นคงปลอดภัยไซเบอร์

MISP Operational Outcomes

The NCSA has continuously expanded its **Indicators of Compromise (IOCs)** repository and enhanced national response capabilities, with the following results:

- **255,110 cyber incidents** recorded
- **62,719,476 IOCs** collected and shared
- **Capacity-building programs** on MISP system operations
- **Advanced cyber threat analysis training** programs
- **Support for operational exercises and academic network activities** in the field of cybersecurity

การยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐาน Global Cybersecurity Index (GCI)
Enhancing National Cybersecurity in Alignment with the Global Cybersecurity Index (GCI)

ยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยขับเคลื่อนผ่านกิจกรรมสำคัญ ได้แก่

Thailand's cybersecurity posture has been strengthened through key initiatives aimed at advancing national cybersecurity capabilities in line with the **GCI.** Key activities include:

จัดอบรมเพื่อเผยแพร่และขับเคลื่อนการยกระดับดัชนีความมั่นคงปลอดภัยไซเบอร์ (GCI) เสริมสร้างความเข้าใจแก่หน่วยงานภาครัฐ หน่วยงานกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญ หน่วยงานการศึกษา และภาคเอกชน บูรณาการกรอบ GCI สู่การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ พร้อมเชื่อมโยงยุทธศาสตร์ นโยบาย และแผนที่เกี่ยวข้อง เพื่อสะท้อนศักยภาพของประเทศอย่างเป็นรูปธรรม

Conducted training programs to disseminate knowledge and drive improvements in the Global Cybersecurity Index (GCI), strengthening understanding among government agencies, regulators, critical information infrastructure organizations, educational institutions, and private sector entities. These efforts integrated the GCI framework into systematic cybersecurity operations and aligned relevant strategies, policies, and action plans to concretely reflect Thailand's national cybersecurity capabilities.

จัด 22 ก.ค. 2568 | ผู้เข้าร่วม 158 คน
Held on 22 July 2025 | Total participants: 158

ประชุมรวบรวมข้อมูล ข้อเท็จจริง และหลักฐานประกอบการประเมินดัชนี GCI เพื่อเตรียมความพร้อมสำหรับการตอบแบบประเมินภายใต้ดัชนีชี้วัด Global Cybersecurity Index ของ International Telecommunication Union (ITU) โดยมุ่งเน้นการรวบรวมข้อมูลที่สอดคล้องกับกรอบการประเมินในทุกมิติ

Convened meetings to collect data, factual information, and supporting evidence for the Global Cybersecurity Index (GCI) assessment in preparation for Thailand's submission to the International Telecommunication Union (ITU). The process focused on ensuring that all information gathered was comprehensive and fully aligned with the assessment framework across all dimensions.

จัด 24 เม.ย. และ 27 พ.ค. 2568
ผู้เข้าร่วม 187 คน
Held on 24 April and 27 May 2025 | Total Participants: 187

การติดตามประเมินผลการดำเนินงานภายใต้นโยบายและแผนการรักษาความมั่นคงปลอดภัยไซเบอร์
Monitoring and Evaluation of the National Cybersecurity Policy and Action Plan Implementation

จัด**กิจกรรมติดตามและประเมินผลการดำเนินงานภายใต้นโยบายและแผนการรักษาความมั่นคงปลอดภัยไซเบอร์** เพื่อเสริมสร้างความรู้และความเข้าใจแก่หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อให้สามารถดำเนินโครงการและกิจกรรมต่าง ๆ ให้สอดคล้องกับนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565-2570 ได้อย่างมีประสิทธิภาพ

ในปี 2568 ได้จัดกิจกรรมติดตามและประเมินผลจำนวน 4 ครั้ง ทั้งในส่วนกลางและส่วนภูมิภาค **มีหน่วยงานที่เกี่ยวข้องเข้าร่วมรวม 1,124 คน**

Activities were conducted to monitor and evaluate the implementation of the National Cybersecurity Policy and Action Plan, with the aim of enhancing knowledge and understanding among government agencies, regulators, and critical information infrastructure organizations. These efforts were intended to enable participating entities to effectively implement projects and activities in alignment with the National Cybersecurity Policy and Action Plan (2022-2027).

In **2025**, a total of **four monitoring and evaluation activities** were conducted at both **central and regional levels,** with participation from **1,124 representatives** of relevant agencies.

ครั้งที่ 1
Session 1:
13 ส.ค. 2568
กรุงเทพฯ
13 August 2025 | Bangkok

ครั้งที่ 2
Session 2:
3 ก.ย. 2568
เชียงใหม่
3 September 2025 | Chiang Mai

ครั้งที่ 3
Session 3:
12 ก.ย. 2568
กรุงเทพฯ
12 September 2025 | Bangkok

ครั้งที่ 4
Session 4:
16 ธ.ค. 2568
ขอนแก่น
16 September 2025 | Khon Kaen

The Life Cycle of Policy and Action plan on cybersecurity

2565
2022
ประกาศนโยบายและแผนฯ ในราชกิจจานุเบกษา
Policy and Plan Announcement

ประกาศนโยบายและแผนฯ ในราชกิจจานุเบกษา มีผลบังคับใช้ตั้งแต่ 10 ธ.ค. 2565 เป็นต้นไป
The National Cybersecurity Policy and Action Plan were officially published in the **Royal Gazette, effective from 10 December 2022 onwards.**

2566
2023
กิจกรรมเผยแพร่นโยบายและแผนฯ
Policy and Plan Dissemination Phase

Kickoff แผนไซเบอร์ฉบับแรกของไทยอย่างเป็นทางการ พร้อมสร้างการรับรู้ให้กับ Reg CII และหน่วยงานภาครัฐ เพื่อขับเคลื่อนแผนปฏิบัติการให้เป็นรูปธรรม
Officially launched Thailand's first national cybersecurity plan, while raising awareness among Reg CII and government agencies to drive the effective and concrete implementation of the action plan.

2567
2024
กิจกรรมติดตามฯ นโยบายและแผนฯ
Monitoring and Follow-up Phase

ติดตามประเมินผลการดำเนินการหลังการเผยแพร่นโยบายและแผนฯ ในปีก่อนหน้า โดยมีการประชุมเชิงปฏิบัติการผ่าน Reg CII และหน่วยงานรัฐ เพื่อขับเคลื่อนนโยบายและแผนทั้ง 4 ยุทธศาสตร์ไปสู่การปฏิบัติ
Conducted follow-up monitoring and evaluation of implementation following the promulgation of the Policy and Plan in the previous year. Workshops were organized through Reg CII and government agencies to drive the implementation of the Policy and Plan across all four strategic pillars.

2568
2025
กิจกรรมติดตามฯ นโยบายและแผนฯ
Monitoring and Follow-up Phase

ติดตามประเมินผลต่อเนื่องเป็นปีที่สอง มีจำนวน CII เพิ่มขึ้น มีการประชุมเชิงปฏิบัติการลงรายละเอียดในระดับกลยุทธ์และตัวชี้วัดภายใต้นโยบายและแผนฯ
Continued monitoring and evaluation were carried out for the second consecutive year, with an increase in the number of organizations of the critical information infrastructure (CII). Workshops were conducted to facilitate in-depth strategic discussions, including performance indicators under the Policy and Action Plan.

2569
2026
กิจกรรมทบทวนนโยบายและแผนฯ
Comprehensive Review of Cybersecurity Policy and Action Plan

2570
2027
จัดทำนโยบายและแผนฯ พ.ศ. 2571-2575
Formulation of the National Cybersecurity Policy and Action Plan (2028-2032)

กิจกรรมเพื่อเสริมประสิทธิภาพหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเพื่อลดความเสี่ยงการถูกโจมตีทางไซเบอร์
Activities to Enhance the Effectiveness of Organizations of Critical Information Infrastructure (CII) to Mitigating the Risks of Cyberattacks

จัดขึ้นเพื่อ**พัฒนากรอบการประเมินความพร้อมและการปรับตัวด้านไซเบอร์ (Cyber Resilience Assessment)** ที่มีเกณฑ์เชิงปริมาณและเชิงคุณภาพชัดเจน โดยเชื่อมโยงระดับความเสี่ยงตั้งต้น (Inherent Risk) เข้ากับชุดมาตรการตามระดับความพร้อม (Maturity Level) อย่างเป็นระบบ เพื่อช่วยให้หน่วยงานเห็นความเสี่ยงและแนวทางยกระดับความมั่นคงไซเบอร์อย่างตรงจุด

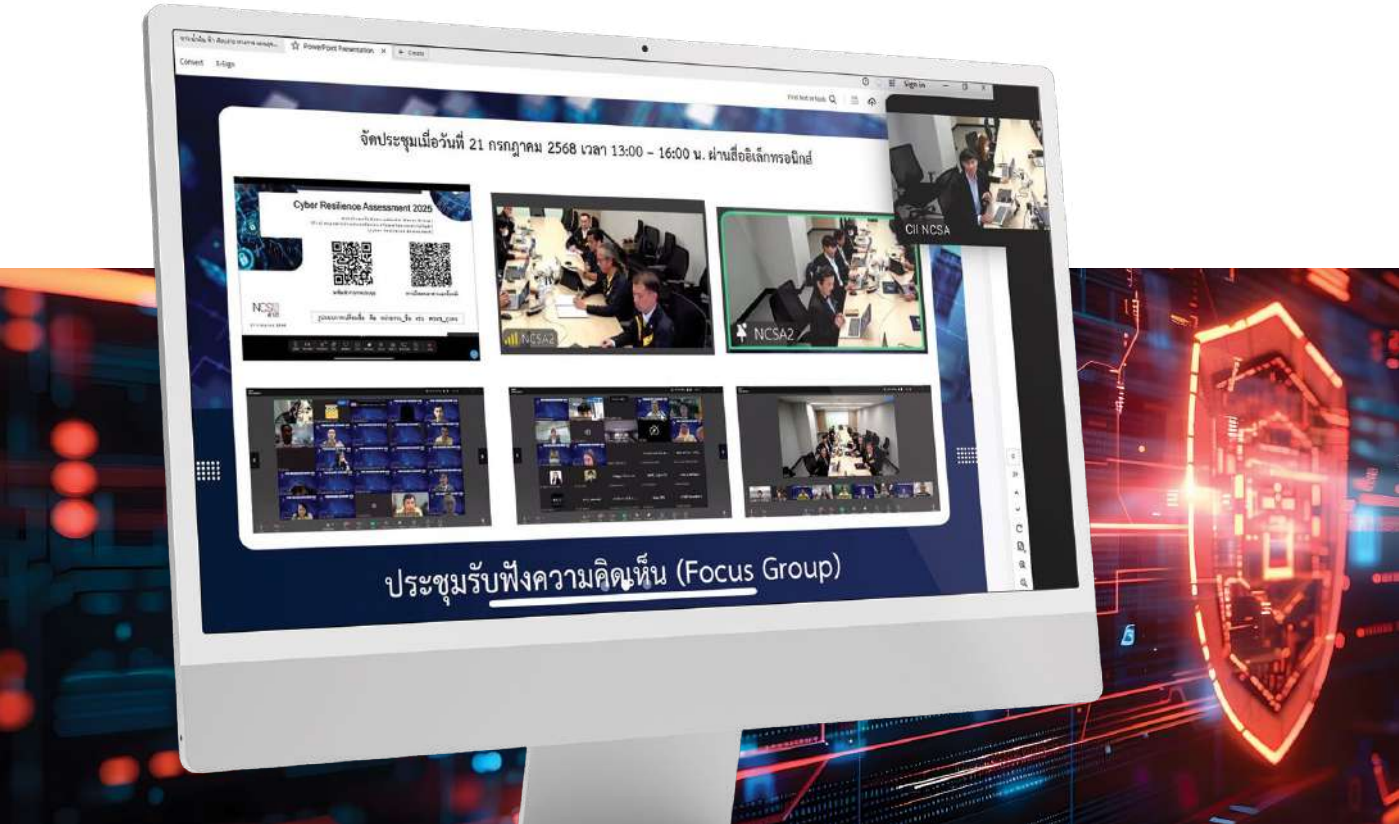
หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถใช้กรอบการประเมินดังกล่าวในการ**ประเมินตนเอง**เพื่อ**วัดระดับความพร้อม**และความสามารถในการป้องกัน รับมือ และฟื้นตัวจากภัยไซเบอร์ ซึ่งช่วยสนับสนุนการวางแผนและตัดสินใจเชิงนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ

These **activities were undertaken to develop a Cyber Resilience Assessment framework** with clearly defined quantitative and qualitative criteria, systematically linking inherent risk levels with corresponding control measures based on maturity levels. The framework enables organizations to clearly identify their risk exposure and targeted pathways for enhancing cybersecurity capabilities.

Organizations of critical information infrastructure (CII) can apply this assessment framework for **self-assessment** to evaluate their level of readiness and their capacity to prevent, respond to, and recover from cyber threats. The framework thereby supports effective cybersecurity planning and informed policy-level decision-making.

ปี 2568 มีการประชุมชี้แจงการใช้งานระบบผ่านสื่ออิเล็กทรอนิกส์ 1 ครั้ง เมื่อวันที่ 21 กรกฎาคม 2568 มีผู้เข้าร่วม 480 คน

In 2025, one briefing meeting on the use of the system was conducted via electronic media. The meeting was held on 21 July 2025, with 480 participants in attendance.



กิจกรรมยกระดับขีดความสามารถการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Self-Assessment)
Activities to Enhance Cybersecurity Capability (Cybersecurity Self-Assessment)

มุ่งทบทวนและประเมินระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อนำผลการประเมินไปใช้พัฒนาขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานอย่างเป็นระบบและต่อเนื่อง

These activities focus on reviewing and assessing the cybersecurity maturity of government agencies, regulators, and the organizations of critical information infrastructure (CII), with the assessment results used to systematically and continuously enhance their cybersecurity capabilities.

จัดประชุมชี้แจงรายละเอียดการประเมิน ขีดความสามารถการรักษาความมั่นคงปลอดภัยไซเบอร์ทางสื่ออิเล็กทรอนิกส์ เมื่อวันที่ 27 พฤษภาคม 2568 มีผู้เข้าร่วมมากกว่า 600 คน
Conducted a detailed briefing on the Cybersecurity Self-Assessment framework via electronic media on **27 May 2025,** with **over 600 participants.**

จัดประชุม Self-Assessment Clinic ระหว่างวันที่ 4-5 มิถุนายน 2568
Organized a Self-Assessment Clinic held from **4-5 June 2025,** providing hands-on guidance and consultations.

จัดทำเอกสารโครงการและแผนการดำเนินงาน ได้แก่ Self-Assessment Project Kick-Off และหนังสือส่งแผนการทำงานโครงการ
Prepared project documentation and implementation plans, including the **Self-Assessment Project Kick-Off** and official project implementation notification letters.

คัดเลือก 38 หน่วยงานเข้ารับคำปรึกษาเชิงลึก ผ่านสื่ออิเล็กทรอนิกส์ หรือ ณ สถานที่ทำการของหน่วยงาน ระหว่างเดือนมิถุนายน-กันยายน 2568
Selected 38 agencies to receive **in-depth advisory support,** delivered through electronic channels or on-site consultations during **June-September 2025.**

จัดทำรายงานสรุปผลการปรับปรุงแก้ไขและการให้คำปรึกษาหลังการดำเนินงาน
Compiled a summary report on improvement outcomes and post-implementation advisory results to support further development and policy-driven decision-making.

การจัดทำแผนเผชิญเหตุด้านไซเบอร์
National Cyber Incident Response Plan

ทบทวนแผนเผชิญเหตุด้านไซเบอร์ระดับชาติ และจัดทำแผนเผชิญเหตุด้านไซเบอร์สำหรับหน่วยงาน เพื่อเป็นแนวทางในการแก้ไขปัญหาในกรณีเกิดเหตุภัยคุกคามทางไซเบอร์ในแต่ละระดับได้ทันท่วงที

Review and update the National Cyber Incident Response Plan, and develop tailored cyber incident response plans for relevant agencies to provide practical guidance for timely and effective responses to cybersecurity incidents at each level.

แผนเผชิญเหตุ 5 รุ่น รวม 400 คน 173 หน่วยงาน
Five Rounds of Incident Response Planning Workshops Total participants: 400 persons from 173 agencies

รุ่นที่ 1-19 ส.ค. 68
ด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ และหน่วยงานของรัฐ **72 คน | 37 หน่วยงาน**
Round 1-19 August 2025
National security sector, critical government services, and government agencies
72 participants | 37 agencies

รุ่นที่ 2-20 ส.ค. 68
ด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ และหน่วยงานของรัฐ **57 คน | 25 หน่วยงาน**
Round 2-20 August 2025
National security sector, critical government services, and government agencies
57 participants | 25 agencies

รุ่นที่ 3-25 ส.ค. 68
ด้านการศึกษา ด้านสาธารณสุข
151 คน | 62 หน่วยงาน
Round 3-25 August 2025
The education sector and the public health sector
151 participants | 62 agencies

รุ่นที่ 4-26 ส.ค. 68
ด้านการเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม และหน่วยงานภาครัฐ
48 คน | 20 หน่วยงาน
Round 4-26 August 2025
Finance and banking sector, information and communication technology sector, and government agencies
48 participants | 20 agencies

รุ่นที่ 5-27 ส.ค. 68
ด้านสาธารณูปโภค ด้านการขนส่งและโลจิสติกส์ และหน่วยงานภาครัฐ
72 คน | 29 หน่วยงาน
Round 5-27 August 2025
Public utilities sector, transportation and logistics sector, and government agencies
72 participants | 29 agencies

ระบบช่วยเหลือ (Help Desk) ของ ThaiCERT
ThaiCERT Help Desk System

เป็นศูนย์กลางให้คำปรึกษา ช่วยเหลือ รับแจ้งเหตุ และแจ้งเตือนเหตุการณ์ภัยคุกคามทางไซเบอร์แก่หน่วยงานรัฐ หน่วยงานกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และประชาชน

Serves as a central hub for consultation, assistance, incident reporting, and coordination in response to cyber threats for Government Agencies, Regulators, Organizations of Critical Information Infrastructure (CII), and the public.

โทรศัพท์
02 114 3531
Telephone:
+66 2 114 3531

Appilcation:
THCert HelpDesk

Facebook:
ThaiCERT

Email:
thaicert@ncsa.or.th

LINE OA:
ThaiCERT

Website: https:
//thaicertservice.ncsa.or.th/

LINE: @THAICERT

APP: THCERTHELPDESK

รับแจ้งเหตุถึงปัจจุบัน **4,023** เหตุการณ์

Cyber Incident Reports in FY2025
4,023 incidents

การพัฒนาระบบสนับสนุนการตอบสนอง
Development of an Incident Response Support System

ใช้ระบบตอบสนองภัยคุกคามไซเบอร์โดย**อัตโนมัติ** ผ่าน Chatbot ให้บริการผ่าน Line OA และ Facebook Messenger และเชื่อมต่อกับคลังความรู้เพื่อค้นหา FAQ การแจ้งเตือน และแนวทางป้องกันแก้ไขภัยไซเบอร์อย่างรวดเร็ว

Deployment of an **automated cyber incident response system,** integrating chatbot services via LINE Official Account and Facebook Messenger, connected to a centralized knowledge base to provide FAQs, alerts, and guidance for rapid cyber incident prevention and mitigation.

การเฝ้าระวังภัยคุกคามเชิงรุกผ่าน 3 โครงการย่อย ได้แก่
Proactive Cyber Threat Monitoring

Implemented through **three sub-projects:**

1. โครงการเพิ่มประสิทธิภาพการตรวจจับเชิงรุก 25 หน่วยงาน
   Proactive Threat Detection Enhancement Project implemented across 25 agencies
2. โครงการสนับสนุนการจัดตั้ง Sectoral CERT (ขนส่งและพลังงาน)
   Sectoral CERT Establishment Support Project (Transport and Energy Sectors)
3. กิจกรรมยกระดับความมั่นคงปลอดภัยหน่วยงานโครงสร้างพื้นฐานสำคัญที่มีความเสี่ยง
   Activities to enhance cybersecurity readiness for high-risk organizations of critical information infrastructure

ผลงานและโครงการสำคัญประจำปี
KEY OF THE YEAR ACHIEVEMENTS AND PROJECTS

- สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Capacity)
  Enhancing national cybersecurity capacity (human resources, knowledge ecosystem, and technology) ***(Capacity)***
- บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)
  Strengthening cooperation networks to enhance preparedness for cyber incident response and recovery ***(Partnership)***
- สร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Resilience)
  Ensuring the cybersecurity and resilience of government services and critical information infrastructure ***(Resilience)***
- สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน (Standard)
  Raising the quality and standards of national-level agencies ***(Standard)***

สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ (บุคลากร องค์ความรู้ และเทคโนโลยี)

Enhancing National Cybersecurity Capacity *(Human Resources, Knowledge, and Technology)*

มุ่งเพิ่มบุคลากรที่มีความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ ควบคู่ไปกับการสร้างความตระหนักรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์แก่ทุกภาคส่วน พร้อมส่งเสริมการวิจัยและพัฒนานวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์ให้สอดรับกับเป้าหมายของประเทศในการพัฒนาศักยภาพด้านการวิจัยและเทคโนโลยีความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ

This initiative aims to strengthen the national cybersecurity workforce by increasing the number of skilled cybersecurity professionals, while simultaneously enhancing cybersecurity awareness and skills across all sectors. In parallel, it promotes research and development as well as innovation in cybersecurity, aligned with national goals to advance research capacity and cybersecurity technologies at the national level.

สร้างความตระหนักรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์ เสริมศักยภาพคนไทยในทุกภาคส่วน
Building Cybersecurity Awareness and Skills, Empowering Thai Talent Across All Sectors

สร้างเกราะป้องกันทางความคิด ติดอาวุธทางปัญญา สู้ภัยไซเบอร์ เดินหน้าพัฒนาศักยภาพคนไทยทั่วประเทศ สู่มาตรฐานโลก พร้อมผนึกพันธมิตรสร้างสังคมดิจิทัลที่มั่นคงและยั่งยืน

Strengthening cyber resilience through intellectual empowerment, enhancing the capabilities of Thai people nationwide to meet global standards, and forging strong partnerships to build a secure and sustainable digital society.

ปั้นมืออาชีพสู่มาตรฐานสากล ผ่านเวทีแข่งขัน Cyber Top Talent
Developing Cybersecurity Professionals to Global Standards Through Competitive Programs: Cyber Top Talent

ยกระดับทักษะและแนะแนวอาชีพด้านความมั่นคงปลอดภัยไซเบอร์ สร้างบุคลากรคุณภาพสู่ตลาดแรงงานและเสริมความพร้อมของสังคมดิจิทัล

Enhancing cybersecurity skills and career pathways to develop a high-quality workforce for the labor market and strengthen the readiness of Thailand's digital society.

- **เป้าหมาย : 80 ทีม**
  Target: 80 teams
- **เข้าร่วมจริง : 1,352 ทีม**
  Actual participation: 1,352 teams
- **สูงกว่าเป้าหมาย : 1,590%**
  Above target: 1,590%
- **จัดกิจกรรมแนะแนวอาชีพ/ฝึกทักษะ 4 ครั้ง บรรลุเป้าหมาย 100%**
  Training / skill-building activities: 4 rounds (100% of target achieved)

ชูศักยภาพพลังหญิงไซเบอร์ ผ่านเวที Women Thailand Cyber Top Talent 2024
Empowering Women in Cybersecurity, through Women Thailand Cyber Top Talent 2024

เปิดเวทีให้เพื่อนหญิง พลังหญิง และผู้ที่มีเพศสภาพเป็นหญิง แสดงศักยภาพ พัฒนาทักษะ และขยายโอกาสสู่สายอาชีพไซเบอร์

Opening opportunities for women and individuals with a female gender identity to showcase their potential, develop cybersecurity skills, and expand career opportunities in the cybersecurity profession.

- **เป้าหมาย : 100 ทีม**
  Target: 100 teams
- **ทีมเข้าร่วมจริง : 793 ทีม**
  Actual participation: 793 teams
- **สูงกว่าเป้าหมาย : 693%**
  Above target: 693%

เฟ้นหาดาวรุ่ง ช้างเผือกไซเบอร์
Discovering Rising Stars: Expanding Cyber Talent Nationwide

สร้างความร่วมมือกับสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) **จัดกิจกรรมการแข่งขัน NCSA X NBTC CYBER TOP TALENT 2025** เพื่อวัดระดับทักษะและเฟ้นหาดาวรุ่งด้านไซเบอร์ จากโรงเรียนในพื้นที่ห่างไกลและพื้นที่ชายขอบทั่วประเทศไทย

In collaboration with the **National Broadcasting and Telecommunications Commission (NBTC),** NCSA organized the **NCSA x NBTC Cyber Top Talent 2025** competition to elevate cybersecurity skills and identify emerging cyber talent from schools in remote and underserved areas across Thailand.

- **เป้าหมาย : ผู้เข้าร่วม 3,000 คน**
  Target participants: 3,000 people
- **ผู้เข้าร่วมจริง : 12,691 คน**
  Actual participants: 12,691 people
- **สูงกว่าเป้าหมาย 323%**
  Above target: 323%

อบรมและทดสอบ “Certified in Cybersecurity” ของ ISC2
Training and Examination: “Certified in Cybersecurity” by ISC2

เตรียมความพร้อมสำหรับการสอบเพื่อรับประกาศนียบัตรมาตรฐานสากลด้านความปลอดภัยทางไซเบอร์ เน้นสร้างความรู้และความเข้าใจพื้นฐานที่จำเป็นอย่างเป็นระบบ เพื่อให้ผู้เข้าร่วมสามารถพิสูจน์ทักษะระดับเริ่มต้นได้อย่างเป็นรูปธรรม อันเป็นก้าวแรกเข้าสู่ตลาดแรงงานด้านไซเบอร์

Preparing participants for internationally recognized cybersecurity certification examinations, with an emphasis on building foundational knowledge and systematic understanding of cybersecurity. This enables participants to demonstrate entry-level skills and take their first step into the cybersecurity workforce.

- **เป้าหมายผู้เข้าอบรม : 10,000 คน**
  Training target: 10,000 participants
- **ผู้เข้ารับการอบรมจริง 11,410 คน**
  Actual participants: 11,410 participants
- **สูงกว่าเป้าหมาย 14%**
  Above target: 14%

ร่วมมือกับ TPQI เป็นผู้ให้บริการฝึกอบรม
Collaboration with TPQI as a Training Provider

ขับเคลื่อนความร่วมมือกับสถาบันคุณวุฒิวิชาชีพ (TPQI) ในการทำหน้าที่เป็นผู้ให้บริการฝึกอบรม (Training Provider) มุ่งเน้นการทดสอบระบบและกระบวนการฝึกอบรมร่วมกันอย่างต่อเนื่อง

Collaboration was strengthened with the Thailand Professional Qualification Institute (TPQI) in its role as a **Training Provider,** with a focus on continuous testing and improvement of training systems and processes.

- **เป้าหมาย : ทดสอบระบบร่วมกับ TPQI 3 ครั้ง**
  Target: Joint system testing with TPQI – 3 rounds
- **ผลการดำเนินงานจริง : 4 ครั้ง**
  Actual implementation: 4 rounds
- **สูงกว่าเป้าหมาย : 33%**
  Exceeded target by: 33%

ร่วมกับ บริษัท หัวเว่ย เทคโนโลยี่ (ประเทศไทย) จำกัด จัดอบรมและพัฒนาบุคลากร
Collaboration with Huawei for Training and Workforce Development

ร่วมกับ บริษัท หัวเว่ย เทคโนโลยี่ (ประเทศไทย) จำกัด จัดอบรมเชิงวิชาการ เพื่อยกระดับศักยภาพบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ และส่งเสริมความพร้อมของประเทศในการรับมือภัยคุกคามไซเบอร์ที่ส่งผลต่อสภาพแวดล้อมระบบคลาวด์ในปัจจุบันและอนาคต

กำหนดเป้าหมายผู้เข้ารับการอบรมจำนวน 300 คน ผลการดำเนินงานจริงมีผู้เข้ารับการอบรมจำนวน 50 คน ซึ่งต้องพัฒนารูปแบบการอบรมและการขยายผลในกิจกรรมครั้งต่อไปให้เข้าถึงกลุ่มเป้าหมายได้อย่างมีประสิทธิภาพยิ่งขึ้น

In collaboration with Huawei Technologies (Thailand) Co., Ltd., technical training programs were conducted to enhance cybersecurity workforce capacity and strengthen national readiness to respond effectively to cyber threats, particularly in relation to the evolving cloud ecosystem.

- **Training target:** 300 participants
- **Actual participants:** 50 participants

The program is being refined to improve training formats and expand future activities to reach broader target groups more effectively.

จัดโครงการอบรมร่วมกับ กอ.รมน.
Joint Training Program with ISOC Thailand

ร่วมกับกองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร (กอ.รมน.) ออกแบบหลักสูตรอบรมให้สอดคล้องกับภารกิจด้านความมั่นคงและความต้องการทักษะในปัจจุบัน

In collaboration with the Information Security Operations Center (ISOC Thailand), training curricula were designed to align with current national security missions and emerging cybersecurity needs.

- **เป้าหมาย : ผู้เข้าอบรม 2,000 คน**
  Target trainees: 2,000 participants
- **ผู้เข้าอบรมจริง : 2,339 คน**
  Actual participants: 2,339 participants
- **สูงกว่าเป้าหมาย 17%**
  Exceeded target by: 17%

เรียนรู้ออนไลน์ ผ่านกิจกรรม AIS อุ่นใจไซเบอร์
Online Learning through the “AIS Aunjai Cyber” Initiative

ร่วมมือกับบริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน) ขยายความรู้และความเข้าใจเกี่ยวกับการใช้งานเทคโนโลยีอย่างปลอดภัยไปสู่ประชาชนในวงกว้าง

In partnership with Advanced Info Service Public Company Limited (AIS), online learning activities were delivered to raise public awareness and understanding of safe and responsible use of digital technologies.

- **เป้าหมายผู้ลงทะเบียน : 400,000 คน**
  Target registrants: 400,000 people
- **ผู้ลงทะเบียนจริง : 600,000 คน**
  Actual registrants: 600,000 people
- **สูงกว่าเป้าหมาย : 50%**
  Exceeded target by: 50%

จัดโครงการอบรมร่วมกับ สพฐ.
Training Programs in Collaboration with OBEC

ร่วมกับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน (สพฐ.) ส่งต่อความรู้ด้านความมั่นคงปลอดภัยไซเบอร์สู่กลุ่มเป้าหมายเด็กและเยาวชนไทย

In collaboration with the **Office of the Basic Education Commission (OBEC)** The training programes were conducted to promote cybersecurity awareness and knowledge among Thai children and youth.

- **เป้าหมาย : ผู้เข้าอบรม 2,000 คน**
  Target participants: 2,000 persons
- **มีผู้เข้ารับการอบรมจริง : 2,051 คน**
  Actual participants: 2,051 persons
- **สูงกว่าเป้าหมาย 3%**
  Exceeded target by: 3%

จับมือ Microsoft จัดอบรมสำหรับนักเรียน นักศึกษา บุคลากร และประชาชนทั่วไป
Collaboration with Microsoft for Cybersecurity Training

ร่วมมือกับ Microsoft จัดอบรมหลักสูตรเฉพาะทาง เช่น หลักสูตรเปิดโลกทักษะ AI และหลักสูตร Microsoft AI Skills for All เปิดโอกาสให้นักเรียน นักศึกษา บุคลากร และประชาชนทั่วไป ได้เพิ่มพูนศักยภาพในด้านความปลอดภัยไซเบอร์

NCSA partnered with **Microsoft** to deliver specialized training programs for students, university students, personnel, and the general public. These programs included courses such as **AI Fundamentals** and **Microsoft AI Skills for All,** aimed at enhancing digital and cybersecurity capabilities across all population groups.

- **เป้าหมาย : ผู้เข้าอบรม 10,000 คน**
  Target participants: 10,000 persons
- **มีผู้เข้ารับการอบรมจริง : 34,282 คน**
  Actual participants: 34,282 persons
- **สูงกว่าเป้าหมาย 243%**
  Exceeded target by: 243%

พัฒนาความรู้ร่วมกับโรงเรียนสารสาสน์ และโรงเรียนเตรียมอุดมศึกษาพัฒนาการ Cybersecurity Education with Sarasas Schools and Triam Udom Suksa Pattanakarn School

บรรจุหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ในเครือโรงเรียนสารสาสน์ และโรงเรียนเตรียมอุดมศึกษาพัฒนาการ เพื่อสร้างศักยภาพครู บุคลากรทางการศึกษา และนักเรียน ให้มีความรู้ด้านความมั่นคงปลอดภัยไซเบอร์

Cybersecurity curricula were integrated into the Sarasas school network and Triam Udom Suksa Pattanakarn School to strengthen the capacity of teachers, educational personnel, and students in cybersecurity knowledge and awareness.

- **เป้าหมาย : ผู้เข้าร่วม 2,000 คน**
  Target participants: 2,000 persons
- **ผู้เข้าร่วมจริง : 2,788 คน**
  Actual participants: 2,788 persons
- **สูงกว่าเป้าหมาย 39%**
  Exceeded target by: 39%

สร้างการรับรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่ประชาชนทั่วไป Public Cybersecurity Awareness for All Citizens

ส่งต่อความรู้ด้านความมั่นคงปลอดภัยไซเบอร์สู่ทุกกลุ่มเป้าหมาย ทั้งเด็ก เยาวชน คนทำงาน ผู้สูงอายุ และคนพิการ ผ่านกิจกรรม **NCSA Cybersecurity Knowledge Sharing**

Cybersecurity awareness was extended to all target groups, including children, youth, working adults, senior citizens, and persons with disabilities, through the **NCSA Cybersecurity Knowledge Sharing** activities.

- **เป้าหมาย : ผู้เข้าร่วม 1,200 คน**
  Target participants: 1,200 persons
- **ผู้เข้าร่วมจริง : 19,102 คน**
  Actual participants: 19,102 persons
- **สูงกว่าเป้าหมายที่ตั้งไว้ถึง 1,492%**
  Exceeded target by: 1,492%

พัฒนาและฝึกอบรมหลักสูตรระดับประกาศนียบัตรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ประชาชน
Development and Provision of Certification-Level Cybersecurity Training Programs for the Public

จัดทำรายงานการศึกษาเบื้องต้น (Inception Report) เพื่อเป็นกรอบแนวทางในการพัฒนาหลักสูตรที่เหมาะสมสำหรับประชาชน โดยกำหนดโครงสร้างหลักสูตรและแนวทางการจัดการเรียนรู้เบื้องต้นไว้แล้ว

Preparation of an Inception Report to establish a framework for the development of appropriate certificate-level cybersecurity training for the public, including the preliminary curriculum structure and learning approaches.

พัฒนาบุคลากรและวิทยากรด้านความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐานสากลให้ประชาชน
Development of Cybersecurity Personnel and Instructors in Line with International Standards

เสริมสมรรถนะด้านไซเบอร์ให้ประชาชนมีความรู้ตามมาตรฐานสากล รองรับความเสี่ยงดิจิทัลที่เพิ่มขึ้น และสร้างฐานกำลังคนที่มีคุณภาพ ผ่านหลักสูตรอบรมเชิงปฏิบัติการที่ได้มาตรฐานและเข้าถึงกลุ่มเป้าหมายได้อย่างทั่วถึง

Enhancing public cybersecurity competencies in line with international standards to address rising digital risks and to build a high-quality workforce. This will be delivered through standardized, hands-on training programs designed to reach target groups nationwide.

- **เป้าหมาย : ผู้เข้าอบรม 1,070 คน**
  Target number of trainees: 1,070
- **ผู้เข้ารับการอบรมจริง : 2,278 คน**
  Actual number of trainees: 2,278
- **สูงกว่าเป้าหมาย : 113%**
  Exceeded the target by 113%

ในปี 2569 จะดำเนินการพัฒนา 2 หลักสูตร ตามเป้าหมายที่กำหนดไว้
In 2026, two certification programs will be developed in line with the established targets.

เพิ่มขีดความสามารถแก่บุคลากรด้านความมั่นคงปลอดภัยไซเบอร์
Enhancing the Capacity of Cybersecurity Personnel

เสริมสร้างศักยภาพบุคลากรหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อยกระดับขีดความสามารถของผู้ปฏิบัติงานทุกระดับ ให้มีความพร้อมในการกำกับ ดูแล และบริหารจัดการงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างมีประสิทธิภาพ

Strengthening the capabilities of personnel from government agencies, regulators, and critical information infrastructure (CII) organizations to enhance the readiness of practitioners at all levels for effective cybersecurity governance, oversight, and management.

เดินหน้าโครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ระยะที่ 2
Advancing the Intensive Cybersecurity Capacity Building Program - Phase 2

มุ่งพัฒนาบุคลากรให้มีความรู้และทักษะเฉพาะทางที่ทันสมัย เพื่อป้องกัน ลดผลกระทบ และพร้อมรับมือภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพตามมาตรฐานสากล

Focusing on the development of advanced and specialized cybersecurity knowledge and skills to prevent, mitigate, and respond effectively to cyber threats in line with international standards.

- **เป้าหมาย : 9 หลักสูตร ผู้เข้าอบรม 5,000 คน**
  Target: 9 training programs / 5,000 participants
- **ผลการดำเนินงานจริง : 11 หลักสูตร ผู้เข้าอบรม 14,344 คน**
  Actual results: 11 training programs / 14,344 participants

สร้างการรับรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้หน่วยงานเป้าหมาย (NCSA Cyber Clinic)
Building Cybersecurity Awareness for Target Agencies (NCSA Cyber Clinic)

จัดอบรมเพื่อพัฒนาขีดความสามารถให้บุคลากรหน่วยงานเป้าหมายในการปฏิบัติตามกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์

Delivering training programs to enhance cybersecurity capacity for personnel in designated target agencies, supporting compliance with national cybersecurity standards and frameworks.

- **เป้าหมาย : 65 หน่วยงาน**
  Target: 65 agencies
- **หน่วยงานเข้าร่วมจริง : 114 หน่วยงาน**
  Actual: 114 agencies
- **สูงกว่าเป้าหมาย 75%**
  Exceeded the target by 75%

ฝึกซ้อมรับมือภัยคุกคามไซเบอร์ระดับชาติ Thailand's National Cyber Exercise (NCX)

จัดขึ้นเพื่อทดสอบและพัฒนาขีดความสามารถในการรับมือกับภัยคุกคามไซเบอร์ของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้องตามที่กำหนดไว้ใน พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 การฝึกแบ่งเป็น 2 ส่วนหลัก ได้แก่

Organized to test and strengthen the capabilities of government agencies, regulators, critical information infrastructure (CII) organizations, and other relevant entities in responding to cyber threats, in accordance with the Cybersecurity Act 2019.

The exercise consists of two main components:

1 ด้านกระบวนการบริหารจัดการ
ซ้อมการตัดสินใจและประสานงานผ่านรูปแบบ War Room
Management Aspect: Decision-making and coordination exercises are conducted through a War Room format.

2 ด้านเทคนิค ฝึกปฏิบัติจริง (Hands-on) เพื่อรับมือสถานการณ์ไซเบอร์จำลอง
Technical Aspect: Hands-on exercises to respond to simulated cyber incidents.

การประชุม Meetings

CDC	จำนวน 71 คน 71 participants	31 หน่วยงาน 31 organizations
IPC	จำนวน 72 คน 72 participants	25 หน่วยงาน 25 organizations
MPC	จำนวน 82 คน 82 participants	38 หน่วยงาน 38 organizations
FPC	จำนวน 75 คน 75 participants	31 หน่วยงาน 31 organizations
ECG #1	จำนวน 16 คน 16 participants	13 หน่วยงาน 13 organizations
ECG #2	จำนวน 16 คน 16 participants	13 หน่วยงาน 13 organizations
ECG #3	จำนวน 14 คน 14 participants	14 หน่วยงาน 14 organizations
ECG #4	จำนวน 13 คน 13 participants	14 หน่วยงาน 14 organizations
ECG #5	จำนวน 15 คน 15 participants	14 หน่วยงาน 14 organizations
ECG #6	จำนวน 19 คน 19 participants	12 หน่วยงาน 12 organizations
Basic	จำนวน 595 คน 595 participants	308 หน่วยงาน 308 organizations
Advanced	จำนวน 120 คน 120 participants	90 หน่วยงาน 90 organizations
War room	จำนวน 1,016 คน 1,016 participants	101 หน่วยงาน 101 organizations

กำหนดการฝึก Exercise Timeline and Structure

ปีงบประมาณ 2568 Fiscal Year 2025

- 19 มิถุนายน 2568 (19 June 2025) — CDC (Concept & Design Conference)
- 3 กรกฎาคม 2568 (3 July 2025) — IPC (Initial Planning Conference)
- 24 กรกฎาคม 2568 (24 July 2025) — MPC (Main Planning Conference)
- 20 สิงหาคม 2568 (20 August 2025) — FPC (Final Planning Conference)
- มิถุนายน – ตุลาคม 2568 (June – October 2025) — Exercise DEV (Exercise Development)
- Online 3-5 ก.ย. 68 Hands on with System (ตลอดเดือน ก.ย.) ➔ Online: 3–5 Sep 2025 Hands-on with System (throughout Sep)
- Onsite 27-29 ต.ค. 68 (ตจว.) Hands on with System (ตลอดเดือน พ.ย.) ➔ Onsite: 27–29 Oct 2025 (Provincial Area) Hands-on with System (throughout Nov) — Pre-Ex (Pre-Ex / Academic)
- Onsite 08 ธ.ค. 68 (Live fire) ➔ Onsite: 8 Dec 2025 (Live-fire Exercise)
- Online 09 ธ.ค. 68 (AAR + war room) ➔ Online: 9 Dec 2025 (After Action Review: AAR + War Room) — Live Fire Exercise

CDC (Concept & Design Conference)
ออกแบบและพัฒนาแนวคิดการจัดการฝึก
Design and development of the exercise framework:
1. ร่างวัตถุประสงค์การฝึก Exercise objectives
2. ร่างผลลัพธ์ที่คาดหวัง Expected outcomes
3. ร่างสถานการณ์ฝึก Exercise scenarios
4. ร่างรูปแบบการฝึก Exercise formats
5. ร่างโครงสร้างการฝึก Exercise structure
6. ร่างระบบสนับสนุนการฝึก Exercise support systems

IPC (Initial Planning Conference)
ประชุมวางแผนขั้นต้น
Initial planning meeting:
1. ยืนยันวัตถุประสงค์การฝึกและผลลัพธ์ที่คาดหวัง Confirmation of exercise objectives and expected outcomes
2. ร่างแนวทางการกำหนดโจทย์ฝึก Approval of exercise scenarios
3. ร่างกำหนดการฝึก Definition of exercise scope
4. ร่างกิจกรรมสนับสนุนการฝึก Supporting activities
5. ร่างรายชื่อหน่วยงานที่จะเชิญเข้าร่วมการฝึก Identification of agencies to be invited to participate

MPC (Main Planning Conference)
ประชุมวางแผนขั้นกลาง
Main planning meeting:
1. ร่างลำดับสถานการณ์ฝึก Finalization of exercise scenarios
2. ร่างจำนวนและบทบาทของผู้ที่จะเข้ารับการฝึก Determination of the number and roles of participants
3. กรอบการควบคุมการฝึกและประเมินผล Development of exercise control and evaluation plans
4. แผนกิจกรรมสนับสนุน Plan for supporting activities

FPC (Final Planning Conference)
ประชุมวางแผนขั้นสุดท้าย
Final planning meeting:
1. วัตถุประสงค์การฝึก Exercise objectives
2. โจทย์ฝึกหรือประเภทโจทย์ฝึก และผลลัพธ์ที่คาดหวัง Confirmation of scenarios and expected outcomes
3. ร่างรายชื่อผู้ที่จะเข้ารับการฝึก list of participants

Exercise DEV (Exercise Development)
จัดทำสถานการณ์และโจทย์ฝึก
Development of exercise scenarios and injects
1. จัดทำสถานการณ์ฝึก Development of exercise scenarios
2. โจทย์ฝึก และผลลัพธ์ที่คาดหวัง Exercise injects and expected outcomes
3. กรอบการประเมินระดับความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ Readiness assessment criteria for cyber incident response

Pre-Ex (Pre-Ex / Academic)
การฝึกเตรียมการ
Preparatory training:
1. จัดการฝึกเตรียมการ Exercise preparation training
2. จัดการสอบคัดเลือกเข้าสู่รอบ Advance Participant screening and selection for the Advanced level
3. ประเมินผลการฝึกเตรียมการ Evaluation of the preparatory exercise

Live Fire Exercise
การฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ (Live fire)
Live cyber exercise to assess technical capabilities:
1. จัดการฝึก Live fire Live cyber attack simulation
2. ประเมินผล / AAR After Action Review (AAR)
3. ใบประกาศนียบัตร Awarding of certificates

Concept Development Conference: CDC
Exercise Development : Exercise Dev.
Initial Planning Conference: IPC
Pre Exercise : Pre-Ex
Middle Planning Conference : MPC
After Action Review : AAR
Final Planning Conference: FPC

ส่งเสริมการวิจัยและพัฒนานวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์
Promoting Research and Innovation in Cybersecurity

มุ่งยกระดับการศึกษา งานวิจัย และการพัฒนานวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์ ควบคู่กับการสร้างความร่วมมือระหว่างหน่วยงานวิจัย สนับสนุนการลงทุนในเทคโนโลยีด้านความมั่นคงไซเบอร์ และผลักดันการพัฒนาผลิตภัณฑ์ที่สามารถนำไปใช้เชิงพาณิชย์ได้อย่างยั่งยืน

This initiative aims to advance education, research, and innovation in cybersecurity, while fostering collaboration among research institutions, supporting investment in cybersecurity technologies, and driving the development of products that can be sustainably commercialized and practically deployed.

ส่งเสริมผู้ประกอบการไซเบอร์ไทย ลดพึ่งพาเทคโนโลยีต่างชาติ
Strengthening Thai Cybersecurity Entrepreneurs and Reducing Dependence on Foreign Technologies

กิจกรรมประชาคมไซเบอร์ ครั้งที่ 3 เมื่อวันที่ 14 กรกฎาคม 2568 จัดสัมมนาและรับฟังความคิดเห็นเพื่อจัดทำแผนส่งเสริมอุตสาหกรรม เป็นเวทีให้ภาครัฐ เอกชน สถาบันวิจัย และผู้ประกอบการ ร่วมกำหนดทิศทางการพัฒนาอย่างยั่งยืน

The 3rd Cyber Community Forum, held on 14 July 2025, was organized to gather insights and recommendations for formulating policies and measures to promote Thailand's cybersecurity industry. The forum brought together representatives from government agencies, the private sector, research institutions, and cybersecurity entrepreneurs to jointly define sustainable development directions for the domestic cybersecurity ecosystem.

ร่วมกับ สนช. จัดงานแถลงข่าวความสำเร็จของความร่วมมือในการสนับสนุนผู้ประกอบการนวัตกรรมด้านไซเบอร์ ภายใต้โครงการ "แปลงเทคโนโลยีเป็นทุน" ในงาน Startup x Innovation Thailand Expo 2025 (SITE 2025) เพื่อผลักดันสตาร์ทอัพไทยพัฒนาเทคโนโลยีที่แข่งขันได้ ลดการพึ่งพาต่างชาติ

In collaboration with the National Innovation Agency (NIA), a press conference was held to announce the achievements of the cooperation in supporting Thai cybersecurity entrepreneurs under the initiative "Transforming Technology into Capital," at the Startup x Innovation Thailand Expo 2025 (SITE 2025). The initiative aims to empower Thai startups to develop competitive cybersecurity technologies and reduce reliance on foreign solutions.

จัดทำและปรับปรุงฐานข้อมูลผู้ให้บริการและผู้ประกอบการภาคอุตสาหกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
Development and Enhancement of the Database of Cybersecurity Service Providers and Industry Operators

ในปี 2568 นี้ ได้นำข้อมูลผู้ประกอบการเข้าสู่เว็บไซต์ CybrePlus และสามารถสืบค้นแยกตามบริการได้เรียบร้อย 72 ราย คิดเป็น 100% จากจำนวนผู้ประกอบการในปัจจุบัน

In 2025, data on cybersecurity operators were uploaded to the CybrePlus website and made searchable by service categories. A total of 72 operators are listed, representing 100% of the operators currently in operation.

กำหนดทิศทางและสนับสนุนการวิจัยเพื่อสร้างองค์ความรู้และเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์
Setting Directions and Supporting Research to Advance Knowledge and Technology in Cybersecurity

แต่งตั้งคณะทำงานและจัดประชุมร่วมกับเครือข่ายนักวิจัยด้านความมั่นคงปลอดภัยไซเบอร์จากทั่วประเทศ เพื่อรวบรวมข้อเสนอเชิงนโยบายและจัดทำแผนการพัฒนาและสนับสนุนการวิจัยที่สำคัญของประเทศ กระบวนการดังกล่าวนำไปสู่การพิจารณาและรับรองนักวิจัย พร้อมใช้เป็นข้อมูลประกอบการสนับสนุนแหล่งทุน การจัดสรรงบประมาณ และการกำหนดทิศทางการพัฒนางานวิจัยด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ

Dedicated working committees were appointed, and joint meetings were held with nationwide cybersecurity research networks to gather policy recommendations and formulate national priority research development and support plans. This process led to the review and endorsement of researchers and provides a basis for funding support, budget allocation, and the systematic direction of cybersecurity research.

ส่งเสริมและขยายองค์ความรู้ด้านวิชาการทั้งในระดับประเทศและระดับนานาชาติ
Promoting and Expanding Academic Knowledge at the National and International Levels

- จัดทำบทความ **“Thailand’s Preparedness for Post-Quantum Era”** นำเสนอบนเวทีของ IEEE โดยนักวิจัยของ สกมช.และอยู่ระหว่างการเผยแพร่บน IEEE Xplore
- จัดทำบทความ **“การออกแบบกรอบความร่วมมือเพื่อการแบ่งปันชุดข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์อย่างมั่นคงปลอดภัยและมีจริยธรรมเพื่อส่งเสริมการวิจัยด้านปัญญาประดิษฐ์”**

- Preparation of the paper **“Thailand’s Preparedness for the Post-Quantum Era,”** presented at an IEEE conference by NCSA researchers and currently under publication on **IEEE Xplore**.
- Development of the paper **“Designing a Collaborative Framework for Secure, Safe, and Ethical Cybersecurity Data Sharing to Support Artificial Intelligence Research.”**

IEEE Advancing Technology for Humanity


Thailand's Preparedness for Post-Quantum Era

นำเสนอเอกสารวิจัยต่อ IEEE Conference Co-Chair เมื่อ 14 ก.ย.68
Presentation of research papers to the IEEE Conference Co-Chair on 14 September 2025

เดินหน้าขับเคลื่อน ศชวช.
Driving HTCR Forward

ศูนย์รวมผู้เชี่ยวชาญการวิจัยเพื่อความมั่นคงปลอดภัยไซเบอร์แห่งประเทศไทย (ศชวช.) เปิดตัวอย่างเป็นทางการเมื่อวันที่ 13 สิงหาคม 2568 และได้เดินหน้าขับเคลื่อนกิจกรรมด้านการวิจัย การแลกเปลี่ยนองค์ความรู้ และการพัฒนาศักยภาพนักวิจัยอย่างต่อเนื่อง เพื่อยกระดับงานวิจัยด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ

The Thailand Hub of Talents in Cybersecurity Research (HTCR) was officially launched on 13 August 2025 and has since been actively driving research initiatives, knowledge exchange, and researcher capacity development to advance cybersecurity research and strengthen Thailand's national cybersecurity resilience in a sustainable manner.

จัดตั้งสถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
Establishment of the Thailand National Cyber Academy

ออกแบบสถาบันและได้รับแบบแปลนจัดตั้งเรียบร้อยแล้ว ถือเป็นก้าวสำคัญในการเตรียมความพร้อมด้านโครงสร้างพื้นฐานที่จะสนับสนุนการฝึกอบรมและพัฒนาบุคลากรไซเบอร์ สำหรับประเทศไทยในอนาคต

สถาบันนี้มีบทบาทเป็นศูนย์กลางในการพัฒนาทักษะความมั่นคงปลอดภัยไซเบอร์ ทั้งสำหรับเจ้าหน้าที่รัฐ ภาคเอกชน และประชาชนทั่วไป รวมถึงสนับสนุนการยกระดับมาตรฐานความปลอดภัยและการรับมือภัยคุกคามไซเบอร์ที่ซับซ้อนขึ้นอย่างต่อเนื่อง

The academy has been fully designed and approved for establishment, marking a significant milestone in strengthening foundational infrastructure to support cybersecurity training and workforce development for Thailand's future. It will serve as a **central hub for cybersecurity capacity building,** catering to government officials, private sector personnel, and the general public. It will also play a key role in **raising national cybersecurity standards** and enhancing preparedness against increasingly complex cyber threats on a continuous basis.

จัดหาโครงสร้างพื้นฐานที่จำเป็นสำหรับการวิจัยความมั่นคงปลอดภัยไซเบอร์
Establishing Essential Infrastructure for Cybersecurity Research

เพื่อพัฒนาระบบรับรองผู้ให้บริการไซเบอร์

ยกระดับการบริหารจัดการข้อมูลการรับรองคุณภาพผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ ผ่านการพัฒนาฐานข้อมูลกลางโดย สกมช. เพื่อให้หน่วยงานรัฐและเอกชนตรวจสอบคุณภาพได้อย่างโปร่งใส เลือกใช้บริการตามมาตรฐานเดียวกัน เพิ่มความเชื่อมั่นในอุตสาหกรรม และเสริมขีดความสามารถการแข่งขันของประเทศในระดับสากล

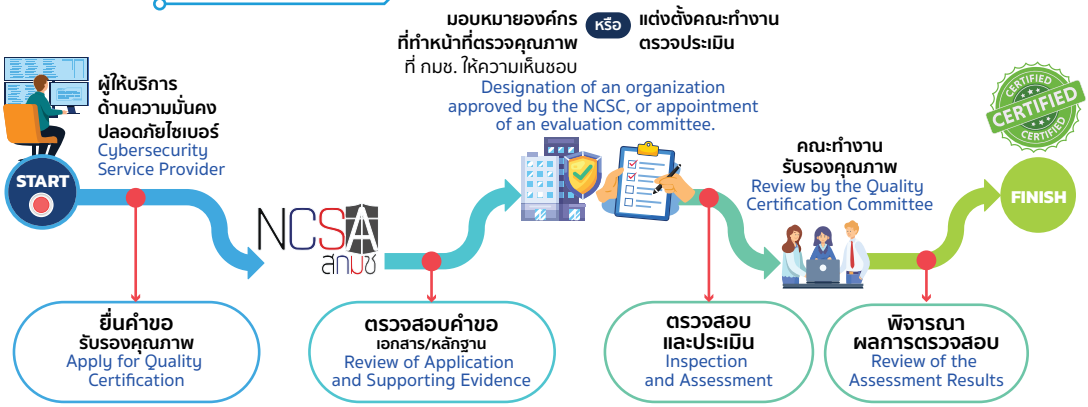
To develop a certification system for cybersecurity service providers by enhancing the management of certification data and quality assurance through a centralized database established by the NCSA. This will enable both public and private sector organizations to verify service quality transparently, select providers based on common standards, build trust within the industry, and strengthen Thailand's global competitiveness.

เพื่อจัดหาเครื่องมือและอุปกรณ์ที่จำเป็น

สำหรับการดำเนินงานของศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์ ช่วยสนับสนุนการทดสอบ วิเคราะห์ และวิจัยด้านเทคโนโลยีความมั่นคงปลอดภัยไซเบอร์

To procure essential tools and equipment for cybersecurity research centers in order to support testing, analysis, and research in cybersecurity technologies, thereby enabling the effective operation of national cybersecurity research facilities.

ขั้นตอนการดำเนินการ
Operational Process



ประกาศ กมช.
เรื่อง มาตรฐานและแนวทางส่งเสริมฯ
Notification of the NCSC
Re: Standards and Guidelines for Promoting the Development of Cybersecurity Service Delivery Systems, B.E. 2566 (2023)

ติดต่อสอบถามเพิ่มเติม

โทร : 0 2502 7825 | Tel: +66 2 502 7825
อีเมล : Research@ncsa.or.th | Email: Research@ncsa.or.th

การจัดตั้งห้องปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Lab)
Establishment of the Cyber Security Lab

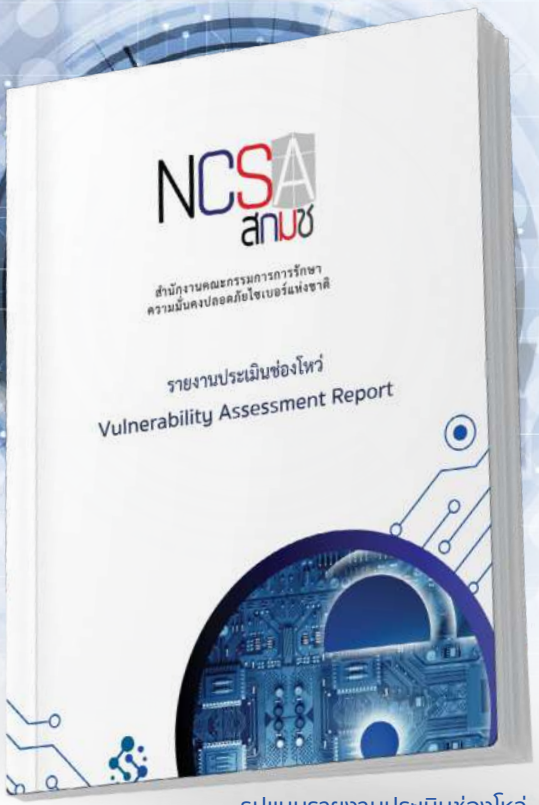
ในปี 2568 ThaiCERT ดำเนินการตรวจสอบและประเมินช่องโหว่ระบบสารสนเทศ และทดสอบการเจาะระบบอย่างต่อเนื่อง เพื่อเฝ้าระวังและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของหน่วยงานรัฐและเอกชน กระบวนการดังกล่าวช่วยให้หน่วยงานเห็นจุดอ่อนของระบบและนำไปสู่การปรับปรุงมาตรการป้องกันได้อย่างเหมาะสม

จากการตรวจสอบช่องโหว่ระบบของ **90 หน่วยงาน** แบ่งเป็น **หน่วยงานรัฐด้านอื่น ๆ 61 หน่วยงาน** ด้านสาธารณสุข 25 หน่วยงาน ด้านบริการภาครัฐที่สำคัญ 2 หน่วยงาน และด้านเทคโนโลยีสารสนเทศและโทรคมนาคม 2 หน่วยงาน พบว่า ส่วนใหญ่จัดอยู่ในกลุ่มที่มีช่องโหว่ใน**ระดับความรุนแรงปานกลาง** คิดเป็น **86%** ของทั้งหมด

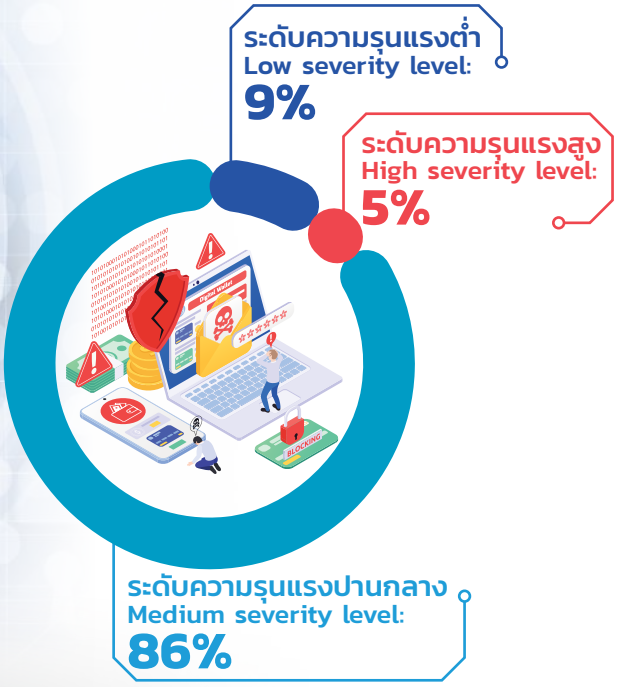
In 2025, ThaiCERT conducted continuous vulnerability assessments and penetration testing of information systems to monitor and evaluate cybersecurity risks across government and private-sector entities. The process enabled organizations to identify system weaknesses and supported the implementation of appropriate protective measures.

A total of **90 organizations** were assessed, comprising **61 government agencies** in other sectors, 25 in the public health sector, 2 responsible for critical government services, and 2 in the information technology and telecommunications sector.

The findings show that most vulnerabilities were classified at the **medium severity level**, representing **86%** of all identified issues.



รูปแบบรายงานประเมินช่องโหว่
Vulnerability Assessment Report



บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (PARTNERSHIP)

PARTNERSHIP: STRENGTHENING COOPERATION FOR CYBER INCIDENT RESPONSE AND RECOVERY

มุ่งเสริมสร้างความร่วมมือและเครือข่ายระหว่างหน่วยงานภาครัฐ ภาคเอกชน และองค์กรระหว่างประเทศ เพื่อยกระดับความพร้อมในการรับมือภัยไซเบอร์อย่างบูรณาการ และสนับสนุนการฟื้นคืนระบบสู่ภาวะปกติอย่างมีประสิทธิภาพ

To strengthen collaboration and networks among government agencies, the private sector, and international organizations in order to enhance integrated cyber resilience and support the efficient restoration of systems to normal operations.

ส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและเอกชน
Promoting and Supporting Public-Private Collaboration

บูรณาการความร่วมมือกับหน่วยงานภาครัฐ ภาคเอกชน ให้มีการแลกเปลี่ยน แบ่งปันองค์ความรู้ แนวคิด วิธีการ ประสบการณ์ในการรับมือภัยคุกคามทางไซเบอร์ที่เกิดขึ้น เพื่อยกระดับหน่วยงานของรัฐให้มีขีดความสามารถเพิ่มมากขึ้น

Collaboration between government agencies and the private sector facilitates the exchange of information, expertise, best practices, and operational experience in addressing cyber threats. Through this cooperation, the capabilities of government agencies are further enhanced.

บูรณาการความร่วมมือ สกมช.-สคส. ในการป้องกันการละเมิดข้อมูลส่วนบุคคลจากภัยคุกคามทางไซเบอร์
Integrated cooperation between NCSA and PDPC to prevent personal data breaches arising from cyber threats.

ร่วมกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) บูรณาการการทำงานเพื่อป้องกันการรั่วไหลและการละเมิดข้อมูลส่วนบุคคลจากภัยคุกคามทางไซเบอร์ ผ่านการประชุมวางแผน การแต่งตั้งคณะทำงานร่วม และการตรวจประเมินหน่วยงานของรัฐที่มีการประมวลผลข้อมูลส่วนบุคคลจำนวนมาก ตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐ ซึ่งต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2566

The National Cyber Security Agency (NCSA) works in close collaboration with the Office of Personal Data Protection Committee (PDPC) to integrate operational efforts aimed at preventing personal data breaches and violations arising from cyber threats. This collaboration includes joint planning, the establishment of joint working groups, and assessments of government agencies that process large volumes of personal data, in accordance with the Notification of the Personal Data Protection Committee on Personal Data Controllers and Personal Data Processors that are state agencies required to appoint a Data Protection Officer 2023.

ในช่วงกุมภาพันธ์-มิถุนายน 2568 ได้เข้าตรวจและให้คำแนะนำด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลแก่หน่วยงาน 30 แห่ง พร้อมเสนอแนะการดำเนินการให้สอดคล้องกับมาตรฐานสากล

Cybersecurity and Personal Data Protection Advisory Activities (February-June 2025)

Between February and June 2025, cybersecurity and personal data protection assessments and recommendations were provided to **30 government agencies,** with tailored recommendations prioritized according to the urgency and risk level of each agency.

MOU กับ DEPA เสริมแกร่งผู้ประกอบการไซเบอร์ไทย

MOU with DEPA to Strengthen Thai Cybersecurity Entrepreneurs

ลงนามบันทึกความเข้าใจกับสำนักงานส่งเสริมเศรษฐกิจดิจิทัล (depa) เพื่อสนับสนุนผู้ประกอบการด้านความมั่นคงปลอดภัยไซเบอร์ของไทยให้พัฒนาผลิตภัณฑ์และบริการตามมาตรฐาน และเชื่อมโยงหน่วยงานรัฐให้เข้าถึงผลิตภัณฑ์ไทยได้สะดวกขึ้น ความร่วมมือนี้มุ่งสร้างระบบนิเวศอุตสาหกรรมไซเบอร์ ผ่านการพัฒนาฐานข้อมูลผู้ประกอบการ การรับรองคุณภาพ การจับคู่ทางธุรกิจ และการเพิ่มโอกาสทางธุรกิจ เสริมความสามารถในการแข่งขันและขับเคลื่อนเศรษฐกิจดิจิทัลอย่างยั่งยืน

A Memorandum of Understanding (MOU) was signed with the Digital Economy Promotion Agency (DEPA) to support Thai cybersecurity entrepreneurs in developing products and services that comply with recognized standards, while enabling government agencies to more easily access locally developed solutions.

This collaboration aims to build a strong cybersecurity industry ecosystem through the development of an entrepreneur database, quality certification, business matching, and expanded market opportunities. The partnership will enhance competitiveness and drive the sustainable growth of Thailand's digital economy.

MOU กับ NIA สร้างระบบนิเวศไซเบอร์ไทยสู่มาตรฐานสากล

MOU with NIA to Build a Thai Cybersecurity Ecosystem Aligned with International Standards

ลงนามบันทึกความเข้าใจกับสำนักงานนวัตกรรมแห่งชาติ (NIA) เพื่อขับเคลื่อนนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์ของไทย เน้นการเชื่อมโยงองค์ความรู้ เทคโนโลยี และแหล่งทุนภาครัฐ สนับสนุนสตาร์ทอัพและผู้ประกอบการพัฒนาผลิตภัณฑ์ที่นำไปใช้จริงได้ สร้างระบบนิเวศนวัตกรรมไซเบอร์ และยกระดับขีดความสามารถในการแข่งขันของประเทศในระดับภูมิภาคและสากล

An MOU was signed with the National Innovation Agency (NIA) to advance cybersecurity innovation in Thailand. The collaboration emphasizes integration of knowledge, technology, and public-sector funding mechanisms to support startups and entrepreneurs in developing deployable cybersecurity products.

Thailand Cybersecurity Product and Service Awards 2024

ปลุกพลังไซเบอร์ไทย เปิดเวทีประชันนวัตกรรมผลิตภัณฑ์และบริการด้านความมั่นคงปลอดภัยไซเบอร์สุดยิ่งใหญ่ มีผู้ร่วมส่งผลงานรวมทั้งหมด 23 ผลงาน แบ่งเป็นประเภทผลิตภัณฑ์และบริการ 12 ผลงาน และประเภทต้นแบบผลิตภัณฑ์และบริการ 11 ผลงาน และมีผลงานที่ได้รับรางวัลทั้งสิ้น 9 ผลงาน เพื่อส่งเสริมให้ผู้ประกอบการ พัฒนาคุณภาพและประสิทธิภาพของผลิตภัณฑ์และบริการต่อไป

A national platform showcasing innovative cybersecurity products and services, with 23 submissions across product/service and prototype categories, and 9 award-winning entries-aimed at encouraging entrepreneurs to further enhance the quality and effectiveness of cybersecurity solutions.

หนุนงาน อว.Fair 2025 และ NST Fair 2025

Supporting MHESI FAIR 2025 and NST Fair 2025

เปิดบูธสร้างเครือข่ายนักวิจัย พร้อมกิจกรรมสร้างสรรค์การเรียนรู้ของครอบครัวผ่าน Cyber Boardgame ระหว่าง 9-17 สิงหาคม 2568

Hosted a booth to strengthen research networks and offered creative family learning activities through the NCSA Cyber Boardgame, held from 9-17 August 2025.

โครงการยกระดับภาคธุรกิจ SMEs เพื่อป้องกันและรับมือภัยคุกคามทางไซเบอร์ และคุ้มครองข้อมูลส่วนบุคคล
Cybersecurity Essentials for Entrepreneurs Project for Cyber Threat Protection and Personal Data Protection

เชิญชวนเข้าร่วมโครงการ : วันที่ 5 กุมภาพันธ์ 2568 ถ่ายทอดสดผ่าน Facebook NCSA Thailand และ Zoom เชิญผู้ประกอบการ SMEs เข้าร่วมโครงการ **“ยกระดับภาคธุรกิจเพื่อป้องกันและรับมือภัยคุกคามทางไซเบอร์”**

SMEs were invited to participate in the project on **“Cybersecurity Essentials for Entrepreneurs”**, launched on **5 February 2025**, via live broadcasts on Facebook NCSA Thailand and Zoom.

ฝึกอบรมออนไซต์เสริมศักยภาพ SMEs : กิจกรรมครั้งที่ 1 วันที่ 15 มีนาคม 2568 มุ่งสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล ปัจจุบันจัดแล้ว **3 รุ่น มีผู้เข้าร่วมจากภาคธุรกิจกว่า 1,406 คน**

SME Capacity-Building Training
- Activity 1: 15 March 2025
- Objective: Raise awareness of cybersecurity and personal data protection
- Currently implemented in **3 rounds.**
- Total participants: over **1,406 business operators**

ผนึกความร่วมมือภาคธุรกิจและการศึกษา : กิจกรรมครั้งที่ 2 วันที่ 29 มีนาคม 2568 ร่วมกับบริษัท ซีพี ซีดดิ้ง โซเชียลอิมแพคท์ จำกัด และมหาวิทยาลัยธรรมศาสตร์ ส่งเสริมความพร้อมด้านไซเบอร์ให้ SMEs ภายใต้แนวคิด “อยู่รอด-อยู่เป็น-อยู่เย็น-อยู่ยาว” เพื่อความยั่งยืนของธุรกิจ

Business and Academic Collaboration
- **Activity 2:** 29 March 2025
- Conducted in collaboration with CP Seeding Social Impact Co., Ltd. and **Thammasat University**
- Promoted cybersecurity awareness among SMEs under the concept: *“Stay Adaptable, Stay Sustainable”*
- Aimed at strengthening long-term business resilience and sustainability in the digital era

ความร่วมมือระหว่างประเทศ
International Cooperation

ส่งเสริมและบูรณาการความร่วมมือกับหน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์ของต่างประเทศ ทั้งระดับ **ทวิภาคีและพหุภาคี** เพื่อยกระดับความมั่นคงไซเบอร์และรับมือภัยคุกคามที่ซับซ้อนในระดับโลกอย่างมีประสิทธิภาพ

Thailand promotes and strengthens cooperation with cybersecurity agencies of other countries at both bilateral and multilateral levels, with the aim of reinforcing cyber resilience and enhancing preparedness to address increasingly complex global cyber threats in an effective and coordinated manner.

สรุปสถิติความร่วมมือระหว่างประเทศ (ปีงบประมาณ 2568)
Summary of International Cooperation Statistics (Fiscal Year 2025)

งานยุทธศาสตร์ความร่วมมือทวิภาคี
Bilateral Cooperation Activities

ประสานงาน/ร่วมมือกับต่างประเทศ
International Coordination and Joint Activities
จำนวน Total: **173** ครั้ง Activities

ประชุม/อบรม/สัมมนา
Meetings, Training, and Seminars
จำนวน Total: **72** ครั้ง Activities

พิจารณา/ให้ความเห็น/สนับสนุนข้อมูล
Consultations, Comments, and Information Support
จำนวน Total: **55** ครั้ง Activities

รวม Total Bilateral Activities: **300** ครั้ง Activities

งานยุทธศาสตร์ความร่วมมือพหุภาคี
Multilateral Cooperation Activities

ประสานงาน/ร่วมมือกับต่างประเทศ
International Coordination and Joint Activities
จำนวน Total: **329** ครั้ง Activities

ประชุม/อบรม/สัมมนา
Meetings, Training, and Seminars
จำนวน Total: **139** ครั้ง Activities

พิจารณา/ให้ความเห็น/สนับสนุนข้อมูล
Consultations, Comments, and Information Support
จำนวน Total: **132** ครั้ง Activities

รวม Total Multilateral Activities: **600** ครั้ง Activities

รวมทั้งสิ้น 900 ครั้ง
Overall Total: 900 International Cooperation Activities

ความร่วมมือในกรอบพหุภาคีที่สำคัญ
Key Multilateral Cooperation Frameworks

1 **งาน 9th Singapore International Cyber Week (SICW) 2024**

ระหว่างวันที่ 14-17 ตุลาคม 2567 พล.อ.ต. อมร ชมเชย เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในฐานะตัวแทนของประเทศไทย เข้าร่วมงาน Singapore International Cyber Week 2024 (SICW) การประชุมรัฐมนตรีอาเซียนด้านความมั่นคงปลอดภัยไซเบอร์ ครั้งที่ 9 (9th ASEAN Ministerial Conference on Cybersecurity: AMCC) และการประชุมอื่น ๆ ที่เกี่ยวข้อง ณ สาธารณรัฐสิงคโปร์ เพื่อแลกเปลี่ยนนโยบาย มาตรฐาน และความร่วมมือในการรับมือภัยคุกคามใหม่ ๆ รวมถึงประเด็น AI ในระดับภูมิภาคและระดับโลก

9th Singapore International Cyber Week 2024 (SICW)

From 14-17 October 2024, AVM Amorn Chomchoey, Secretary-General of the NCSC, represented Thailand at the 9th Singapore International Cyber Week (SICW), the 9th ASEAN Ministerial Conference on Cybersecurity (AMCC), and other related meetings in Singapore, to exchange views on policies, standards, and cooperation, including responses to emerging threats and artificial intelligence at both regional and global levels.

2 การประชุมอาเซียน-รัสเซีย ระหว่างวันที่ 24-25 ตุลาคม 2567

ระหว่างวันที่ 24-25 ตุลาคม 2567 พลตรี ธีรวุฒิ วิทยากรณ์ รองเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และนางอสิดา สุขสว่าง ผู้อำนวยการฝ่ายยุทธศาสตร์ความร่วมมือระหว่างประเทศ สำนักนโยบายยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ เข้าร่วมการประชุมหารือระหว่างอาเซียนกับรัสเซียในประเด็นที่เกี่ยวข้องกับความมั่นคงในการใช้เทคโนโลยีสารสนเทศและการสื่อสาร (ASEAN-Russia Dialogue on ICT Security-related Issues) ครั้งที่ 4 การประชุมระหว่างไทยและรัสเซียด้านความมั่นคงปลอดภัยสารสนเทศระหว่างประเทศ (Thailand-Russia Interagency Meeting in the Field of International Information Security: IIS) ครั้งที่ 2 และการประชุม International Cyber Security Conference Kuban CSC 2024 ณ เมืองโซชี สหพันธรัฐรัสเซีย เพื่อหารือความร่วมมือด้านไซเบอร์ และ ICT ในเวทีระหว่างประเทศ

ASEAN-Russia Engagement

From 24-25 October 2024, Maj. Gen. Teerawut Wittayakorn, Deputy Secretary-General of the NCSC, and Mrs. Asida Suksawang, Director of the International Affairs Division, Cybersecurity Policy and Strategy Office, participated in ASEAN-Russia meetings, including the ASEAN-Russia Dialogue on ICT Security-Related Issues, the Thailand-Russia Interagency Meeting in the Field of International Information Security (IIS), and the International Cyber Security Conference "Kuban CSC 2024" in Sochi, the Russian Federation, to strengthen cooperation in cybersecurity and ICT at the international level.

3 การอบรม Cybersecurity Capacity Building Programme

ระหว่างวันที่ 19-23 พฤศจิกายน 2568 สกมช. ร่วมกับ UNIDIR โดยการสนับสนุนจากรัฐบาลแคนาดา จัดอบรม Cybersecurity Capacity Building Programme ณ United Nations Conference Centre (UNCC), UNESCAP ถนนราชดำเนินนอก กรุงเทพฯ เพื่อยกระดับศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ภาครัฐ โครงสร้างพื้นฐานสำคัญ ภาควิชาการ ภาคเอกชน และผู้มีส่วนเกี่ยวข้อง

Cybersecurity Capacity Building Programme

From 19-23 November 2025, the NCSA, in collaboration with UNIDIR and with the support of the Government of Canada, organized the Cybersecurity Capacity Building Programme at the United Nations Conference Centre (UNCC), UNESCAP, Bangkok. The programme aimed to enhance cybersecurity capabilities for government agencies, critical information infrastructure organizations, academia, the private sector, and other relevant stakeholders.

4 การประชุม ANSAC ครั้งที่ 16

ระหว่างวันที่ 9-12 มิถุนายน 2568 ผศ.ดร. วราภรณ์ พรหมวิกรณ์ ผู้ช่วยเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หัวหน้าคณะผู้แทนไทย พร้อมด้วย นาวาอากาศเอก ธวัชชัย มากพานิช ผู้อำนวยการสำนักงานนโยบายยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ เข้าร่วมการประชุมสภาปฏิบัติการอาเซียนด้านความมั่นคงปลอดภัยบนเครือข่าย (ASEAN Network Security Action Council: ANSAC) ครั้งที่ 16 และการประชุมเชิงปฏิบัติการเพื่อจัดทำยุทธศาสตร์ความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ของอาเซียน ค.ศ. 2026-2030 (ASEAN Cybersecurity Cooperation Strategy Workshop: ACCS) ณ เมืองเสียมราฐ ราชอาณาจักรกัมพูชา เพื่อติดตามความคืบหน้าของกิจกรรมและโครงการต่าง ๆ ในภูมิภาค

16th ANSAC Meeting

From 9-12 June 2025, Asst. Prof. Waraporn Promwikorn, Ph.D., Assistant Secretary-General of the NCSC, together with Air Vice Marshal Tawatchai Makpanich, Director of the Cybersecurity Policy and Strategy Office, participated in the 16th Meeting of the ASEAN Network Security Action Council (ANSAC) and the ASEAN Cybersecurity Cooperation Strategy (ACCS) Workshop for 2026-2030, held in Siem Reap, Kingdom of Cambodia.

5 การประชุม OEWG on security of and in the use of ICTs

ระหว่างวันที่ 7-11 กรกฎาคม 2568 ผศ.ดร. วราภรณ์ พรหมวิกรณ์ ผู้ช่วยเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ทำหน้าที่หัวหน้าคณะผู้แทนไทย เข้าร่วมการประชุมสมัยที่ 11 (Substantive Session) ของคณะทำงานแบบเปิด (Open-Ended Working Group: OEWG) ว่าด้วยความมั่นคงของและในการใช้เทคโนโลยีสารสนเทศและการสื่อสาร ณ สำนักงานใหญ่สหประชาชาติ นครนิวยอร์ก สหรัฐอเมริกา เพื่อพิจารณารายงานและหารือแนวทางเสริมสร้างความร่วมมือระหว่างประเทศด้านความมั่นคงไซเบอร์

OEWG on Security of and in the Use of ICTs

From 7-11 July 2025, Asst. Prof. Waraporn Promwikorn, Ph.D., Assistant Secretary-General of the NCSC, served as Head of the Thai Delegation to the 11th substantive session of the Open-Ended Working Group (OEWG) on security of and in the use of ICTs at the United Nations Headquarters in New York, United States of America. The session considered reports and discussed approaches to strengthening international cooperation in cybersecurity.

ความร่วมมือในกรอบทวิภาคีที่สำคัญ
Key Bilateral Cooperation Frameworks

1 ต้อนรับคณะ LaoCERT แลกเปลี่ยนความร่วมมือด้านไซเบอร์

วันที่ 20 มกราคม 2568 สกมช. ต้อนรับคณะผู้แทน LaoCERT และแลกเปลี่ยนการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของไทย โดยนำเสนอแนวทางของ ThaiCERT โครงสร้างการจัดการภัยคุกคาม และกลไกประสานงานระดับประเทศ พร้อมหารือความร่วมมือในอนาคต โดยเฉพาะการแลกเปลี่ยนข้อมูลภัยคุกคามในระดับภูมิภาค

Welcoming LaoCERT and Enhancing Cybersecurity Cooperation

On 20 January 2025, the NCSA welcomed a delegation from LaoCERT to exchange experiences on cybersecurity operations. The meeting included presentations on Thailand's cybersecurity governance framework, the ThaiCERT threat management structure, and national-level coordination mechanisms. Both sides also discussed future cooperation, particularly the exchange of cyber threat information at the regional level.

2 ต้อนรับคณะ ITU, JICA และหน่วยงานจากภูฏาน

วันที่ 4 กุมภาพันธ์ 2568 สกมช. ต้อนรับคณะผู้แทนจากสหภาพโทรคมนาคมระหว่างประเทศ (ITU) องค์การความร่วมมือระหว่างประเทศของญี่ปุ่น (JICA) และหน่วยงานภาครัฐจากประเทศภูฏาน เพื่อแลกเปลี่ยนองค์ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ โดยนำเสนอภารกิจของ สกมช. และ ThaiCERT การทำงานของศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ แนวทางรับมือเหตุการณ์ไซเบอร์ และบทเรียนจากกรณีศึกษา รวมถึงการพัฒนาความร่วมมือด้านข่าวกรองและบุคลากร

Welcoming Delegations from ITU, JICA, and Bhutan

On 4 February 2025, the NCSA welcomed delegations from the International Telecommunication Union (ITU), the Japan International Cooperation Agency (JICA), and relevant government agencies from Bhutan to exchange knowledge on cybersecurity. The programme included presentations on the NCSA's mandate, ThaiCERT operations, the Cybersecurity Operations Center, cyber incident response approaches, and lessons learned from case studies. Discussions also explored opportunities for future cooperation, particularly in cyber threat intelligence and workforce development.

3 การเสริมศักยภาพบุคลากรด้านการทูตไซเบอร์

ระหว่างวันที่ 24 กรกฎาคม 2568 ผู้แทน สกมช. เข้าร่วมการฝึกอบรมด้านการทูตไซเบอร์ (Cyber Diplomacy) ณ สถาบันการต่างประเทศเทวะวงศ์วโรปการ จัดโดยกระทรวงการต่างประเทศ ร่วมกับ Clingendael Academy สถาบันฝึกอบรมด้านการทูตชั้นนำของเนเธอร์แลนด์ เพื่อพัฒนาขีดความสามารถด้านความร่วมมือระหว่างประเทศ เสริมสร้างความเข้าใจบรรทัดฐานและหลักการสากลในมิติไซเบอร์

Enhancing Capacity in Cyber Diplomacy

From 2 to 4 July 2025, representatives of the NCSA participated in a Cyber Diplomacy training programme hosted by the Ministry of Foreign Affairs of Thailand in collaboration with the Clingendael Academy of the Netherlands. The programme aimed to strengthen participants' capacities in international cybersecurity policy, negotiation, and engagement, with an emphasis on global norms and principles in cyberspace.

4 การหารือร่วมกับเอกอัครราชทูตบังกลาเทศส่งเสริมความร่วมมือไซเบอร์

วันที่ 25 กรกฎาคม 2568 สกมช. ต้อนรับเอกอัครราชทูตบังกลาเทศประจำประเทศไทย เพื่อหารือประเด็นความมั่นคงปลอดภัยไซเบอร์ในบริบทการป้องกันประเทศ

Courtesy Call by the Ambassador of Bangladesh

On 25 July 2025, the NCSA received a courtesy call from the Ambassador of Bangladesh to Thailand. The discussion focused on cybersecurity cooperation and national approaches to cyber defence, with an exchange of views on strengthening preventive measures and advancing collaboration between the two countries.

5 การประชุมเชิงปฏิบัติการร่วมกับอิสราเอล

ระหว่างวันที่ 5-7 สิงหาคม 2568 สกมช. ร่วมกับสถานเอกอัครราชทูตอิสราเอลประจำประเทศไทย จัดประชุมเชิงปฏิบัติการ The 1st Thailand-Israel Cybersecurity Workshop ณ กรุงเทพมหานคร เพื่อเสริมสร้างศักยภาพและความเข้าใจด้านความมั่นคงปลอดภัยไซเบอร์แก่หน่วยงานภาครัฐและภาคเอกชนของไทย โดยได้รับการถ่ายทอดองค์ความรู้และประสบการณ์จากผู้เชี่ยวชาญด้านความมั่นคงไซเบอร์ของอิสราเอล ซึ่งสามารถนำไปประยุกต์ใช้ในการป้องกันและรับมือภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพ

Thailand-Israel Cybersecurity Workshop

From 5-7 August 2025, the NCSA, in collaboration with the Embassy of Israel in Thailand, organized the 1st Thailand-Israel Cybersecurity Workshop in Bangkok. The workshop aimed to enhance capacity and deepen understanding of cybersecurity among Thai public and private sector organizations. The programme featured knowledge sharing and practical experience delivered by Israel's cybersecurity experts, with discussions on applying best practices to strengthen Thailand's capabilities in preventing and responding to cyber threats effectively.

Thailand International Cyber Week 2025

ร่วมกับ VNU Asia Pacific จัดงาน **Thailand International Cyber Week 2025 คู่ขนานกับ Cybersec Asia 2025** เปิดเวทีความร่วมมือระหว่างภาครัฐ เอกชน การศึกษา และพันธมิตรต่างประเทศ เพื่อแลกเปลี่ยนความรู้ เทคโนโลยี และแนวทางพัฒนาด้านความมั่นคงไซเบอร์

ภายในงาน ประกอบด้วยการสัมมนาวิชาการ การจัดแสดงนวัตกรรม การแข่งขัน CTF และการจับคู่ทางธุรกิจ ให้ผู้ประกอบการไทยเชื่อมโยงกับพันธมิตรต่างชาติ มุ่งขยายความร่วมมือระหว่างประเทศ เสริมภาพลักษณ์ไทยในฐานะผู้นำด้านความมั่นคงปลอดภัยไซเบอร์ของภูมิภาค และสนับสนุนการเติบโตของเศรษฐกิจดิจิทัลอย่างมั่นคงและยั่งยืน

In collaboration with **VNU Asia Pacific,** Thailand will host **Thailand International Cyber Week 2025**, co-located with **Cybersec Asia 2025,** serving as a platform for collaboration among the public sector, private sector, educational institutions, and international partners to exchange knowledge, technologies, and development directions in cybersecurity.

The event will feature academic seminars, innovation exhibitions, Capture the Flag (CTF) competitions, and business matching activities, enabling Thai cybersecurity operators to connect with international partners. The initiative aims to expand international cooperation, enhance Thailand's image as a regional cybersecurity leader, and support the sustainable growth of the digital economy.

- **เป้าหมายผู้เข้าร่วมอบรม : 120 คน**
  Target number of participants: **120 persons**
- **ผลการดำเนินงานจริง : 1,474 คน**
  Actual number of participants: **1,474 persons**
- **เกินเป้าหมาย : 1,128%**
  Achievement rate: **1,128%**

ASEAN-Japan Cybersecurity Capacity Building Centre

ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) เป็นศูนย์กลางฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ ระดับภูมิภาคอาเซียนภายใต้ความร่วมมือระหว่างอาเซียนกับญี่ปุ่น มีบทบาทสำคัญในการพัฒนาบุคลากรให้สามารถรับมือภัยคุกคามดิจิทัลที่ซับซ้อนยิ่งขึ้น

ปีนี้ถือเป็นปีแห่งความสำเร็จที่โดดเด่นของ AJCCBC ในการขยายผลและตอบสนองต่อความต้องการของผู้เข้าร่วมได้มากกว่าที่คาดการณ์ สะท้อนให้เห็นถึงศักยภาพและความสำคัญของการฝึกอบรมด้านไซเบอร์ในภูมิภาคอาเซียน

The **ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC)** serves as a regional training hub for cybersecurity capacity building and acts as a key mechanism for strengthening cooperation between ASEAN Member States and Japan. The Centre plays a vital role in developing cybersecurity professionals capable of addressing increasingly complex digital threats.

This year marks a significant milestone for AJCCBC, demonstrating outstanding achievements in expanding training programmes and responding to growing demand from participants beyond initial targets. The outcomes reflect the Centre's strong potential and the critical importance of cybersecurity training in the ASEAN region.

สร้างบริการภาครัฐ
และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้มีความมั่นคงปลอดภัยไซเบอร์ และฟื้นคืนสู่สภาพปกติได้ (RESILIENCE)

BUILDING GOVERNMENT SERVICES AND CRITICAL INFORMATION INFRASTRUCTURE WITH CYBERSECURITY AND RESILIENCE

มุ่งเน้นกำหนดมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ ปกป้องระบบข้อมูลและเครือข่ายของหน่วยงานภาครัฐ ส่งเสริมความพร้อมในการฟื้นคืนระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศและระบบบริการภาครัฐ ให้กลับสู่สภาพปกติได้อย่างรวดเร็ว ปลอดภัย และทันเวลา

Focusing on establishing cybersecurity protection measures to safeguard data systems and networks of government agencies, while enhancing preparedness for the recovery of critical information infrastructure and public service systems. This aims to ensure a rapid, secure, and timely return to normal operations following cyber incidents.

กำหนดมาตรการการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
Establishing Minimum Cybersecurity Measures for Organizations of Critical Information Infrastructure (CII)

สร้างความตระหนักรู้ให้บุคลากรทุกระดับ เกี่ยวกับบทบาทสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ระบบสารสนเทศที่สำคัญของประเทศมั่นคงปลอดภัยและพร้อมรับมือภัยคุกคาม

Raising awareness among personnel at all levels regarding their critical roles in maintaining cybersecurity, to ensure that the nation's critical information systems remain secure and resilient against cyber threats.

LEAD IMPLEMENTER & LEAD AUDITOR

เดินหน้าพัฒนาขีดความสามารถกระบวนการปฏิบัติงานด้านไซเบอร์ตามมาตรฐานสากลของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานของรัฐอย่างต่อเนื่อง

Continuously developing operational capabilities and competencies in cybersecurity in accordance with international standards for organizations of critical information infrastructure, supervisory or regulatory agencies, and government entities.

- **เป้าหมาย : ผู้เข้าอบรม 150 คน**
  Target number of trainees: 150 persons
- **ผู้เข้าร่วมอบรมจริง : 255 คน**
  Actual participants: 255 persons
- **สูงกว่าเป้าหมาย 70%**
  Exceeded target by: 70%

ปกป้องระบบข้อมูลและเครือข่ายของหน่วยงานภาครัฐ
Protection of Government Data and Networks

กำหนดมาตรฐานความมั่นคงปลอดภัย ประเมินความเสี่ยงตั้งแต่เริ่มใช้เทคโนโลยี และบูรณาการบุคลากร ข้อมูล ระบบ และกระบวนการ เพื่อรับมือภัยคุกคามไซเบอร์อย่างมีประสิทธิภาพ

Establish cybersecurity standards and conduct risk assessments from the early stages of technology adoption, integrating people, data, systems, and processes to ensure effective protection against cyber threats.

จัดกิจกรรมประเมินความเสี่ยงต่อภัยคุกคามไซเบอร์
Cyber Risk Assessment Activities

จัดงาน **Cyber Security Forum 4/2025: Risk & Self-Assessment** เมื่อวันที่ **30 กันยายน 2568** เพื่อศึกษา วิเคราะห์ และประเมินความเสี่ยงภัยคุกคามไซเบอร์ทั้งในระดับประเทศและระดับกลุ่มหน่วยงาน

Organized the **Cyber Security Forum 4/2025: Risk & Self-Assessment** on **30 September 2025,** to study, analyze, and assess cybersecurity risks at both the national level and across groups of agencies.

- เพื่อนำไปพิจารณากำหนดนโยบาย และมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ
  To support the formulation of national cybersecurity policies and protection measures
- เพื่อนำไปกำหนดแนวทางและมาตรการลดความเสี่ยงระดับกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานรัฐ
  To define guidelines and risk-reduction measures for Critical Information Infrastructure (CII) and government agencies

มีผู้เข้าร่วมจำนวน 221 คน
Number of participants: 221 persons

จัดทำมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์
Development of Cybersecurity Standards for Websites

จัดทำมาตรฐานขั้นต่ำเพื่อคุ้มครองความมั่นคงปลอดภัยของเว็บไซต์หน่วยงานรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญ รวมถึงหน่วยงานเอกชนตาม **พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562** ครอบคลุมเว็บไซต์ที่เชื่อมต่ออินเทอร์เน็ต เว็บไซต์ที่มีข้อมูลสำคัญ เว็บไซต์บริการประชาชน เว็บไซต์ให้บริการเกี่ยวกับโครงสร้างพื้นฐานสำคัญของประเทศ และธุรกรรมทางอิเล็กทรอนิกส์ ทั้งบนระบบองค์กร ระบบคลาวด์ และเว็บโฮสติ้ง

Developed baseline cybersecurity standards to protect websites of government agencies, supervisory or regulatory authorities, and organizations of critical information infrastructure, as well as relevant private-sector entities, in accordance with the Cybersecurity Act B.E. 2562 (2019). The standards cover: Internet-connected websites, websites containing sensitive information, public service websites, websites providing services related to critical information infrastructure, and apply to organizational systems, cloud systems, and web hosting environments.

แนวปฏิบัติการใช้ AI อย่างปลอดภัย
AI Security Guidelines

จัดทำกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับ AI ที่สามารถนำไปใช้ได้จริงในบริบทของประเทศไทย มุ่งเสริมสร้างการพัฒนาและการใช้งาน AI อย่างมั่นคงปลอดภัย มีความรับผิดชอบ สอดคล้องกับหลักธรรมาภิบาลและกฎหมายที่เกี่ยวข้อง โดยผ่านการรับฟังความคิดเห็นจากภาคส่วนที่เกี่ยวข้องอย่างรอบด้าน เพื่อให้แนวปฏิบัตินี้สามารถเสริมสร้างความมั่นคงปลอดภัยในการพัฒนาและการใช้งาน AI ได้อย่างมีประสิทธิภาพ

Developed an operational framework for cybersecurity in relation to AI that can be practically applied within the Thai context, promoting the development and use of AI that is secure, responsible, and aligned with ethical principles and relevant laws.

The guideline was developed through comprehensive stakeholder consultations to ensure that it effectively strengthens the secure development and use of AI.

กรอบการทำงานด้านการรักษาความปลอดภัยไซเบอร์ระบบคลาวด์
National Cloud Security Framework

จัดทำกรอบการทำงานด้าน Cloud Security ของประเทศไทย เพื่อยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ ทั้งในส่วนของผู้ใช้บริการคลาวด์ (Cloud Service Customer) และผู้ให้บริการคลาวด์ (Cloud Service Provider) รวมถึงการบูรณาการการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ระหว่าง สกมช. กับหน่วยงานที่เกี่ยวข้อง

To develop a National Cloud Security Framework for Thailand to enhance cybersecurity for cloud computing systems, covering both Cloud Service Customers (CSCs) and Cloud Service Providers (CSPs), as well as to strengthen the integration and coordination of cloud cybersecurity operations between the National Cyber Security Agency (NCSA) and relevant stakeholders.

กรอบแนวทางการทำงานเตรียมความพร้อม Operational Preparedness Framework

1. **กำหนดความต้องการและเกณฑ์ร่วมกันจำแนกข้อมูล** แบ่งความรับผิดชอบ (Shared Responsibility) และกำหนดคุณสมบัติผู้ตรวจสอบ
   Establish shared requirements and criteria for data classification define the Shared Responsibility Model, and specify qualifications for auditors and assessors.
2. **จัดลำดับความสำคัญ (Prioritize)** รวบรวมความเห็นและสื่อสารแนวทางให้ผู้บริหารและหน่วยงานที่เกี่ยวข้องเข้าใจตรงกัน
   Prioritize key issues, consolidate feedback, and communicate the agreed approach to executives and relevant agencies to ensure a common understanding
3. **วางแผนยุทธศาสตร์บูรณาการ 5 ปี** เน้นดึงผู้เชี่ยวชาญร่วมทำกฎหมายสร้างระบบตรวจรับรองและพัฒนาบุคลากรผ่าน NCSA Cyber Clinic
   Develop a five-year integrated strategy, emphasizing collaboration with subject-matter experts in legal development, establishing certification and assessment systems, and strengthening workforce capacity through the NCSA Cyber Clinic.
4. **ดำเนินการภายใต้ Cloud First Policy** ตั้งทีมเฉพาะกิจเพื่อขับเคลื่อนการปฏิบัติงานและเร่งแก้ไขอุปสรรคอย่างจริงจัง
   Execute initiatives in alignment with the Cloud First Policy by establishing dedicated task forces to drive implementation and proactively resolve operational barriers.
5. **ประเมินผลและปรับปรุงต่อเนื่อง** ติดตามผลใกล้ชิดและแจ้งเวียนการเปลี่ยนแปลงผ่านแพลตฟอร์มกลางให้ทุกหน่วยงานทราบ
   Conduct continuous monitoring and evaluation, closely track progress, and disseminate updates and changes through a centralized platform to ensure all agencies remain informed.

สร้างศักยภาพของหน่วยงานระดับชาติ ให้มีคุณภาพและมาตรฐาน (STANDARDS)

STRENGTHENING THE CAPACITY OF NATIONAL-LEVEL AGENCIES to Ensure Quality and Standards

มุ่งยกระดับศักยภาพหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐานสากล โดยเสริมขีดความสามารถในการป้องกัน รับมือ และตอบสนองต่อภัยคุกคามทางไซเบอร์ ควบคู่การส่งเสริมการแบ่งปันข้อมูลภัยคุกคามและการบูรณาการความร่วมมือ เพื่อสร้างระบบความมั่นคงปลอดภัยไซเบอร์ที่เข้มแข็ง ยั่งยืน และเชื่อถือได้

This initiative aims to enhance the capacity of national-level agencies to meet international quality and standard requirements by strengthening their ability to prevent, respond to, and recover from cybersecurity threats. It also promotes threat information sharing and integrated cooperation to build a robust, sustainable, and trusted national cybersecurity ecosystem.

เพิ่มขีดความสามารถในการรับมือและตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
Enhancing Cybersecurity Incident Response and Resilience Capabilities.

ยกระดับการรับมือและตอบสนองภัยไซเบอร์ พัฒนานโยบาย คน กระบวนการ และเทคโนโลยีให้ได้มาตรฐาน พร้อมสนับสนุนที่มี CERT และแผนฉุกเฉินเพื่อเสริมความมั่นคงของโครงสร้างพื้นฐาน

To strengthen national cyber incident response and resilience, policies, personnel, processes, and technologies are developed in accordance with recognized standards. This includes supporting CERT operations and emergency response planning to reinforce the security of critical information infrastructure.

จัดทำแผนแม่บท ICT และ Enterprise Architecture และปรับปรุงระบบเทคโนโลยีสารสนเทศสำนักงาน
Development of the ICT Master Plan and Enterprise Architecture

ในปีงบประมาณ 2568 ได้จัดทำแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร ICT Masterplan และสถาปัตยกรรมองค์กร (Enterprise Architecture) ระยะ 5 ปี พ.ศ.2566-2570 เรียบร้อยแล้ว

In fiscal year 2025, the Office completed the **ICT Master Plan and Enterprise Architecture (EA)** with a five-year implementation framework (2023-2027), providing a clear roadmap for technology and organizational development.

ปรับปรุงระบบเทคโนโลยีสารสนเทศสำนักงาน โดยได้มีการเตรียมการเพื่อดำเนินการหลังได้รับงบประมาณในปีงบประมาณถัดไป

Upgrading Internal Information Technology Systems: Information technology systems of the Office are being upgraded, with preparatory work completed to support implementation following budget allocation in the next fiscal year.

พัฒนาระบบ Smart Back Office ให้สามารถสนับสนุนงานหลักได้ทุกกระบวนงาน
Development of a Smart Back Office System to Support Core Operations

ติดตั้งระบบบริหารจัดการทรัพยากรองค์กร (Enterprise Resource Planning: ERP) และใช้งานเต็มรูปแบบแล้วตั้งแต่เดือนเมษายน 2568 เป็นต้นมา

The Office has implemented an **Enterprise Resource Planning (ERP)** system to enhance organizational resource management. The system has been fully operational since April 2025 and supports core administrative and operational processes.

ยกระดับการให้บริการประชาชน ย้ายสำนักงานสู่ศูนย์ราชการโซนซี
Enhancing Public Service Delivery and Relocating the Office to the Government Complex, Zone C

ดำเนินโครงการย้ายที่ตั้งสำนักงานไปยังศูนย์ราชการเฉลิมพระเกียรติฯ โซนซี ภายใต้โครงการพัฒนาพื้นที่ส่วนขยายของบริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.) ซึ่งคณะรัฐมนตรีมีมติอนุมัติตั้งแต่ปี 2561 เพื่อเพิ่มประสิทธิภาพการให้บริการแก่ประชาชน ลดภาระงบประมาณการเช่าสำนักงานของหน่วยงานภาครัฐ และใช้ประโยชน์พื้นที่ศูนย์ราชการอย่างเต็มศักยภาพ

ทั้งนี้ สกมช. ได้รับการจัดสรรพื้นที่ในปีงบประมาณ 2567 และดำเนินการปรับปรุงอาคาร ระบบเทคโนโลยีสารสนเทศ และระบบสนับสนุนสำนักงาน ให้สอดคล้องกับโครงสร้างองค์กรและจำนวนบุคลากร เพื่อรองรับการปฏิบัติงานอย่างต่อเนื่อง โดยเริ่มปฏิบัติงาน ณ ที่ทำการใหม่ตั้งแต่วันที่ 1 กรกฎาคม 2568 เป็นต้นมา

The project involves relocating the NCSA headquarters to the Government Complex, Zone C, under the area expansion development project of Dhanarak Asset Development Co., Ltd. (DAD). The Cabinet approved the project in 2018 (B.E. 2561) with the objective of enhancing service efficiency, reducing rental expenses for office buildings, and maximizing the utilization of government complex facilities.

In fiscal year 2024 (B.E. 2567), NCSA was allocated office space and budget to renovate office facilities, information technology systems, and back-office systems to align with the organizational structure and staffing requirements. Operational activities at the new location officially commenced on 1 July 2025 (B.E. 2568), ensuring continuity and efficiency in service delivery.

พัฒนาระบบสนับสนุนการเผชิญเหตุภัยคุกคามทางไซเบอร์แบบเคลื่อนที่เร็ว
Development of a Rapid Cyber Incident Response Capability (Cyber Mobile Response Team)

ThaiCERT สนับสนุนหน่วยงานภาครัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศในการให้การช่วยเหลือแนะนำ สนับสนุนการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น โดยดำเนินกระบวนการทางนิติวิทยาศาสตร์ การตรวจพิสูจน์พยานหลักฐานทางดิจิทัล รวมถึงสนับสนุนการฟื้นฟูเพื่อให้หน่วยงานสามารถกลับมาดำเนินภารกิจหรือให้บริการได้ต่อไปตามมาตรฐานสากล

บริการสำคัญคือ **"รถตู้ปฏิบัติการสนับสนุนการเผชิญเหตุภัยคุกคามทางไซเบอร์แบบเคลื่อนที่เร็ว"** สนับสนุนปฏิบัติงานภาคสนาม พร้อมทีมผู้เชี่ยวชาญและอุปกรณ์ด้านความมั่นคงไซเบอร์ สำหรับวิเคราะห์ ควบคุมสถานการณ์ และเก็บพยานหลักฐานทางนิติวิทยาศาสตร์ตลอดจนสนับสนุนการตรวจพิสูจน์ทางดิจิทัล

ThaiCERT, under NCSA, provides support to government agencies and organizations of critical information infrastructure (CII) by offering assistance, guidance, and technical support in responding to and mitigating cybersecurity incidents. This includes incident response operations based on scientific methodologies, digital forensic investigations, evidence examination, and recovery support, enabling affected agencies to resume operations or public services in accordance with international standards.

A key service is the **Cyber Mobile Response Team**, which delivers rapid, on-site cyber incident response support. The team comprises cybersecurity experts and specialized equipment to analyze, contain, and manage cyber incidents, collect and preserve digital evidence, and support digital forensic investigations throughout the response lifecycle.

สร้างสังคมดิจิทัลที่ปลอดภัย ด้วยพลังการสื่อสาร
Building a Safe Digital Society through Strategic Communication

ขับเคลื่อนงานสื่อสารองค์กรอย่างเป็นระบบ เพื่อยกระดับความรู้และความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ให้ประชาชนทุกกลุ่ม โดยมุ่งให้ Cybersecurity เป็นเรื่องใกล้ตัว เข้าใจง่าย และนำไปใช้ป้องกันตนเองได้จริง

NCSA continues to strengthen its organizational communication mission to enhance public knowledge, understanding, and awareness of cybersecurity across all population groups. The goal is to make **"Cybersecurity a relatable issue that everyone can understand and protect themselves against."**

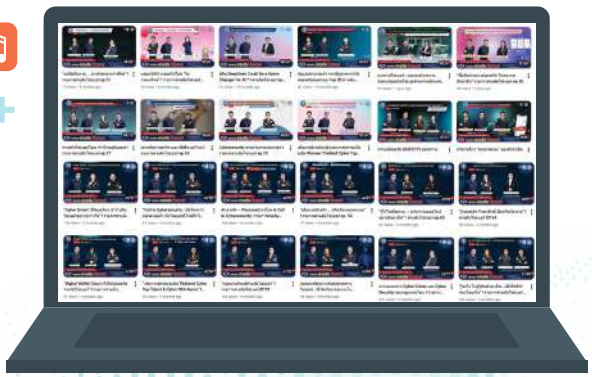
"สื่อออนไลน์" ศูนย์กลางข้อมูลไซเบอร์ที่ประชาชนเชื่อถือ ช่องทาง **NCSA Thailand บน Facebook** เติบโตอย่างต่อเนื่อง **มียอดผู้ติดตามทะลุ 60,000 คน** เป็นแหล่งข้อมูลที่ประชาชนไว้วางใจและเข้ามาอัปเดตข่าวสารทุกวัน ไม่ว่าจะเป็นการแจ้งเตือนภัยไซเบอร์ การให้ความรู้เชิงป้องกัน หรือการสื่อสารสถานการณ์สำคัญที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ของประเทศ

"Online Media" - A Trusted Cyber Information Hub for the Public
The **NCSA Thailand Facebook page** continues to grow steadily, with **over 60,000** followers, serving as a trusted source of information for the public. The platform regularly disseminates cybersecurity alerts, preventive knowledge, and key communications related to national cybersecurity situations, helping citizens stay informed and vigilant.

"สื่อโทรทัศน์" ถ่ายทอดภัยใกล้ตัว เข้าใจง่าย ใช้ได้จริง ผลิตรายการมากกว่า 18 ตอน นำเสนอประเด็นภัยไซเบอร์ที่ประชาชนอาจเผชิญในชีวิตประจำวัน เช่น การหลอกลวงออนไลน์ในรูปแบบต่าง ๆ และเทคนิคการป้องกันตนเองจากภัยไซเบอร์ **เข้าถึงผู้ชมรวมกว่า 200,000 คน**

"Television Media" - Cyber Threats Explained Simply and Practically
More than **18 television episodes** were produced, addressing cyber threats commonly encountered in daily life, such as various forms of online fraud, along with practical self-protection techniques. These programs reached over 200,000 viewers, enhancing public awareness and digital safety literacy.

"สื่อวิทยุ" เสียงแห่ง Cyber Safety ที่เข้าถึงทุกพื้นที่ รายการวิทยุ **"สายลับไซเบอร์"** ออกอากาศประจำวันอาทิตย์ตลอดทั้งปี **รวมกว่า 50 ตอน มียอดรับฟังมากกว่า 160,000 ครั้ง** ทำหน้าที่เป็นสื่อกลางถ่ายทอดสาระด้านความมั่นคงปลอดภัยไซเบอร์เพื่อสร้างความตระหนักรู้ให้ประชาชนในวงกว้าง โดยเฉพาะในพื้นที่ที่การเข้าถึงสื่อดิจิทัลยังมีข้อจำกัด



"Radio Media" - The Voice of Cyber Safety Reaching Every Community
The radio program **"Cyber Safety Hotline"** aired weekly throughout the year, totaling over 50 episodes, with more than **160,000 listening sessions.** The program serves as a key channel for communicating cybersecurity awareness nationwide, particularly in areas with limited access to digital media.

ดำเนิน “กิจกรรมเพื่อสังคม (CSR)” ปลูกฝังความรู้ไซเบอร์ตั้งแต่วัยเยาว์ จำนวน 4 ครั้ง ในปี 2568

Corporate Social Responsibility Activities (CSR): Cultivating Cyber Awareness from a Young Age

Total: 4 activities in Fiscal Year 2025 (B.E. 2568)

1

ThaiPBS Kids Day 2568 - “สกมช. เสริมเกราะป้องกันภัยไซเบอร์ให้น้อง ๆ” ณ องค์การกระจายเสียงและแพร่ภาพสาธารณะแห่งประเทศไทย (ThaiPBS)

ThaiPBS Kids Day 2025 - “NCSA Strengthens Cyber Protection for Children”: Held at the **Thai Public Broadcasting Service (ThaiPBS)**, focusing on child-friendly cyber safety education.

2

กิจกรรม **“รู้ รอด ปลอดภัย ท่องโลกไซเบอร์อย่างมั่นใจ”** ณ โรงเรียนระยองวิทยาคม

“Learn Smart, Travel the Cyber World Safely” Activity: Conducted at **Rayongwittayakom School**, promoting safe and confident internet use among students.

3

กิจกรรม **“รู้คิด รู้เท่าทัน ภัยไซเบอร์”** ณ โรงเรียนอนุบาลสุขสวัสดิ์

“Think Before You Click: Cyber Awareness” Activity: Held at **Anuban Suksawat School**, introducing basic cyber safety concepts for young children.

4

กิจกรรม **“ไซเบอร์ฮีโร่ ผจญภัยในโลกออนไลน์อย่างปลอดภัย”** ณ โรงเรียนพหลโยธิน (พ่วงเจริญอุปถัมภ์)

“Cyber Heroes: Staying Safe in the Online World” Activity: Organized at **Phahon Yothin School (Puang Charoen Upatham School)**, fostering awareness of online risks and safe digital behavior.

ส่งเสริมความร่วมมือในประชาคมไซเบอร์
Promoting Collaboration within the Cyber Community

ส่งเสริมความร่วมมือระหว่างหน่วยงานในประชาคมไซเบอร์ ดำเนินการจัดกิจกรรมประชาคมไซเบอร์รวม 4 ครั้ง เพื่อ **พัฒนาคน ระบบ และนโยบาย**ด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นรูปธรรม

A total of four cyber community forums were organized to support the development of **people, systems, and policies** in the field of cybersecurity in a concrete and sustainable manner.

ครั้งที่ 1

"สร้างคน สร้างงาน สร้างชาติ สร้างโลกไซเบอร์และความมั่นคงปลอดภัยไซเบอร์ เพื่อการเป็นพลเมืองดิจิทัล"

มุ่งปูพื้นฐานกำลังคนไซเบอร์ให้สอดคล้องตลาดแรงงานอนาคต เชื่อมโยงนโยบายพัฒนาฝีมือแรงงานกับหลักสูตรอาชีวศึกษา สาขานักปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พร้อมเวทีเสวนาและเวิร์กชอปเสริมทักษะพลเมืองดิจิทัลและการรับมือภัยออนไลน์

Forum 1
"Building People, Creating Jobs, Strengthening the Nation: Cybersecurity and Cyber Safety for a Digital Workforce"
This forum focused on strengthening the foundations of the cybersecurity workforce to align with future labor market demands, linking workforce development policies with vocational education curricula in cybersecurity operations. The forum also addressed guidelines and mechanisms to enhance digital citizenship skills and online threat resilience.

ครั้งที่ 2

"พนักงานเจ้าหน้าที่ ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กับบทบาทการรับมือภัยคุกคามทางไซเบอร์ระดับโลก"

เน้นสร้างความเข้าใจบทบาท หน้าที่ และกลไกการปฏิบัติงานของพนักงานเจ้าหน้าที่ การเฝ้าระวังและตอบสนองเหตุไซเบอร์ พร้อมแลกเปลี่ยนองค์ความรู้จากผู้เชี่ยวชาญ

Forum 2
"Government Officials under the Cybersecurity Act B.E. 2562 and Their Roles in Responding to Global Cyber Threats"
This forum aimed to enhance understanding of the **roles, responsibilities, and operational mechanisms** of government officials under the Cybersecurity Act B.E. 2562, with emphasis on cyber threat monitoring, incident response, and knowledge exchange with cybersecurity experts.

ครั้งที่ 3

"การสัมมนาและรับฟังความคิดเห็นเพื่อจัดทำแผนการส่งเสริมอุตสาหกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์"

เป็นเวทีระดมความเห็นจากภาครัฐ เอกชน สถาบันวิจัย และผู้ประกอบการด้านไซเบอร์ เพื่อออกแบบแนวทางขับเคลื่อนอุตสาหกรรมให้เติบโตอย่างยั่งยืน พร้อมผลักดันผลิตภัณฑ์ไซเบอร์ไทย ผ่านตราสัญลักษณ์ dSURE บัญชีนวัตกรรมไทย และมาตรการจูงใจการใช้ของไทย

Forum 3
"Seminar and Public Consultation for Developing the National Cybersecurity Industry Promotion Plan"
This forum served as a platform for gathering input from the **public sector, private sector, research institutions, and cybersecurity entrepreneurs** to design strategic directions for the sustainable growth of Thailand's cybersecurity industry. The outcomes supported the promotion of Thai cybersecurity products through mechanisms such as the **dSURE trust mark**, the **Thailand Innovation Account,** and incentives to encourage the use of domestically developed technologies.

ครั้งที่ 4

"การสัมมนาและรับฟังความคิดเห็นต่อ (ร่าง) แนวปฏิบัติเพื่อความมั่นคงปลอดภัยสำหรับระบบปัญญาประดิษฐ์ (AI Security Guidelines)"

มุ่งกำหนดแนวปฏิบัติด้านความมั่นคงปลอดภัย AI ที่ใช้ได้จริง ครอบคลุมตลอดวงจรชีวิต AI และสอดคล้องมาตรฐานสากล ผ่านการเสวนาและการมีส่วนร่วมของผู้เกี่ยวข้อง

Forum 4
"Seminar and Public Consultation on the (Draft) AI Security Guidelines"
This forum focused on defining **practical and implementable AI security guidelines,** covering the entire AI lifecycle and aligning with international standards. The process emphasized multi-stakeholder participation to ensure that the guidelines are applicable, trustworthy, and consistent with global best practices.

ปรับปรุงพัฒนาพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์
Enhancement of the Cybersecurity Act

ในปีงบประมาณ 2567 สกมช. ได้ประเมินผลสัมฤทธิ์พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พบว่าการเปลี่ยนแปลงของเทคโนโลยีและรูปแบบอาชญากรรมไซเบอร์ที่ซับซ้อนขึ้น ทำให้กฎหมายเดิมไม่สามารถรองรับสถานการณ์ได้อย่างมีประสิทธิภาพและทันท่วงที

ในปีงบประมาณ พ.ศ. 2568 สกมช. ได้ริเริ่มปรับปรุงแก้ไข **พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562** และกฎหมายลำดับรอง ให้มีความทันสมัย ยืดหยุ่น และเสริมประสิทธิภาพการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทุกรูปแบบ

ในการปรับปรุงแก้ไขกฎมายดังกล่าว ได้จัดให้มี**การสัมมนารับฟังความคิดเห็น จำนวน 5 ครั้ง ครอบคลุมทั้ง 4 ภูมิภาค** โดยมีหน่วยงานรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานเอกชน ตลอดจนนักวิชาการและประชาชนทั่วไป **เข้าร่วมแสดงความคิดเห็นทั้งในรูปแบบออนไซต์และออนไลน์ รวมกว่า 2,000 คน**

In Fiscal Year 2024, the **NCSA** conducted an evaluation of the enforcement of the **Cybersecurity Act B.E. 2562 (2019).** The assessment found that rapid technological advancements and increasingly sophisticated cybercrime patterns have rendered certain provisions of the existing law insufficient to effectively and timely address current cyber threat situations.

In Fiscal Year 2025, the **NCSA** initiated amendments to the **Cybersecurity Act B.E. 2562,** along with related subordinate legislation, with the objective of enhancing the effectiveness of cyber threat prevention, response, and cooperation mechanisms across all forms of cyber threats.

As part of the legislative amendment process, **five public consultation forums** were conducted, covering **all four regions of Thailand,** with participation from government agencies, regulatory and supervisory authorities, organizations of critical information infrastructure (CII), private sector entities, academics and the general public. Public opinions were collected through both **onsite and online channels,** with **more than 2,000 participants** in total.

ภายหลังการรับฟังความคิดเห็น ได้จัดทำ **(ร่าง) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (ฉบับที่...) พ.ศ. ...** และเปิดรับฟังความคิดเห็นผ่านระบบกลางทางกฎหมาย **(www.law.go.th)** ครั้งที่ 1 เรียบร้อยแล้ว โดยสาระสำคัญมุ่งเสริมประสิทธิภาพการบริหารจัดการเหตุภัยไซเบอร์ การแจ้งและรายงานเหตุ มาตรการตอบโต้ภัยคุกคามที่กระทบต่อประเทศ และการกำหนดโทษให้ชัดเจนยิ่งขึ้น ตั้งเป้าผลักดันร่างกฎหมายให้ผ่านกระบวนการนิติบัญญัติและประกาศใช้ต่อไป

Following the consultation process, a **Draft Amendment to the Cybersecurity Act (Revision ...), B.E. ...** was prepared and opened for public consultation via the central legal consultation platform **(www.law.go.th)** for the **first round**, which has been successfully completed. Key objectives of the draft amendment include: strengthening the efficiency of cyber incident management, enhancing cyber incident notification and reporting mechanisms, improving response measures for cyber threats with national impact, and introducing clearer and more effective penalty provisions. The draft law is now being advanced through the legislative process in preparation for formal enactment and promulgation.

ครั้งที่ 1

ครั้งที่ 1 กรุงเทพมหานคร
เมื่อวันที่ 9 มิถุนายน 2568
Session 1: Bangkok
9 June 2025

ครั้งที่ 2

ครั้งที่ 2 เชียงใหม่
เมื่อวันที่ 20 มิถุนายน 2568
Session 2: Chiang Mai
20 June 2025

ครั้งที่ 3

ครั้งที่ 3 อุดรธานี
เมื่อวันที่ 4 กรกฎาคม 2568
Session 3: Udon Thani
4 July 2025

ครั้งที่ 4

ครั้งที่ 4 สุราษฎร์ธานี
เมื่อวันที่ 25 กรกฎาคม 2568
Session 4: Surat Thani
25 July 2025

ครั้งที่ 5

ครั้งที่ 5 กรุงเทพมหานคร
เมื่อวันที่ 1 สิงหาคม 2568
Session 5: Bangkok
1 August 2025

ออกกฎหมายลำดับรอง เพื่อป้องกัน รับมือและลดความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
Issuance of Subordinate Legislation to Prevent, Respond to, and mitigate Cybersecurity Risks

ประกาศ กมช. เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568 (Website Security Standard Version 1.0)

กำหนดมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยของเว็บไซต์สำหรับหน่วยงานของรัฐ หน่วยงานกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อยกระดับความปลอดภัยของคอมพิวเตอร์ ระบบ และโปรแกรมที่เกี่ยวข้อง **มีผลบังคับใช้ตั้งแต่วันที่ 16 กันยายน 2569** เป็นต้นไป

Notification of the NCSC on Website Security Standards B.E. 2568 (2025) (Website Security Standard Version 1.0)

This Notification prescribes **minimum cybersecurity standards for websites** of government agencies, supervisory or regulatory authorities, and **organizations of critical information infrastructure (CII)**, with the objective of enhancing the security of computer systems, systems, and related programs. The standards shall **enter into force from 10 September B.E. 2569 (2026) onwards.**

หน้า ๓๓
เล่ม ๑๔๒ ตอนพิเศษ ๓๐๕ ง ราชกิจจานุเบกษา ๑๖ กันยายน ๒๕๖๘

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์
พ.ศ. ๒๕๖๘

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีหน้าที่และอำนาจสร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ จึงสมควรมีมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ เพื่อให้การดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๙ (๔) มาตรา ๒๒ (๑๓) และ (๑๖) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ในคราวการประชุมครั้งที่ ๖/๒๕๖๕ เมื่อวันที่ ๔ พฤศจิกายน ๒๕๖๕ มติคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในคราวการประชุมครั้งที่ ๔/๒๕๖๖ เมื่อวันที่ ๒๖ พฤศจิกายน ๒๕๖๖ และมติคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในคราวการประชุมครั้งที่ ๑๓/๒๕๖๘ เมื่อวันที่ ๒๙ สิงหาคม ๒๕๖๘ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. ๒๕๖๘"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดำเนินการให้เว็บไซต์ของตน เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ ที่กำหนดท้ายประกาศนี้

ให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ดำเนินการส่งเสริมและสนับสนุนให้หน่วยงานเอกชนนำมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามแนบท้ายประกาศนี้ ไปปรับใช้เป็นแนวทางในสร้างมาตรฐานการรักษาความมั่นคงปลอดภัยเว็บไซต์ของตนด้วย

เล่มรวมกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ 2.0
Cyber Security Laws 2.0

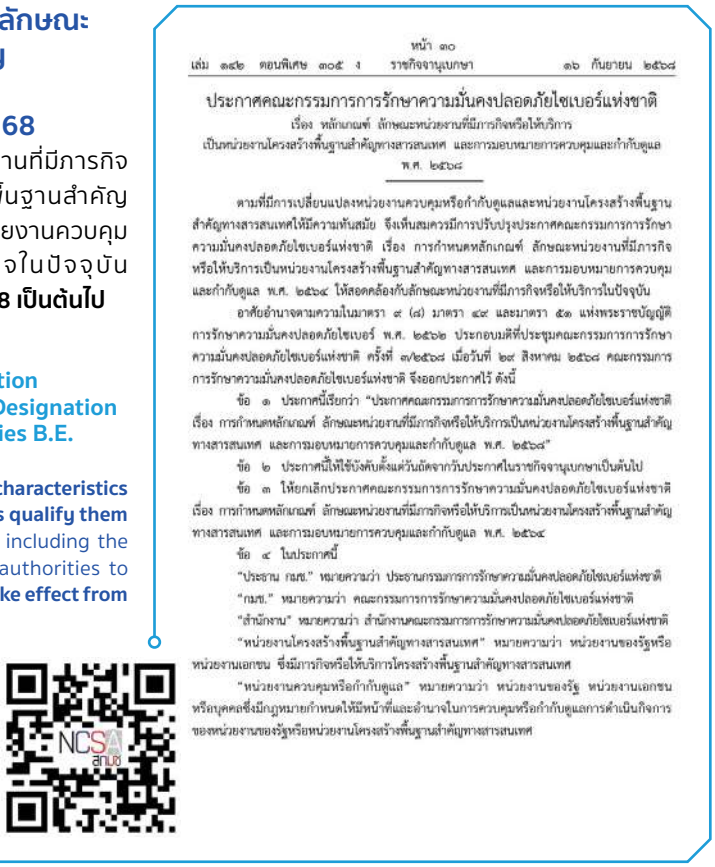
จัดทำในรูปแบบ 2 ภาษา (ไทย-อังกฤษ)
Available in both Thai and English

ประกาศ กมช. เรื่อง หลักเกณฑ์และลักษณะหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2568

กำหนดหลักเกณฑ์และลักษณะของหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงการมอบหมายหน่วยงานควบคุมหรือกำกับดูแลให้สอดคล้องกับภารกิจในปัจจุบัน **มีผลบังคับใช้ตั้งแต่วันที่ 17 กันยายน 2568 เป็นต้นไป**

Notification of the NCSC on Criteria and Characteristics of Critical Information Infrastructure Organizations and the Designation of Supervisory or Regulatory Authorities B.E. 2568 (2025)

This Notification establishes the **criteria and characteristics of organizations whose missions or services qualify them as Critical Information Infrastructure (CII),** including the designation of supervisory or regulatory authorities to oversee compliance. The Notification **shall take effect from 17 September B.E. 2568 (2025) onwards.**



หน้า ๓๐
เล่ม ๑๔๒ ตอนพิเศษ ๓๐๕ ง ราชกิจจานุเบกษา ๑๖ กันยายน ๒๕๖๘

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง หลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๘

ตามที่มีการเปลี่ยนแปลงหน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความทันสมัย จึงเห็นสมควรมีการปรับปรุงประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ ให้สอดคล้องกับลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในปัจจุบัน

อาศัยอำนาจตามความในมาตรา ๙ (๘) มาตรา ๔๙ และมาตรา ๕๓ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๓/๒๕๖๘ เมื่อวันที่ ๒๘ สิงหาคม ๒๕๖๘ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๘"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ให้ยกเลิกประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔

ข้อ ๔ ในประกาศนี้

"ประธาน กมช." หมายความว่า ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

"กมช." หมายความว่า คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

"สำนักงาน" หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

"หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ" หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

"หน่วยงานควบคุมหรือกำกับดูแล" หมายความว่า หน่วยงานของรัฐ หน่วยงานเอกชน หรือบุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

Infographic ประกาศสำคัญที่คนทำงานด้านไซเบอร์ "ต้องรู้"

Key Infographics: Cybersecurity Notifications That Agencies "Must Know"

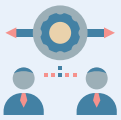
พัฒนาสมรรถนะของบุคลากรสู่ความเป็นผู้นำด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
Developing Personnel Competencies toward Cybersecurity Leadership

พัฒนาบุคลากร
Personnel Development

เสริมสร้างศักยภาพ ความรู้ และวัฒนธรรมองค์กร มุ่งพัฒนาบุคลากรอย่างรอบด้าน ทั้งด้านสมรรถนะ ความผูกพัน และคุณภาพชีวิต เพื่อสร้างบุคลากรที่พร้อมรับมือภัยคุกคามไซเบอร์ในทุกมิติ

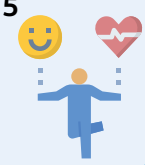
Strengthening capacity, knowledge, and organizational culture by developing personnel holistically-covering competencies, engagement, and quality of life-to build a workforce that is fully prepared to address cybersecurity threats in all dimensions.

NCSA Town Hall 2025
สื่อสารทิศทางองค์กร
สร้างความเข้าใจและอัตลักษณ์ NCSA
Communicating organizational direction and strengthening the shared understanding and identity of NCSA



NCSA Cyber Strong Award
ยกย่องบุคลากรต้นแบบ
สะท้อนคุณค่าหลักขององค์กร
Recognizing exemplary personnel and reflecting the organization's core values

NCSA Happy Healthy 2025
ส่งเสริมสุขภาพกาย-ใจ
และความสุขในการทำงาน
Promoting physical and mental well-being, and happiness at work



NCSA Outing 2025
สร้างความสัมพันธ์
และความสามัคคีในองค์กร
Strengthening relationships and unity within the organization

พัฒนาทักษะและองค์ความรู้
Skills Development and Knowledge Advancement

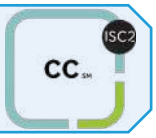
ยกระดับสมรรถนะตามมาตรฐานสากล
ส่งเสริมการเรียนรู้และพัฒนาทักษะที่จำเป็นต่อภารกิจด้านความมั่นคงปลอดภัยไซเบอร์

Enhancing Competencies in Line with International Standards
Promoting continuous learning and development of essential skills required for cybersecurity missions.

TOEIC Simulation Test
บุคลากรเข้าร่วมจำนวน **123** คน
Number of participating personnel: **123**

CompTIA Security+
บุคลากรเข้าร่วมอบรมและทดสอบจำนวน **45** คน
Number of personnel attending training and certification exam: **45**

SC² Certified in Cybersecurity (CC)
ผู้สอบผ่าน **38** คน
38 candidates passed



บริหารทรัพยากรบุคคล
Human Resource Management

บริหารงานบุคคลอย่างยืดหยุ่น โปร่งใส และเป็นธรรมปรับรูปแบบการทำงานให้สอดคล้องกับวิถีการทำงานยุคใหม่ และยึดหลักธรรมาภิบาลในการบริหารบุคลากร

Manage human resources with flexibility, transparency, and fairness, adapting work arrangements to align with modern ways of working, and upholding the principles of good governance in personnel management.

Hybrid Working: Work from Anywhere
สนับสนุนการทำงานนอกสถานที่ตามแนวทาง Next Normal
Hybrid Working: Work from Anywhere Support remote and off-site work in accordance with the Next Normal approach.

การบรรจุและแต่งตั้งเป็นพนักงาน
ดำเนินการตามหลักเกณฑ์ที่ชัดเจนและเป็นธรรม
Recruitment and Appointment
Conduct recruitment and appointments based on clear and fair criteria.

การเลื่อนตำแหน่ง
ใช้หลักเกณฑ์ที่โปร่งใสและตรวจสอบได้
Promotion Apply transparent and verifiable criteria for promotions.

ความเสมอภาคระหว่างเพศ
ส่งเสริมการปฏิบัติงานโดยไม่เลือกปฏิบัติ
Gender Equality Promote non-discriminatory practices and equal treatment in the workplace.

การสรรหาและเสริมสร้างกำลังคน
Recruitment and Workforce Strengthening

เสริมกำลังคนรองรับภารกิจด้านไซเบอร์ของประเทศ
สกมช. ดำเนินการสรรหาบุคลากรที่มีความรู้ ความสามารถและความเชี่ยวชาญเฉพาะด้าน เพื่อรองรับภารกิจเชิงยุทธศาสตร์

Building National Cybersecurity Workforce Capacity
The NCSA conducted recruitment of personnel with knowledge, capabilities, and specialized expertise to support national strategic cybersecurity missions.

บรรจุแต่งตั้งพนักงานใหม่ จำนวน 40 อัตรา
New personnel recruited: 40 positions.

PM AWARDS 2025 รางวัลแห่งปีด้านความมั่นคงปลอดภัยไซเบอร์ เชิดชูองค์กรไทยต้นแบบ ย้ำพลังความร่วมมือทุกภาคส่วน คือกุญแจสู่ความปลอดภัยดิจิทัลของประเทศ

PM Awards 2025 Cybersecurity Excellence Awards Recognising Outstanding Thai Organizations and Reinforcing the Power of Multi-Sector Collaboration Toward National Digital Security

รัฐบาลเดินหน้าผลักดัน **"การปราบปรามสแกมเมอร์และอาชญากรรมออนไลน์เป็นวาระแห่งชาติ"** ควบคู่การยกระดับความมั่นคงปลอดภัยไซเบอร์ของประเทศ ผ่านการจัดกิจกรรม **Prime Minister Awards: Thailand Cybersecurity Excellence Awards 2025** รางวัลจากนายกรัฐมนตรีเพื่อเชิดชูองค์กรไทยต้นแบบด้านความปลอดภัยทางไซเบอร์ทั้งภาครัฐและเอกชน

The Government is advancing its flagship policy to designate **the suppression of scam gangs and online crime as a national agenda,** driving the enhancement of Thailand's cybersecurity through the organization of the **Prime Minister Awards: Thailand Cybersecurity Excellence Awards 2025.** The awards, presented by the Prime Minister, aim to recognise exemplary Thai organizations-both public and private-that demonstrate excellence in cybersecurity practices.

2 รางวัลใหญ่
Two Major Awards

Best Performance Award
องค์กรที่ป้องกันและรับมือภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพ
Presented to organizations that demonstrate effective prevention and response to cyber threats.

Most Contributions Award
หน่วยงานที่มีบทบาทสำคัญในการยกระดับความมั่นคงไซเบอร์ของประเทศ
Presented to organizations that play a significant role in elevating Thailand's national cybersecurity capability.

ปีนี้มีองค์กรสมัครเข้าร่วม กว่า 200 หน่วยงาน ผ่านการประเมินตามมาตรฐานสากล และมีผู้ได้รับรางวัลรวมกว่า 173 หน่วยงาน แบ่งเป็น
In 2025, more than **200 organizations** applied for consideration. Following evaluation based on international standards, a total of 173 **organizations** received awards, comprising:

- **ระดับดีเลิศ** (Tier 1) รับโล่รางวัลและประกาศนียบัตร
  Excellent Level (Tier 1) - Received a Trophy and Certificate
  24 หน่วยงาน | 24 Organizations
- **ระดับดีมาก** (Tier 2) รับประกาศนียบัตร
  Very Good Level (Tier 2) - Received a Certificate
  53 หน่วยงาน | 53 Organizations
- **ระดับดี** (Tier 3) รับประกาศนียบัตร
  Good Level (Tier 3) - Received a Certificate
  36 หน่วยงาน | 36 Organizations
- **ระดับเข้าร่วม** (Tier 4) รับประกาศนียบัตร
  Participation Level (Tier 4) - Received a Certificate
  53 หน่วยงาน | 53 Organizations
- และ**หน่วยงาน** Most Contributions Awards
  And recipients of the Most Contributions Awards
  อีก **7 หน่วยงาน | 7 Organizations**

ผลการดำเนินงานด้านอื่น ๆ

OTHER KEY PERFORMANCE OUTCOMES

รายงานผลการดำเนินงานของคณะกรรมการตรวจสอบประจำปีงบประมาณ 2568

Annual Performance Report of the Audit Committee Fiscal Year 2025

คณะกรรมการตรวจสอบได้ปฏิบัติหน้าที่และความรับผิดชอบด้วยความรู้ ความสามารถ ความรอบคอบ และความเป็นอิสระอย่างเหมาะสม เพื่อประโยชน์ของผู้มีส่วนได้ส่วนเสียอย่างเท่าเทียมกันโดยยึดถือหลักเกณฑ์และกฎหมายที่เกี่ยวข้อง ดังนี้

The Audit Committee performed its duties and responsibilities with due knowledge, competence, diligence, and independence, ensuring fairness to all stakeholders in compliance with relevant legal frameworks, including:

- หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561 และที่แก้ไขเพิ่มเติม (พ.ศ. 2562, 2564 และ 2566)

  Ministry of Finance regulations on internal control standards for government agencies B.E. 2561 and subsequent amendments (B.E. 2562, 2564, and 2566)

- หลักเกณฑ์ตามมาตรา 5/8 แห่งพระราชบัญญัติองค์การมหาชน (ฉบับที่ 2) พ.ศ. 2559

  Section 5/8 of the Organization Act (No. 2) B.E. 2559

- ข้อบังคับคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ว่าด้วยการตรวจสอบภายใน พ.ศ. 2567 และที่แก้ไขเพิ่มเติม พ.ศ. 2568

  Internal audit regulations of the Committee Managing the National Cyber Security Agency Office B.E. 2567 and amendments B.E. 2568

ผลการประเมินสถานะของหน่วยงานภาครัฐในการเป็นระบบราชการ 4.0 (PMQA 4.0) ประจำปีงบประมาณ พ.ศ. 2568
Public Sector Management Quality Award 4.0 (PMQA 4.0) - Assessment Results

สกมช. ปี 2568 | คะแนนรวม 421.43 คะแนน
NCSA, Fiscal Year 2025 Total Score: 421.43 points

หมวดการประเมิน Assessment Categories		คะแนน Score
หมวด Category 1	**การนำองค์การ** Organizational Leadership	416.67
หมวด Category 2	**การวางแผนเชิงยุทธศาสตร์** Strategic Planning	433.33
หมวด Category 3	การให้ความสำคัญกับผู้รับบริการและผู้มีส่วนได้ส่วนเสีย Customer and Stakeholder Focus	450.00
หมวด Category 4	การวัด การวิเคราะห์ และการจัดการความรู้ Measurement, Analysis, and Knowledge Management	466.67
หมวด Category 5	การมุ่งเน้นบุคลากร Workforce Focus	460.00
หมวด Category 6	การมุ่งเน้นระบบการปฏิบัติการ Operations Focus	466.67
หมวด Category 7	ผลลัพธ์การดำเนินการ Results	256.67

ผลการประเมินคุณธรรมและความโปร่งใส ในการดำเนินงานของหน่วยงานภาครัฐ (Integrity and Transparency Assessment: ITA) ประจำปีงบประมาณ พ.ศ. 2568
Results of the Integrity and Transparency Assessment in Government Agencies (ITA)

สกมช. ปี 2568 | คะแนนรวม 92.72 คะแนน
NCSA, Fiscal Year 2025 | Overall Score: 92.72 points

รายการประเมิน Assessment Items	คะแนน Score
แบบวัดการรับรู้ของผู้มีส่วนได้ส่วนเสียภายใน (Internal Integrity and Transparency Assessment) หรือแบบวัด IIT Internal Stakeholders' Perception of Integrity and Transparency within the Agency	94.00
แบบวัดการรับรู้ของผู้มีส่วนได้ส่วนเสียภายนอก (External Integrity and Transparency Assessment) หรือแบบวัด EIT (เก็บข้อมูลโดย สกมช.) External Stakeholders' Perception (assessed by NCSA)	86.86
แบบวัดการรับรู้ของผู้มีส่วนได้ส่วนเสียภายนอก (External Integrity and Transparency Assessment) หรือแบบวัด EIT (เก็บข้อมูลโดยสำนักงาน ป.ป.ช.) External Stakeholders' Perception (assessed by the National Anti-Corruption Commission - NACC)	83.92
แบบวัดการเปิดเผยข้อมูลสาธารณะ (Open Data Integrity and Transparency Assessment) หรือแบบวัด OIT Public Disclosure of Agency Information	97.25

สกมช. ผ่านการประเมินองค์กรคุณธรรม ในระดับ คุณธรรมต้นแบบ ประจำปีงบประมาณ พ.ศ. 2568
The NCSA has passed the Moral Organization Assessment at the **"Moral Role Model"** level for Fiscal Year 2025.

ผลการประเมินองค์กรคุณธรรม ประจำปีงบประมาณ พ.ศ. 2568
Results of the Moral Organization Assessment for Fiscal Year 2025

การประเมินองค์กรคุณธรรมเป็นกลไกสำคัญในการส่งเสริมการทำความดีและการพัฒนาจิตสำนึกรับผิดชอบต่อสังคม ช่วยหล่อหลอมให้บุคลากรยึดมั่นในคุณค่าพื้นฐานของความเป็นมนุษย์ อันเป็นรากฐานของการพัฒนาทรัพยากรมนุษย์ให้มีคุณภาพ เป็นทั้งคนดี คนเก่ง และมีพฤติกรรมที่สะท้อนคุณธรรม 5 ประการ ได้แก่ พอเพียง วินัย สุจริต จิตอาสา และกตัญญู ซึ่งล้วนมีบทบาทสำคัญต่อการพัฒนาประเทศอย่างยั่งยืน

The Moral Organization Assessment is a key mechanism for promoting ethical governance and responsible organizational development. It helps instill and reinforce core moral values among personnel, which form the foundation of human dignity. These values serve as the basis for human resource development toward quality personnel-individuals who are both competent and ethical-reflecting the five core moral values, namely **Sufficiency, Discipline, Integrity, Responsibility, and Altruism.** These values play a crucial role in fostering sustainable national development.

แผนปฏิบัติการด้านการส่งเสริมคุณธรรมในภาพรวมของ สกมช. ประจำปีงบประมาณ พ.ศ. 2568
Overall Action Plan for Moral Promotion of the National Cyber Security Agency for Fiscal Year 2025

สกมช. ดำเนินโครงการ/กิจกรรม ภายใต้**แผนปฏิบัติการด้านการส่งเสริมคุณธรรมแห่งชาติ ระยะที่ 2 (พ.ศ. 2566-2570)** ซึ่งมุ่งพัฒนาคนไทยให้มีพฤติกรรมที่สะท้อนคุณธรรม 5 ประการ บนพื้นฐานหลักธรรมทางศาสนา หลักปรัชญาของเศรษฐกิจพอเพียง และวิถีวัฒนธรรมไทยที่ดีงาม เพื่อเสริมสร้างสังคมคุณธรรม และลดปัญหาการทุจริตอย่างเป็นรูปธรรม

The NCSA has implemented projects/activities under the **National Moral Promotion Action Plan, Phase 2 (2023-2027)**, with the objective of fostering ethical behavior among Thai citizens based on the **five core moral values**, grounded in religious principles, the Sufficiency Economy Philosophy, and Thai cultural ethics. The plan aims to build a moral society and systematically reduce corruption.

คณะทำงานจัดทำและขับเคลื่อนแผนปฏิบัติการด้านการส่งเสริมคุณธรรมในภาพรวม ของ สกมช. ได้พิจารณาคัดเลือกโครงการ/กิจกรรมที่สำคัญหรือโดดเด่น จำนวน 3 เรื่อง ได้แก่
The working committee responsible for developing and driving the overall Moral Promotion Action Plan of the NCSA considered and selected three key or outstanding projects/activities, as follows:

1 กิจกรรมลดการใช้กระดาษ
Paper Reduction Initiative
Reducing paper usage by **more than 42%**

ลดการใช้กระดาษได้มากกว่า 42%

2 โครงการยกย่องเชิดชูบุคคลต้นแบบที่ปฏิบัติตนเป็นแบบอย่างที่ดีตามคุณธรรม 5 ประการ (พอเพียง วินัย สุจริต จิตอาสา กตัญญู)
A project to honor and recognize role-model individuals who demonstrate exemplary conduct in accordance with the five moral values: Sufficiency, Discipline, Integrity, Volunteer Spirit, and Gratitude.

3 กิจกรรม CSR
CSR Activities to Drive Sustainable Organizational Integrity

3 SAFE, SECURE, AND TRUSTED CYBERSPACE

แนวทางดำเนินงานปี 2569

แนวโน้มภัยคุกคามในปี 2569

OPERATIONAL DIRECTION FOR 2026

Cyber Threat Landscape in 2026

แนวโน้มภัยสำคัญ :
Key Threat Trends:

AI-Powered Social Engineering / Deepfake-as-a-Service, Cloud/SaaS Takeover & Machine Account Abuse, RaaS 2.0 (Double/Triple Extortion + AI), Shadow AI & Data Leakage, OT/IoT & Machine Identity Quantum-Risk Readiness

ปัจจัยสำคัญที่ทำให้ภัยคุกคามความมั่นคงไซเบอร์รุนแรงขึ้น
Key factors contributing to the escalation of Cybersecurity threats

ความตึงเครียดทางภูมิรัฐศาสตร์ (Geopolitical Tensions)
รัฐมหาอำนาจใช้ไซเบอร์เป็นเครื่องมือเชิงยุทธศาสตร์ ทั้งการจารกรรม ปฏิบัติการข้อมูลข่าวสาร และการโจมตีโครงสร้างพื้นฐานสำคัญ เพิ่มแรงกดดันให้ประเทศต้องเลือกข้าง และเสี่ยงยกระดับเป็นสงครามไซเบอร์ที่กระทบรัฐ เศรษฐกิจ และประชาชนโดยตรง

Geopolitical Tensions
Major powers increasingly leverage cyberspace as a strategic instrument-ranging from cyber espionage and information operations to attacks on critical infrastructure. These dynamics intensify pressure on states to take sides and raise the risk of cyber warfare which directly impacts governments, economies, and citizens.

AI ปัจจัยเร่งที่สำคัญ
AI เพิ่มทั้งศักยภาพการป้องกันและความรุนแรงของการโจมตี โดยช่วยตรวจจับภัยคุกคามได้เร็วขึ้น แต่ขณะเดียวกันลดต้นทุนอาชญากรรมไซเบอร์ เพิ่ม Deepfake ข้อมูลเท็จ และการโจมตีอัตโนมัติ

AI as a Catalyst
Artificial intelligence enhances both defensive capabilities and complexity of cyberattacks by enabling faster threat detection. At the same time, it significantly lowers the barrier for cybercrime-fueling deepfakes, synthetic content, and automated attacks.

การพึ่งพาโครงสร้างพื้นฐานดิจิทัลสูงขึ้น
หน่วยงานมีการใช้ระบบเทคโนโลยีดิจิทัลเชื่อมต่อในทุก ๆ ระบบที่สำคัญ เช่น พลังงาน การเงิน คมนาคม การโจมตีเพียงจุดเดียวอาจกระทบบริการสำคัญทั้งระบบ

Growing Dependence on Digital Infrastructure
Government agencies increasingly rely on digital systems across critical sectors such as energy, finance, and transportation. Any disruption can cascade across essential public services and national systems.

การพึ่งพาเทคโนโลยีต่างประเทศ
เสี่ยงต่อการถูกจำกัดการเข้าถึงเทคโนโลยีหากเกิดความขัดแย้งทางการเมืองหรือมีมาตรการคว่ำบาตร รวมทั้งควบคุมความเสี่ยงได้ไม่เต็มที่ และสูญเสียอธิปไตยทางเทคโนโลยีในระยะยาว

Dependence on Foreign Technologies
Reliance on external technologies exposes states to access restrictions, geopolitical constraints, sanctions, and supply-chain risks-while also limiting sovereign risk control and causing long-term technological dependency.

การแพร่กระจายข้อมูลอย่างรวดเร็วบนแพลตฟอร์มออนไลน์
ข่าวปลอม และ Deepfake แพร่กระจายเร็วพอ ๆ กับข้อเท็จจริง อัลกอริทึมสร้าง Echo Chamber บ่อนทำลายความเชื่อมั่น กระตุ้นความแตกแยก และคุกคามเสถียรภาพภายในประเทศได้โดยไม่ต้องอาศัยเหตุการณ์จริง

Rapid Information Dissemination via Online Platforms
Disinformation and deepfake content spread as fast as facts. Algorithm-driven echo chambers undermine trust, intensify social polarization, and threaten internal stability-without requiring any real-world trigger.

ขาดแคลนบุคลากรและขีดความสามารถไซเบอร์ของรัฐ
คนไม่พอและทักษะไม่ทันภัยคุกคาม ทำให้การป้องกันและฟื้นคืนระบบสู่สภาวะปกติทำได้ล่าช้า และสูญเสียความเชื่อมั่นทั้งในสายตานานาชาติและประชาชน

Shortage of Cybersecurity Workforce and Capability Gaps
Insufficient personnel and skills misaligned with evolving threats slow prevention and recovery efforts, eroding trust at both international and public levels.

การเติบโตของสกุลเงินดิจิทัลและการอำพรางธุรกรรม
สกุลเงินดิจิทัลเอื้อต่อการซ่อนตัวและฟอกเงิน อาชญากรรมไซเบอร์ เช่น Ransomware และการหลอกลวงออนไลน์ใช้คริปโตเป็นช่องทางหลัก เนื่องจากระบบไร้ศูนย์กลาง ตรวจสอบยาก และทำธุรกรรมข้ามประเทศได้โดยไม่พึ่งระบบธนาคาร

Growth of Digital Assets and Cyber-Enabled Financial Crime
Digital assets facilitate anonymity and money laundering. Cybercrime-such as ransomware and online fraud-often exploits cryptocurrencies due to decentralized systems, limited traceability, and cross-border transactions outside traditional banking oversight.

ภารกิจสำคัญที่ต้องเดินหน้าอย่างต่อเนื่องในปี 2569
Key Priority Actions to Be Continuously Advanced in 2026

- พัฒนาและปรับปรุงกฎหมายที่เกี่ยวข้องให้ทันสมัย รองรับสถานการณ์ปัจจุบัน
  Develop and update relevant laws to keep pace with evolving cyber threats
- สนับสนุนการจัดตั้ง/ยกระดับ Sectoral CERT ของประเทศไทยทุก Sector
  Support the establishment and strengthening of **Sectoral CERTs** across all national sectors
- สร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในทุกระดับ รวมถึงภัยจากสแกมเมอร์ ฟิชชิง และการฉ้อโกงออนไลน์
  Enhance cybersecurity awareness at all levels of society including online scams, phishing, and online fraud
- พัฒนาและยกระดับเทคโนโลยีและบุคลากรด้านไซเบอร์ของประเทศ
  Develop and upgrade national cybersecurity technologies and workforce capabilities
- สร้างความร่วมมือในการยกระดับ GCI ของประเทศไทย
  Promote collaboration under the **Global Cybersecurity Index (GCI)** framework
- พัฒนาแนวทางให้ครอบคลุมทุกระดับ เช่น Cybersecurity MSMEs, Cybersecurity Industry, Cyberbullying
  Expand efforts to cover all groups, such as **Cybersecurity MSMEs, the cybersecurity industry, and cyberbullying prevention**
- ทบทวนนโยบาย แผนยุทธศาสตร์ กลยุทธ์ เพื่อนำไปสู่การจัดทำร่างนโยบายและแผนปฏิบัติการว่าด้วยความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ปีงบประมาณ พ.ศ. 2571-2575
  Review policies, strategies, and action plans toward the formulation of the **National Cybersecurity Policy and Master Plan (FY 2028-2032)**
- การเตรียมความพร้อมสำหรับการปฏิบัติตามประกาศ กมช. ว่าด้วย เรื่องมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ซึ่งจะมีผลบังคับใช้ในวันที่ 10 กันยายน 2569
  Prepare for compliance with the **NCSC Notification on Cloud Security Standards B.E. 2567**, Effective on 10th September 2026

SAFE, SECURE, AND TRUSTED CYBERSPACE

SAFE ความปลอดภัยในการใช้ชีวิตของประชาชน
Safe: Ensuring safety in citizens' daily digital lives

SECURE ความมั่นคงของโครงสร้างพื้นฐานทางสารสนเทศและบริการสำคัญภาครัฐของประเทศ
Secure: Safeguarding national critical information infrastructure and essential government services

TRUSTED สร้างความน่าเชื่อถือ ทั้งในประเทศและสากล
Trusted: Building trust at both national and international levels

SAFE ความปลอดภัยในการใช้ชีวิตของประชาชน Cyber Safety for Citizens

พัฒนาห้องปฏิบัติการทดสอบเจาะระบบ

เพื่อเสริมความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรอย่างรอบด้าน ทั้งการประเมินและลดความเสี่ยง ตรวจจับและวิเคราะห์ช่องโหว่ของระบบได้อย่างรวดเร็วและแม่นยำ ลดผลกระทบต่อข้อมูลและการดำเนินงาน

นอกจากนี้ ยังช่วยยกระดับกระบวนการทดสอบให้สอดคล้องกับมาตรฐานสากล เช่น ISO/IEC 27001 เพิ่มประสิทธิภาพการบริหารความเสี่ยงและความน่าเชื่อถือขององค์กร ควบคู่กับการพัฒนาศักยภาพบุคลากรผ่านสภาพแวดล้อมการฝึกอบรม เพื่อรับมือภัยคุกคามไซเบอร์ที่ซับซ้อนและเปลี่ยนแปลงตลอดเวลา พร้อมเสริมความพร้อมและความเชื่อมั่นให้หน่วยงานรัฐ หน่วยงานกำกับดูแล และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

Development of a Penetration Testing Laboratory

Establish a **Penetration Testing Lab** to enhance cybersecurity resilience across organizations through comprehensive system testing, risk assessment, vulnerability detection, and in-depth analysis. This enables rapid and accurate identification of system weaknesses, reducing impacts on data and operational continuity.

In addition, the lab supports alignment with international standards such as **ISO/IEC 27001**, strengthens risk management effectiveness, and enhances organizational credibility. It also contributes to workforce capacity building through hands-on training environments, preparing personnel to respond to increasingly complex and evolving cyber threats, while reinforcing confidence among government agencies, regulators, and organizations of critical information infrastructure.

SAFE ความปลอดภัยในการใช้ชีวิตของประชาชน
Cyber Safety for Citizens

เดินหน้าโครงการจัดตั้งห้องปฏิบัติการความมั่นคงปลอดภัยไซเบอร์
Advancing the Establishment of a Cybersecurity Operations Laboratory

ยกระดับศักยภาพการป้องกัน ตรวจจับ วิเคราะห์ และตอบสนองต่อภัยไซเบอร์ ครอบคลุมการโจมตีระบบ การโจรกรรมข้อมูล และการโจมตีเรียกค่าไถ่
Enhance capabilities in **prevention, detection, analysis, and response** to cyber threats, covering system intrusions, data breaches, and sophisticated cyberattacks

จัดหาเทคโนโลยี เฝ้าระวัง วิเคราะห์มัลแวร์ และเทคนิคการหลอกลวง
Deploy advanced technologies for **monitoring, malware analysis, and social engineering detection**

จัดหาเครื่องมือพิสูจน์หลักฐานดิจิทัลที่ได้มาตรฐานสากล
Procure **digital forensic tools** that comply with international standards

พัฒนาศักยภาพบุคลากร พร้อมส่งเสริมความร่วมมือรัฐ-เอกชน และการแลกเปลี่ยนข้อมูล
Develop personnel capabilities while promoting **public-private collaboration** and information sharing

เสริมระบบมาตรฐานสากล ลดผลกระทบจากการโจมตี และสร้างความเชื่อมั่นต่อภาคธุรกิจและประชาชน และสอดคล้องยุทธศาสตร์ชาติ
Strengthen cybersecurity systems in line with international standards, reduce impacts from cyberattacks, and build public trust in alignment with national strategies

ร่างแผนปฏิบัติการรับมือภัยคุกคามไซเบอร์แห่งชาติ

ข้อมูลจาก **ThaiCERT** ระบุว่า**ประเทศไทยเผชิญการโจมตีทางไซเบอร์เฉลี่ยกว่า 3,180 ครั้งต่อสัปดาห์ต่อองค์กร สูงกว่าค่าเฉลี่ยโลกมากกว่า 70%** สะท้อนความเสี่ยงที่ทวีความรุนแรงและกระทบต่อหน่วยงานรัฐ โครงสร้างพื้นฐานสำคัญ เศรษฐกิจ และความมั่นคงของประเทศ จึงมีความจำเป็นต้องจัดทำ**ร่างแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์ พ.ศ. ...”** เพื่อเป็นกรอบการรับมือและฟื้นฟูสถานการณ์ทั้งในภาวะปกติและฉุกเฉิน มุ่งเสริมขีดความสามารถในการตอบสนองเหตุการณ์ การเตรียมความพร้อม การจัดตั้งทีมรับมือ และการฝึกซ้อมอย่างเป็นระบบและต่อเนื่อง

Drafting the National Cyber Incident Response Plan

Based on data from **ThaiCERT**, Thailand experiences an average of **over 3,180 cyberattacks per week**, which is **70% higher than global average.** This reflects the increasing severity and impact of cyber threats on government agencies, critical information infrastructure, the economy, and national security.

Therefore, it is essential to develop a **National Cyber Incident Response Plan** to serve as a framework for managing cybersecurity in potential or actual cyber crisis situations. The plan will support **response and recovery operations** at both normal and emergency levels, while strengthening capabilities in incident response, preparedness, the establishment of response teams, and continuous training and exercises.

SAFE ความปลอดภัยในการใช้ชีวิตของประชาชน Cyber Safety for Citizens

จัดตั้งสถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เพื่อเป็นศูนย์กลางองค์ความรู้ ฐานข้อมูล และการขับเคลื่อนการพัฒนาบุคลากรและประชาชนด้านความมั่นคงปลอดภัยไซเบอร์อย่างเต็มรูปแบบ โดยมีแผนดำเนินงานสำคัญ ดังนี้

Establishment of the Thailand National Cyber Academy

The Thailand National Cyber Academy serves as a **central hub for knowledge, data, and capacity** building for cybersecurity professionals and the public, with key implementation directions as follows:

ปรับปรุงพื้นที่ทำงานและโครงสร้างพื้นฐาน รองรับการฝึกอบรม งานวิชาการ และกิจกรรมพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์
Upgrade facilities and infrastructure to support training, academic activities, and cybersecurity capacity-building programs

พัฒนาหลักสูตรและการเรียนรู้ ที่ทันสมัย สอดคล้องกับสถานการณ์ภัยไซเบอร์ ครอบคลุมทั้งภาคทฤษฎีและภาคปฏิบัติ
Develop modern curricula and learning programs aligned with evolving cyber threat landscapes, covering both theoretical and practical dimensions

เป็นศูนย์กลางรวบรวมองค์ความรู้ ฐานข้อมูล และแนวปฏิบัติด้านไซเบอร์ พร้อมเชื่อมโยงความร่วมมือกับหน่วยงานทั้งในและต่างประเทศ
Serve as a **central repository of cybersecurity knowledge, databases, and best practices,** connected with domestic and international partner organizations

สนับสนุนความร่วมมือระดับภูมิภาค โดยจัดเตรียมสถานที่สำหรับศูนย์ AJCCBC เพื่อฝึกอบรมผู้ปฏิบัติงานด้านไซเบอร์จากประเทศสมาชิกอาเซียน
Strengthen regional cooperation, including preparation of facilities for the **AJCCBC**, to support training for cybersecurity practitioners from ASEAN Member States

SECURE ความมั่นคงของโครงสร้างพื้นฐานทางสารสนเทศและบริการสำคัญภาครัฐของประเทศ
Ensuring the Security of National Information Infrastructure and Critical Government Services

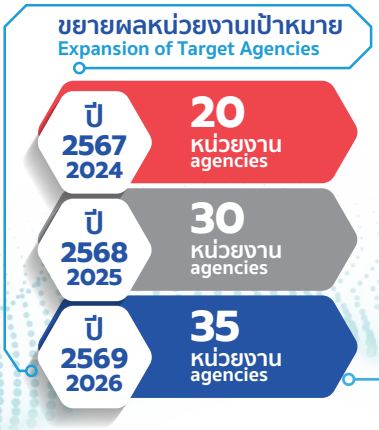
บูรณาการความร่วมมือกับ สคส. ป้องกันการละเมิดข้อมูลส่วนบุคคลจากภัยคุกคามทางไซเบอร์ในหน่วยงานเป้าหมาย
Strengthening Collaboration with the PDPC to Prevent Personal Data Breaches from Cyber Threats in Target Agencies

ในปี 2569 สกมช. มีแผนดำเนินงานร่วมกับ สคส. เดินหน้าบูรณาการความร่วมมือกับหน่วยงานภาครัฐ **35 หน่วยงาน** เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคลจากภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง ตามที่คณะรัฐมนตรีเมื่อวันที่ 21 พฤศจิกายน 2566 และคำสั่งที่เกี่ยวข้อง โดยมุ่งลดความเสี่ยงข้อมูลรั่วไหล เสริมความเชื่อมั่นในการใช้บริการดิจิทัลภาครัฐ และเพิ่มความเข้มแข็งด้านความมั่นคงไซเบอร์ของประเทศ

In 2026, the National Cyber Security Agency (NCSA) will continue to strengthen cooperation with the Office of Personal Data Protection Committee (PDPC) by integrating joint efforts with **35 government agencies** to prevent personal data breaches resulting from cyber threats on an ongoing basis.

This initiative is in line with the Cabinet Resolution dated **21 November 2023**, as well as related directives, with the objectives of:

- Mitigating the risk of personal data leakage
- Enhancing public trust in the use of government digital services
- Strengthening national cybersecurity resilience



เตรียมพร้อมระบบสารสนเทศไทยรับมือภัยไซเบอร์ในยุคควอนตัม
Preparing Thailand's Information Systems for Cyber Threats in the Post-Quantum Era

การพัฒนาอย่างรวดเร็วของเทคโนโลยีคอมพิวเตอร์ควอนตัม ส่งผลให้วิธีการเข้ารหัสที่ใช้อยู่ในปัจจุบันมีความเสี่ยงสูง และก่อให้เกิดภัยคุกคามทางไซเบอร์รูปแบบใหม่

ปี 2569 สกมช. มุ่งยกระดับความมั่นคงทางไซเบอร์ไทยสู่ยุคควอนตัม โดย

- **วางรากฐาน** พัฒนาแผนเตรียมความพร้อมและกรอบตอบสนองภัยคุกคามล่วงหน้า
- **ให้คำปรึกษา** สนับสนุนหน่วยงานภาครัฐและองค์กรโครงสร้างพื้นฐานสำคัญในการปรับตัว
- **เพิ่มขีดความสามารถ** ในการรับมือและฟื้นฟูระบบดิจิทัลทั่วประเทศ

เป้าหมาย: เพื่อระบบดิจิทัลที่ปลอดภัย ยืดหยุ่น และน่าเชื่อถือ พร้อมรับมือความเสี่ยงจากเทคโนโลยีควอนตัม

The rapid advancement of quantum computing technology poses significant risks to existing cryptographic mechanisms and introduces new forms of cyber threats.

In **2026**, NCSA will enhance national readiness for the **post-quantum era** by:

- Developing preparedness plans and response frameworks for post-quantum cyber threats
- Providing guidance and recommendations for government agencies, regulators, and organizations of critical information infrastructure (CII)
- Strengthening cybersecurity resilience across Thailand's information infrastructure and related sectors

These efforts aim to ensure that Thailand's digital systems remain secure, resilient, and trustworthy amid emerging quantum-era cyber risks.

TRUSTED สร้างความน่าเชื่อถือ ทั้งในประเทศและสากล
Building Trust at the National and International Levels

เสริมบทบาท ThaiCERT และจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (NSOC)

ภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2562 ซึ่งกำหนดให้มีนโยบาย แผนแม่บท และแผนปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์เพื่อรองรับทั้งสถานการณ์ปกติและสถานการณ์ภัยคุกคาม

ในปี 2569 นี้ สกมช. จึงมีแผนดำเนินการจัดตั้ง**ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Operation Center: NSOC)** ควบคู่กับการเสริมบทบาทของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ให้เป็นกลไกกลางในการเฝ้าระวัง ติดตาม วิเคราะห์ และประมวลผลข้อมูลภัยคุกคามทางไซเบอร์ รวมถึงการแจ้งเตือนภัยต่อหน่วยงานภาครัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อเสริมสร้างขีดความสามารถของประเทศด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นรูปธรรม และสนับสนุนการพัฒนาประเทศในระยะยาว

Strengthening the Role of ThaiCERT and Establishing the National Cyber Security Operations Center (NSOC)

Under the **Cybersecurity Act, B.E. 2562 (2019)**, which mandates the formulation of policies, master plans, and operational plans for cybersecurity.

In **2026 (B.E. 2569)**, the National Cyber Security Agency (NCSA) planned to intention the **National Cyber Security Operations Center (NSOC)** in parallel with strengthening the role of **ThaiCERT** as the national focal point for cybersecurity.

NSOC will serve as a central hub responsible for:

- Monitoring, tracking, analyzing, and processing cyber threat intelligence
- Issuing timely alerts to government agencies, regulators, and Critical Information Infrastructure (CII) organizations
- Enhancing national cybersecurity capabilities in a systematic and sustainable manner
- Supporting long-term national development and strengthening digital trust

เดินหน้ากิจกรรมระบบช่วยเหลือ (Help Desk)

ThaiCERT ทำหน้าที่เป็นศูนย์กลางให้คำปรึกษา รับแจ้งเหตุและแจ้งเตือนภัยคุกคามทางไซเบอร์แก่หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผ่านระบบช่วยเหลือ (Help Desk) ที่รองรับการรับแจ้ง วิเคราะห์ และตอบสนองต่อเหตุการณ์อย่างทันท่วงทีและครบวงจร

ในปี 2569 สกมช. มีแผนดำเนินงานต่อเนื่องเพื่อให้ Help Desk รองรับการแจ้งเหตุเชิงรุกในหลายช่องทาง เพิ่มประสิทธิภาพการวิเคราะห์และการแจ้งเตือนภัย พร้อมพัฒนาการให้คำแนะนำและแนวทางป้องกันแก้ไขแก่หน่วยงานที่เกี่ยวข้อง เพื่อเสริมความพร้อมในการรับมือภัยคุกคามทางไซเบอร์อย่างเป็นระบบและต่อเนื่อง

Advancing the Cyber Incident Assistance System (Help Desk)

ThaiCERT serves as the national help desk for:

- Receiving incident reports
- Providing consultation and technical guidance
- Issuing cybersecurity alerts to government agencies, regulators, and CII organizations

The Help Desk operates as a **rapid and end-to-end incident response mechanism**, ensuring timely and comprehensive support.

In **2026**, NCSA plans to further enhance the Help Desk by:

- Supporting multi-channel incident reporting
- Improving threat analysis and alerting efficiency
- Upgrading advisory and mitigation guidance
- Strengthening organizational readiness for systematic and continuous cyber incident response

ยกระดับ Help Desk
Enhancing Help Desk Capabilities

รองรับการแจ้งเหตุเชิงรุกหลายช่องทาง
Supporting multi-channel cyber incident reporting

วิเคราะห์ แจ้งเตือนภัย ให้คำปรึกษา และแนวทางป้องกันแก้ไขอย่างทันท่วงที
Providing threat analysis, alerts, consultation, and mitigation guidance in a timely manner

ลดความเสี่ยงและความเสียหายจากภัยไซเบอร์
Reducing cyber risks and minimizing potential damage

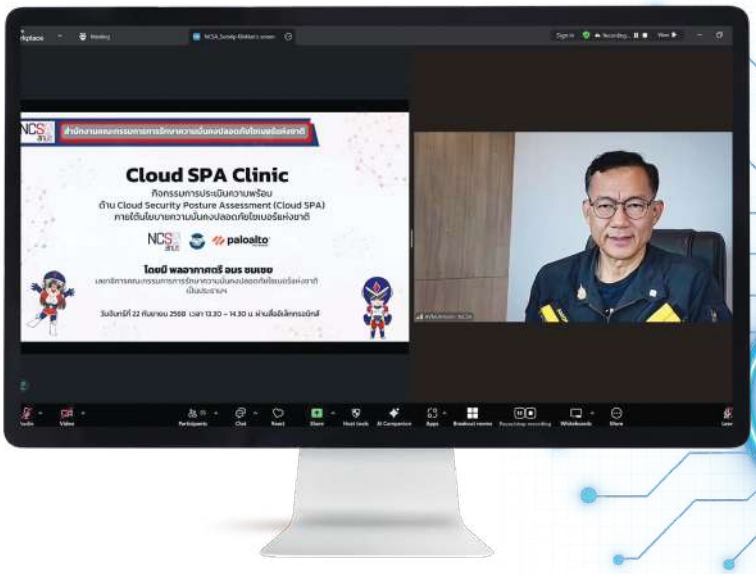
TRUSTED สร้างความน่าเชื่อถือ ทั้งในประเทศและสากล
Building Trust at the National and International Levels

ยกระดับศูนย์บริหารจัดการภัยคุกคามไซเบอร์ เสริมพลังการรับมือเชิงรุก-เชิงลึก

ภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว **ศูนย์บริหารจัดการภัยคุกคามไซเบอร์ (Cyber Threat Management and Response Center)** จึงได้รับการยกระดับขีดความสามารถอย่างต่อเนื่อง เพื่อรองรับภารกิจด้านการตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

Cyber Threat Management and Response Center Initiative

As Cyber threats become increasingly complex and are evolving at rapid pace, the Cyber Threat Management and Response Center has been continuously enhances the system capabilities in detection, analysis and effective response to cyber threats.



เตรียมความพร้อมหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ให้บริการคลาวด์ และหน่วยงานตรวจรับรองมาตรฐาน ก่อนที่มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 จะมีผลบังคับใช้

Preparing the Government Agencies, Regulatory and Supervisory Authorities, Critical Information Infrastructure Organizations, Cloud Service Providers, and Conformity Assessment Bodies Prior to the Enforcement of the Cloud Cybersecurity Standard B.E. 2567 (2024)

รัฐบาลมีการส่งเสริมให้หน่วยงานของรัฐมีการนำการประมวลผลคลาวด์เข้ามาเป็นโครงสร้างพื้นฐานหลักในการให้บริการกับประชาชนเพิ่มมากขึ้น ซึ่งจะส่งผลดีต่อเศรษฐกิจ สังคม และความมั่นคงของชาติ อย่างไรก็ตาม แนวโน้มของภัยคุกคามทางไซเบอร์ที่มีต่อการใช้บริการคลาวด์มีแนวโน้มที่สูงขึ้น ดังนั้น สกมช. จึงได้ออกมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ซึ่งจะมีผลบังคับใช้ในวันที่ 10 กันยายน 2569 โดย สกมช. ได้มีกิจกรรมส่งเสริมการเตรียมความพร้อมให้กับหน่วยงาน เช่น Cloud Security Posture Assessment, Network of Cyber Security Experts of Thailand (NOCSET)

The Government has been promoting the adoption of cloud computing by government agencies as a core infrastructure for delivering public services. This initiative is expected to generate positive impacts on the economy, society, and national security. However, cyber threats targeting cloud services have shown an increasing trend. In response, the National Cyber Security Agency (NCSA) has issued the Cloud Cybersecurity Standard B.E. 2567 (2024), which will come into force on 10 September 2026. To support readiness and compliance, NCSA has implemented various preparedness-enhancing initiatives for relevant organizations, including activities such as Cloud Security Posture Assessment (CSPA) and the Network of Cyber Security Experts of Thailand (NOCSET).

NOCSET
NETWORK OF CYBER SECURITY EXPERTS OF THAILAND

Task force "Cloud Security"
ประกอบด้วย

1 **Task force 501**
แนวปฏิบัติในการประเมิน Cloud Security Posture Assessment

2 **Task force 502**
Checklist หรือแนวปฏิบัติสำหรับการแบ่งประเภทข้อมูลหรือระบบสารสนเทศ

3 **Task force 503**
Checklist หรือแนวปฏิบัติในการประเมินตนเองสำหรับผู้ใช้บริการคลาวด์

4 **Task force 505**
แนวปฏิบัติเกี่ยวกับเทคโนโลยี Secure Cloud Adoption

5 **Task force 506**
แนวปฏิบัติเกี่ยวกับ Cloud Security Compliance Handbook

หน่วยงานที่เข้าร่วม
paloalto NETWORKS · SAP · Microsoft · salesforce · HUAWEI · aws

บทสรุปส่งท้าย
CONCLUSION

ในปีงบประมาณ พ.ศ. 2568 สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้ขับเคลื่อนภารกิจด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศภายใต้แนวคิด **"Team Thailand for Cybersecurity"** ซึ่งมุ่งเน้นการบูรณาการการทำงานร่วมกันของทุกภาคส่วน ทั้งหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภาคเอกชน ภาคการศึกษาและภาคประชาสังคม เพื่อเสริมสร้างความพร้อมของประเทศในการป้องกันและรับมือภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นคืนสู่สภาพปกติของระบบและบริการที่สำคัญของประเทศอย่างมีประสิทธิภาพ ภายใต้กรอบนโยบายและ**แผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570)** แนวคิดดังกล่าวสะท้อนบทบาทของ สกมช. ในฐานะกลไกกลางระดับชาติในการเชื่อมโยงนโยบาย การกำกับดูแล และการปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์เข้าด้วยกัน เพื่อยกระดับความมั่นคงปลอดภัยของบริการภาครัฐ โครงสร้างพื้นฐานสำคัญและระบบเศรษฐกิจดิจิทัลของประเทศ ท่ามกลางบริบทของภัยคุกคามไซเบอร์ที่มีความซับซ้อน เปลี่ยนแปลงอย่างรวดเร็ว และส่งผลกระทบในวงกว้างต่อความมั่นคง เศรษฐกิจ และสังคม

สกมช. ให้ความสำคัญกับการ**ยกระดับขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศในทุกมิติ** ตั้งแต่การกำหนดมาตรการและมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การเสริมสร้างความพร้อมในการป้องกันและการฟื้นคืนสู่สภาพปกติของระบบที่สำคัญของประเทศ ไปจนถึงการพัฒนาแนวทางการบริหารจัดการความเสี่ยงทางไซเบอร์ในระดับองค์กรและระดับประเทศ เพื่อให้บริการสาธารณะและระบบสำคัญสามารถดำเนินการได้อย่างต่อเนื่องและมีเสถียรภาพ

นอกจากนี้ สกมช. ได้ให้ความสำคัญอย่างยิ่งกับการยกระดับและ**พัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ในทุกระดับ** เพื่อสร้างกำลังคนที่มีความรู้ ความเชี่ยวชาญและพร้อมรองรับภารกิจด้านไซเบอร์ของประเทศทั้งในภาวะปกติและภาวะวิกฤต โดยมุ่งเน้นการพัฒนาทักษะเชิงลึกควบคู่กับการสร้างความเข้าใจเชิงนโยบายและการบริหารจัดการความเสี่ยงให้แก่ผู้บริหารและผู้ปฏิบัติงานในหน่วยงานของรัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และภาคเอกชน ตลอดจนการส่งเสริมการเรียนรู้ การฝึกอบรมเชิงปฏิบัติการ และการรับรองสมรรถนะตามมาตรฐานสากล ซึ่งมีส่วนสำคัญในการลดช่องว่างด้านทักษะและเสริมสร้างฐานกำลังคนด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ

ในด้านการ**เตรียมความพร้อมและการรับมือภัยคุกคาม** สกมช. ได้ดำเนินการจัดการฝึกซ้อมรับมือภัยคุกคามไซเบอร์ในระดับประเทศอย่างต่อเนื่อง เพื่อเพิ่มประสิทธิภาพในการตอบสนองต่อเหตุการณ์และลดผลกระทบจากภัยคุกคามทางไซเบอร์ที่อาจส่งผลต่อความมั่นคงของรัฐ บริการสาธารณะ และความเชื่อมั่นของประชาชน ควบคู่กับการเสริมสร้างกลไกการเฝ้าระวัง แจ้งเตือน และตอบสนองต่อเหตุการณ์ไซเบอร์ในระดับชาติ ผ่านการดำเนินงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) เพื่อให้การรับมือภัยคุกคามเป็นไปอย่างทันท่วงที ขณะเดียวกัน สกมช. ได้ผลักดันการบูรณาการความร่วมมือทั้งในประเทศและระหว่างประเทศ เพื่อแลกเปลี่ยนข้อมูลภัยคุกคาม องค์ความรู้ และแนวปฏิบัติที่ดีด้านความมั่นคงปลอดภัยไซเบอร์ อันนำไปสู่การยกระดับบทบาทของประเทศไทยในเวทีความมั่นคงปลอดภัยไซเบอร์ระดับภูมิภาคและระดับโลก

ในปี **พ.ศ. 2569** สกมช. จะยังคงมุ่งมั่นยกระดับความพร้อมของประเทศอย่างต่อเนื่องในการป้องกัน รับมือ และจัดการภัยคุกคามทางไซเบอร์ในทุกรูปแบบ ควบคู่กับการเสริมสร้างระบบนิเวศด้านความมั่นคงปลอดภัยไซเบอร์ที่เข้มแข็ง เพื่อมุ่งสู่การสร้าง **"ความปลอดภัยต่อประชาชน ความมั่นคงต่อระบบ และความน่าเชื่อถือต่อทุกภาคส่วน" (Safe, Secure, and Trusted Cyberspace for Thailand)** อันจะเป็นรากฐานสำคัญในการคุ้มครองประโยชน์สาธารณะ เสริมสร้างความเชื่อมั่นของประชาชน และสนับสนุนการพัฒนาประเทศอย่างมั่นคงและยั่งยืน

In Fiscal Year 2025 (B.E. 2568), the **NCSA** successfully advanced Thailand's national cybersecurity mission under the guiding concept of **"Team Thailand for Cybersecurity."** This approach emphasizes integrated collaboration across all sectors, including government agencies, regulatory authorities, organizations of critical information infrastructure (CII), the private sector, academia, and civil society, to collectively strengthen national capabilities in preventing, responding to, and recovering from cyber threats.

The implementation of this approach has enabled Thailand to enhance the resilience and continuity of critical systems and essential public services, in alignment with the **National Cybersecurity Policy and Action Plan (B.E. 2565-2570)**. The role of NCSA as the central coordinating body has been clearly reflected in its functions of policy formulation, regulatory oversight, operational coordination, and capacity building, ensuring a coherent national cybersecurity framework.

NCSA has placed strong emphasis on **enhancing national cybersecurity capabilities across all dimensions**, starting from the establishment of cybersecurity standards and minimum security requirements for government agencies, regulators, and organizations of CII, to strengthening preparedness for cyber incident prevention, detection, response, and recovery. At the same time, NCSA has continuously promoted organizational and national-level cyber resilience to ensure that public services and critical systems can operate in a stable and uninterrupted manner.

In addition, NCSA has prioritized the **development of cybersecurity human capital** at all levels. This includes advancing technical expertise, policy understanding, and risk management capabilities among executives, practitioners, and operational personnel across government agencies and critical sectors. Through continuous learning, hands-on training, operational exercises, and international-standard certifications, these efforts contribute significantly to narrowing the cybersecurity skills gap and strengthening Thailand's national cybersecurity workforce.

In terms of **preparedness and cyber incident response**, NCSA has continuously conducted national-level cyber exercises to improve response efficiency and minimize the impact of cyber threats on national security, public services, and public trust. At the same time, NCSA has strengthened national monitoring, early warning, and alert mechanisms through the operations of **ThaiCERT**, ensuring timely and coordinated responses to cyber incidents.

In parallel, NCSA has reinforced cross-sectoral and international collaboration to facilitate knowledge exchange, best practices, and the adoption of internationally aligned cybersecurity guidelines. These efforts collectively elevate Thailand's role and standing in regional and global cybersecurity cooperation.

Looking ahead to **Fiscal Year 2026**, NCSA will continue to focus on enhancing Thailand's cybersecurity readiness in a comprehensive and sustainable manner. This includes strengthening prevention, response, and recovery capabilities across all sectors, as well as fostering a robust national cybersecurity ecosystem.

The ultimate goal is to realize the vision of:

"Safe, Secure, and Trusted Cyberspace for Thailand" - ensuring **safety for citizens, security for critical systems and public services**, and **trust at both national and international levels**, as a cornerstone for sustainable national development and long-term digital resilience.

4 FINANCIAL REPORT

รายงานการเงิน

ดาวน์โหลด รายงานทางการเงิน สกมช. 2568

รายงานของผู้สอบบัญชีรับอนุญาต และรายงานการเงิน

รายงานการประเมินผล การใช้จ่ายเงินและทรัพย์สิน

รายงานการสอบทาน ระบบการควบคุมภายใน

รายงานของผู้สอบบัญชีรับอนุญาตและรายงานการเงิน

สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2568

รายงานของผู้สอบบัญชีรับอนุญาต

เสนอ คณะกรรมการบริหาร สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์

ความเห็น

ข้าพเจ้าได้ตรวจสอบรายงานการเงินของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (“หน่วยงาน”) ซึ่งประกอบด้วยงบแสดงฐานะการเงิน ณ วันที่ 30 กันยายน 2568 งบแสดงผลการดำเนินงานทางการเงิน และงบแสดงการเปลี่ยนแปลงสินทรัพย์สุทธิ/ส่วนทุน สำหรับปีสิ้นสุดวันเดียวกันและหมายเหตุประกอบงบการเงิน รวมถึงสรุปนโยบายการบัญชีที่สำคัญ

ข้าพเจ้าเห็นว่า รายงานการเงินข้างต้นนี้แสดงฐานะการเงินของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ณ วันที่ 30 กันยายน 2568 และผลการดำเนินงาน สำหรับปีสิ้นสุดวันเดียวกันโดยถูกต้องตามที่ควรในสาระสำคัญตามมาตรฐานการบัญชีภาครัฐและนโยบายการบัญชีภาครัฐที่กระทรวงการคลังกำหนด

เกณฑ์ในการแสดงความเห็น

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

ข้อมูลอื่น

ผู้บริหารเป็นผู้รับผิดชอบต่อข้อมูลอื่น ข้อมูลอื่นประกอบด้วยข้อมูลซึ่งรวมอยู่ในรายงานประจำปีแต่ไม่รวมถึงรายงานการเงินและรายงานของผู้สอบบัญชีที่อยู่ในรายงานนั้น ซึ่งคาดว่ารายงานประจำปีจะถูกจัดเตรียมให้ข้าพเจ้าภายหลังวันที่ในรายงานของผู้สอบบัญชีนี้

ความเห็นของข้าพเจ้าต่อรายงานการเงินไม่ครอบคลุมถึงข้อมูลอื่นและข้าพเจ้าไม่ได้ให้ความเชื่อมั่นต่อข้อมูลอื่น

ความรับผิดชอบของข้าพเจ้าที่เกี่ยวเนื่องกับการตรวจสอบรายงานการเงินคือ การอ่านและพิจารณาว่าข้อมูลอื่นมีความขัดแย้งที่มีสาระสำคัญกับรายงานการเงินหรือกับความรู้ที่ได้รับจากการตรวจสอบของข้าพเจ้า หรือปรากฏว่าข้อมูลอื่นมีการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญหรือไม่

เมื่อข้าพเจ้าได้อ่านรายงานประจำปี หากข้าพเจ้าสรุปได้ว่ามีการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญ ข้าพเจ้าต้องสื่อสารเรื่องดังกล่าวกับผู้มีหน้าที่ในการกำกับดูแล เพื่อให้ผู้มีหน้าที่ในการกำกับดูแลดำเนินการแก้ไขข้อมูลที่แสดงขัดต่อข้อเท็จจริง

ความรับผิดชอบของผู้บริหารและผู้มีหน้าที่ในการกำกับดูแลต่อรายงานการเงิน

ผู้บริหารมีหน้าที่รับผิดชอบในการจัดทำและนำเสนอรายงานการเงินเหล่านี้โดยถูกต้องตามที่ควรตามมาตรฐานการบัญชีภาครัฐและนโยบายการบัญชีภาครัฐที่กระทรวงการคลังกำหนด และรับผิดชอบเกี่ยวกับการควบคุมภายในที่ผู้บริหารพิจารณาว่าจำเป็นเพื่อให้สามารถจัดทำรายงานการเงินที่ปราศจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญไม่ว่าจะเกิดจากการทุจริตหรือข้อผิดพลาด

ในการจัดทำรายงานการเงิน ผู้บริหารรับผิดชอบในการประเมินความสามารถของหน่วยงานในการดำเนินงานต่อเนื่อง เปิดเผยเรื่องที่เกี่ยวกับการดำเนินงานต่อเนื่องตามความเหมาะสม และการใช้เกณฑ์การบัญชีสำหรับการดำเนินงานต่อเนื่อง เว้นแต่มีข้อกำหนดในกฎหมายหรือเป็นนโยบายรัฐบาลที่จะเลิกหน่วยงานหรือหยุดดำเนินงาน หรือไม่สามารถดำเนินงานต่อเนื่องต่อไปได้

ผู้มีหน้าที่ในการกำกับดูแลมีหน้าที่ในการกำกับดูแลกระบวนการในการจัดทำรายงานทางการเงินของหน่วยงาน

ความรับผิดชอบของผู้สอบบัญชีต่อการตรวจสอบรายงานการเงิน

การตรวจสอบของข้าพเจ้ามีวัตถุประสงค์เพื่อให้ได้ความเชื่อมั่นอย่างสมเหตุสมผลว่ารายงานการเงินโดยรวมปราศจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญหรือไม่ ไม่ว่าจะเกิดจากการทุจริตหรือข้อผิดพลาด และเสนอรายงานของผู้สอบบัญชีซึ่งรวมความเห็นของข้าพเจ้าอยู่ด้วย ความเชื่อมั่นอย่างสมเหตุสมผลคือความเชื่อมั่นในระดับสูงแต่ไม่ได้เป็นการรับประกันว่าการปฏิบัติงานตรวจสอบตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินและมาตรฐานการสอบบัญชีจะสามารถตรวจพบข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญที่มีอยู่ได้เสมอไป ข้อมูลที่ขัดต่อข้อเท็จจริงอาจเกิดจากการทุจริตหรือข้อผิดพลาดและถือว่ามีสาระสำคัญเมื่อคาดการณ์ได้อย่างสมเหตุสมผลว่ารายการที่ขัดต่อข้อเท็จจริงแต่ละรายการหรือทุกรายการรวมกันจะมีผลต่อการตัดสินใจทางเศรษฐกิจของผู้ใช้งบการเงินจากการใช้รายงานการเงินเหล่านี้

ในการตรวจสอบของข้าพเจ้าตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินและมาตรฐานการสอบบัญชี ข้าพเจ้าได้ใช้ดุลยพินิจและการสังเกตและสงสัยเยี่ยงผู้ประกอบวิชาชีพตลอดการตรวจสอบ การปฏิบัติงานของข้าพเจ้ารวมถึง

- ระบุและประเมินความเสี่ยงจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญในรายงานการเงินไม่ว่าจะเกิดจากการทุจริตหรือข้อผิดพลาด ออกแบบและปฏิบัติงานตามวิธีการตรวจสอบเพื่อตอบสนองต่อความเสี่ยงเหล่านั้น และได้หลักฐานการสอบบัญชีที่เพียงพอและเหมาะสมเพื่อใช้เป็นเกณฑ์ในการแสดงความเห็นของข้าพเจ้า ความเสี่ยงที่ไม่พบข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญซึ่งเป็นผลมาจากการทุจริตจะสูงกว่าความเสี่ยงที่เกิดจากข้อผิดพลาด เนื่องจากการทุจริตอาจเกี่ยวกับการสมรู้ร่วมคิด การปลอมแปลงเอกสารหลักฐาน การตั้งใจละเว้นการแสดงข้อมูล การแสดงข้อมูลที่ไม่ตรงตามข้อเท็จจริงหรือการแทรกแซงการควบคุมภายใน

- ทำความเข้าใจในระบบการควบคุมภายในที่เกี่ยวข้องกับการตรวจสอบ เพื่อออกแบบวิธีการตรวจสอบที่เหมาะสมกับสถานการณ์แต่ไม่ใช่เพื่อวัตถุประสงค์ในการแสดงความเห็นต่อความมีประสิทธิผลของการควบคุมภายในของหน่วยงาน

- ประเมินความเหมาะสมของนโยบายการบัญชีที่ผู้บริหารใช้และความสมเหตุสมผลของประมาณการทางบัญชีและการเปิดเผยข้อมูลที่เกี่ยวข้องซึ่งจัดทำขึ้นโดยผู้บริหาร

- สรุปเกี่ยวกับความเหมาะสมของการใช้เกณฑ์การบัญชีสำหรับการดำเนินงานต่อเนื่องของผู้บริหาร และจากหลักฐานการสอบบัญชีที่ได้รับ สรุปว่ามีความไม่แน่นอนที่มีสาระสำคัญที่เกี่ยวกับเหตุการณ์หรือสถานการณ์ที่อาจเป็นเหตุให้เกิดข้อสงสัยอย่างมีนัยสำคัญต่อความสามารถของหน่วยงานในการดำเนินงานต่อเนื่องหรือไม่ ถ้าข้าพเจ้าได้ข้อสรุปว่ามีความไม่แน่นอนที่มีสาระสำคัญข้าพเจ้าต้องกล่าวไว้ในรายงานของผู้สอบบัญชีของข้าพเจ้าโดยให้ข้อสังเกตถึงการเปิดเผยข้อมูลในรายงานการเงินที่เกี่ยวข้องหรือถ้าการเปิดเผย ข้อมูลดังกล่าวไม่เพียงพอ ความเห็นของข้าพเจ้าจะเปลี่ยนแปลงไป ข้อสรุปของข้าพเจ้าขึ้นอยู่กับหลักฐานการสอบบัญชีที่ได้รับจนถึงวันที่ในรายงานของผู้สอบบัญชีของข้าพเจ้า อย่างไรก็ตามเหตุการณ์หรือสถานการณ์ในอนาคตอาจเป็นเหตุให้หน่วยงานต้องหยุดการดำเนินงานต่อเนื่อง

- ประเมินการนำเสนอ โครงสร้าง และเนื้อหาของรายงานการเงินโดยรวม รวมถึงการเปิดเผยข้อมูลว่ารายงานการเงินแสดงรายการและเหตุการณ์ในรูปแบบที่ทำให้มีการนำเสนอข้อมูลโดยถูกต้องตามที่ควรหรือไม่

ข้าพเจ้าได้สื่อสารกับผู้มีหน้าที่ในการกำกับดูแลในเรื่องต่าง ๆ ที่สำคัญ ซึ่งรวมถึงขอบเขตและช่วงเวลาของการตรวจสอบตามที่ได้วางแผนไว้ประเด็นที่มีนัยสำคัญที่พบจากการตรวจสอบรวมถึงข้อบกพร่องที่มีนัยสำคัญในระบบการควบคุมภายในหากข้าพเจ้าได้พบในระหว่างการตรวจสอบของข้าพเจ้า

ผู้สอบบัญชีที่รับผิดชอบงานสอบบัญชีและนำเสนอรายงานฉบับนี้คือ นายสุวัฒน์ มณีกนกสกุล

(นายสุวัฒน์ มณีกนกสกุล)
ผู้สอบบัญชีรับอนุญาต ทะเบียนเลขที่ 8134

บริษัท สอบบัญชีธรรมมิติ จำกัด
กรุงเทพมหานคร
วันที่ 8 มกราคม 2569

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
งบแสดงฐานะการเงิน ณ วันที่ 30 กันยายน 2568

หน่วย:บาท

	หมายเหตุ	2568	2567
สินทรัพย์			
สินทรัพย์หมุนเวียน			
เงินสดและรายการเทียบเท่าเงินสด	4	354,813,068.15	352,397,458.80
ลูกหนี้อื่นระยะสั้น	5	12,194,957.74	18,296,555.87
วัสดุคงเหลือ	6	1,154,501.07	1,192,435.73
รวมสินทรัพย์หมุนเวียน		368,162,526.96	371,886,450.40
สินทรัพย์ไม่หมุนเวียน			
อาคารและอุปกรณ์ - สุทธิ	7	238,333,602.98	130,730,634.34
สินทรัพย์ไม่มีตัวตน - สุทธิ	8	46,396,845.59	129,802,427.80
รวมสินทรัพย์ไม่หมุนเวียน		284,730,448.57	260,533,062.14
รวมสินทรัพย์		652,892,975.53	632,419,512.54
หนี้สินและสินทรัพย์สุทธิ/ส่วนทุน			
หนี้สิน			
หนี้สินหมุนเวียน			
เจ้าหนี้การค้า	9	129,445,860.20	30,911,256.35
เจ้าหนี้เงินโอนและรายการอุดหนุนระยะสั้น	10	11,988,180.56	113,172,874.00
เจ้าหนี้อื่นระยะสั้น	11	1,503,904.58	1,307,508.44
เงินรับฝากระยะสั้น	12	6,593,590.71	7,793,258.63
รวมหนี้สินหมุนเวียน		149,531,536.05	153,184,897.42
รวมหนี้สิน		149,531,536.05	153,184,897.42
สินทรัพย์สุทธิ/ส่วนทุน			
ทุน		-	-
รายได้สูง/(ต่ำ) กว่าค่าใช้จ่ายสะสม	14	503,361,439.48	479,234,615.12
รวมสินทรัพย์สุทธิ/ส่วนทุน		503,361,439.48	479,234,615.12
รวมหนี้สินและสินทรัพย์สุทธิ/ส่วนทุน		652,892,975.53	632,419,512.54

ขอรับรองว่าเป็นรายการอันถูกต้องและเป็นจริง

พันโท (ปณต แสงทับทิม)
ผู้อำนวยการสำนักการเงินและกลยุทธ์องค์กร

พลอากาศตรี (อมร ชมเชย)
เลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หมายเหตุประกอบงบการเงินเป็นส่วนหนึ่งของรายงานการเงินนี้

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
งบแสดงผลการดำเนินงานทางการเงิน
สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2568

หน่วย:บาท

	หมายเหตุ	2568	2567
รายได้			
รายได้จากงบประมาณ	15	517,316,472.00	497,067,800.00
รายได้จากการอุดหนุนจากหน่วยงานภาครัฐ	16	497,642,339.44	111,218,486.00
รวมรายได้		**1,014,958,811.44**	**608,286,286.00**
ค่าใช้จ่าย			
ค่าใช้จ่ายบุคลากร	17	100,028,729.82	68,062,811.92
ค่าตอบแทน	18	2,084,730.00	1,599,800.00
ค่าใช้สอย	19	718,852,807.73	238,453,523.28
ค่าวัสดุ	20	2,849,276.75	9,459,317.81
ค่าสาธารณูปโภค	21	4,257,298.69	736,289.25
ค่าเสื่อมราคาและค่าตัดจำหน่าย	22	162,759,144.09	96,515,925.57
รวมค่าใช้จ่าย		**990,831,987.08**	**414,827,667.83**
รายได้สูง/(ต่ำ) กว่าค่าใช้จ่ายสุทธิ		**24,126,824.36**	**193,458,618.17**

ขอรับรองว่าเป็นรายการอันถูกต้องและเป็นจริง

พันโท (ปณต แสงทับทิม)
ผู้อำนวยการสำนักการเงินและกลยุทธ์องค์กร

พลอากาศตรี (อมร ชมเชย)
เลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หมายเหตุประกอบงบการเงินเป็นส่วนหนึ่งของรายงานการเงินนี้

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
งบแสดงการเปลี่ยนแปลงสินทรัพย์สุทธิ/ส่วนทุน
สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2568

หน่วย:บาท

	หมายเหตุ	ทุน	รายได้สูงกว่าค่าใช้จ่ายสะสม	รวมสินทรัพย์สุทธิ/ส่วนทุน
ยอดคงเหลือ ณ วันที่ 1 ตุลาคม 2566 - ตามที่รายงานไว้เดิม		-	265,665,144.11	265,665,144.11
ผลสะสมจากการแก้ไขข้อผิดพลาดปีก่อน		-	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				
รายได้สูง/(ต่ำ)กว่าค่าใช้จ่ายสำหรับปี		-	193,458,618.17	193,458,618.17
ยอดคงเหลือ ณ วันที่ 30 กันยายน 2567		-	479,234,615.12	479,234,615.12

หน่วย:บาท

	ทุน	รายได้สูงกว่าค่าใช้จ่ายสะสม	รวมสินทรัพย์สุทธิ/ส่วนทุน
ยอดคงเหลือ ณ วันที่ 1 ตุลาคม 2567	-	479,234,615.12	479,234,615.12
การเปลี่ยนแปลงสินทรัพย์สุทธิ/ส่วนทุน สำหรับปี 2568			
รายได้สูง/(ต่ำ)กว่าค่าใช้จ่ายสำหรับปี	-	24,126,824.36	24,126,824.36
ยอดคงเหลือ ณ วันที่ 30 กันยายน 2568	-	503,361,439.48	503,361,439.48

ขอรับรองว่าเป็นรายการอันถูกต้องและเป็นจริง

พันโท
(ปณต แสงทับทิม)
ผู้อำนวยการสำนักการเงินและกลยุทธ์องค์กร

พลอากาศตรี
(อมร ชมเชย)
เลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หมายเหตุประกอบงบการเงินเป็นส่วนหนึ่งของรายงานการเงินนี้

5 PERFORMANCE EVALUATION

การประเมินผลการดำเนินงาน

การประเมินผลการดำเนินงาน
PERFORMANCE EVALUATION

การประเมินผลการดำเนินงานของ สกมช. เป็นการประเมินผลโดยบุคคลภายนอกที่ กบส. เห็นชอบ (บริษัท วินทูเกเตอร์ จำกัด) ทั้งนี้ มติที่ประชุม กบส. เมื่อวันที่ 30 ตุลาคม 2568 เห็นชอบผลการประเมินดังกล่าว โดยแบ่งออกเป็น 2 องค์ประกอบ ดังนี้

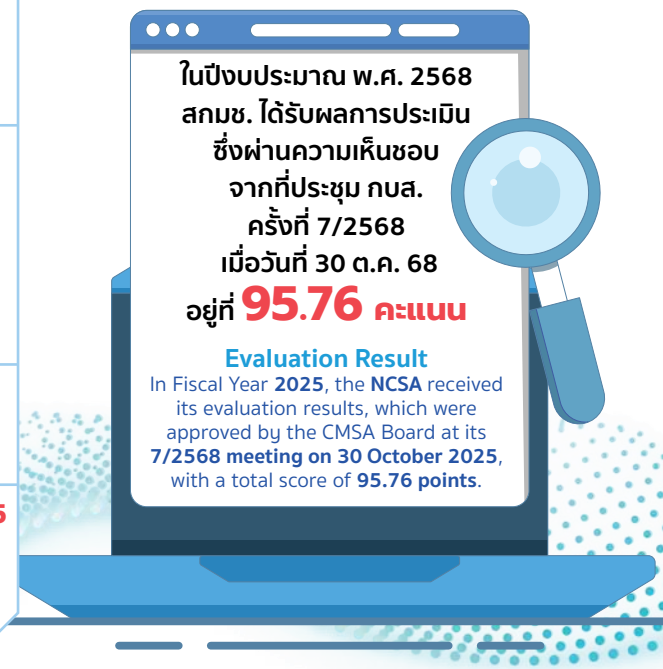
The performance evaluation of the NCSA was conducted by an external evaluator approved by the Board (Win2Gether Co., Ltd.). The Board meeting held on 30 October 2025 approved the evaluation results, which are divided into two components, as follows:

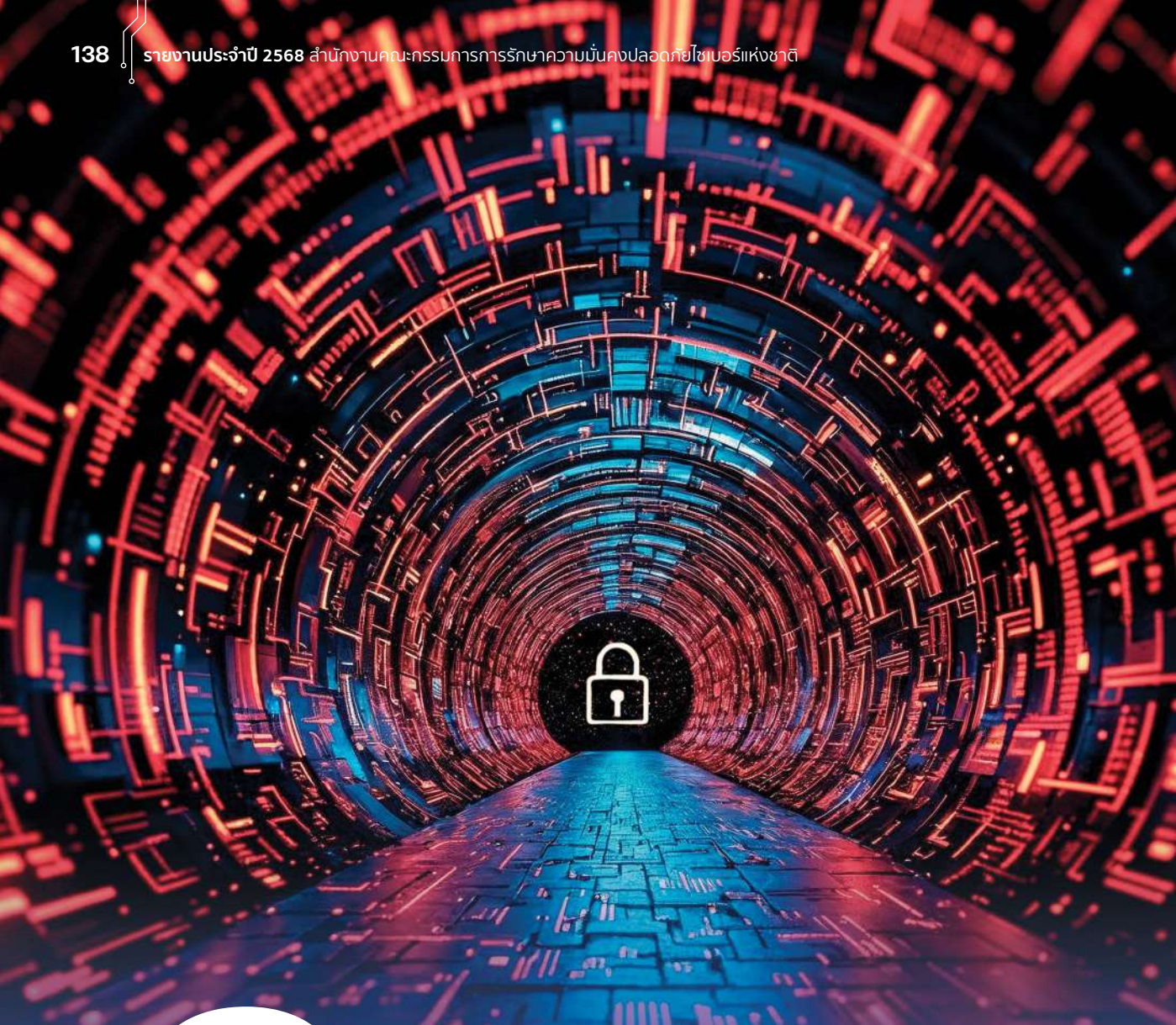
องค์ประกอบที่ 1
Component 1
การประเมินประสิทธิภาพ ประสิทธิผลการดำเนินงาน
Performance Effectiveness Evaluation
ร้อยละ Weight **70%**

	ตัวชี้วัด Indicators	ได้ร้อยละ Percentage
1.1	ร้อยละความสำเร็จในการติดตามประเมินผลการดำเนินงานของหน่วยงานเป้าหมายภายใต้นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565-2570 Percentage of success in monitoring and evaluating the performance of target agencies under the Cybersecurity Policy and Action Plan B.E. 2565-2570 (2022-2027)	10.5
1.2	ร้อยละของหน่วยงานที่ ThaiCERT สนับสนุนปฏิบัติการทางไซเบอร์ได้ตามกำหนดเวลา Percentage of agencies for which ThaiCERT provided cybersecurity operational support within the specified timeframe	14
1.3	ระดับความสำเร็จของจำนวนหน่วยงานเป้าหมายแพลตฟอร์มสำหรับการรับและแบ่งปันเหตุการณ์ภัยคุกคามทางไซเบอร์ Level of success of target agencies having a platform for receiving and sharing cyber threat incident information	14
1.4	ร้อยละความสำเร็จของจำนวนบุคลากรผู้ผ่านการอบรมพัฒนาขีดความสามารถกระบวนการปฏิบัติงานด้านไซเบอร์ตามมาตรฐานสากล (Lead Implementor และ Lead Auditor) Percentage of success in the number of personnel who have completed training to enhance cybersecurity operational capabilities in accordance with international standards (Lead Implementer and Lead Auditor)	14
1.5	ความสำเร็จในการจัดทำแผนเผชิญเหตุด้านไซเบอร์ของหน่วยงานเป้าหมาย Success in the development of a Cyber Incident Response Plan for target agencies	7
1.6	ตัวชี้วัดร่วมขององค์การมหาชนการป้องกันและคุ้มครองข้อมูลส่วนบุคคลจากภัยทางไซเบอร์ Composite indicator of organizational effectiveness in preventing and protecting personal data from cyber threats	10.5

องค์ประกอบที่ 2
Component 2
การประเมินศักยภาพขององค์การมหาชน
Organizational Capability Evaluation
ร้อยละ Weight **30%**

	ตัวชี้วัด Indicators	ได้ร้อยละ Percentage
2.1	การประเมินระดับความพร้อมรัฐบาลดิจิทัล (DG Readiness Survey) Assessment of national digital readiness (DG Readiness Survey)	7.5
2.2	ผลการประเมินสถานะของ สกมช. ในการเป็นระบบราชการ 4.0 (PMQA 4.0) Results of the NCSA's evaluation under the Government 4.0 framework (PMQA 4.0)	8.2
2.3	ความสำเร็จของการประเมินการควบคุมดูแลกิจการของคณะกรรมการองค์การมหาชน Success in evaluating the effectiveness of internal control systems of the public organization the public organization board	10





6 ISSUES, CHALLENGES AND RECOMMENDATIONS

ปัญหา อุปสรรค และข้อเสนอแนะ

ปัญหาและอุปสรรค
CHALLENGES

ตลอดปีงบประมาณ พ.ศ. 2568 ประเทศไทยเผชิญกับสถานการณ์ภัยคุกคามไซเบอร์ที่ทวีความรุนแรงและซับซ้อนมากขึ้นอย่างต่อเนื่อง ทั้งในเชิงปริมาณและรูปแบบของการโจมตี ภัยคุกคามดังกล่าวพัฒนาไปพร้อมกับความก้าวหน้าของเทคโนโลยีดิจิทัล โดยเฉพาะการนำปัญญาประดิษฐ์และเทคนิคการหลอกลวงเชิงจิตวิทยามาใช้ ส่งผลให้ขอบเขตความเสี่ยงขยายตัวครอบคลุมภาครัฐ ภาคเอกชน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ และประชาชนทั่วไป

แม้ว่าหลายภาคส่วนจะตื่นตัวและเริ่มยกระดับมาตรการด้านความมั่นคงปลอดภัยไซเบอร์มากขึ้น แต่ระดับความพร้อมของหน่วยงานและองค์กรยังมีความแตกต่างกันอย่างมีนัยสำคัญ โดยเฉพาะหน่วยงานขนาดเล็ก หน่วยงานในส่วนภูมิภาค และผู้ประกอบการขนาดกลางและขนาดย่อม ซึ่งยังประสบข้อจำกัดด้านบุคลากร ความเชี่ยวชาญ และทรัพยากร ส่งผลให้การป้องกันและการตอบสนองต่อเหตุการณ์ไซเบอร์ยังไม่เป็นไปอย่างทั่วถึงและเท่าเทียม

ในมิติของการบูรณาการระดับประเทศ การแลกเปลี่ยนข้อมูลภัยคุกคามและการประสานความร่วมมือระหว่างหน่วยงาน แม้จะมีพัฒนาการที่ชัดเจนมากขึ้น แต่ยังต้องเผชิญกับความท้าทายด้านความเชื่อมั่น ข้อจำกัดทางกฎหมาย และความแตกต่างของกระบวนการทำงานในแต่ละหน่วยงาน ทำให้การสร้างภาพรวมสถานการณ์ไซเบอร์ระดับประเทศยังไม่สามารถดำเนินการได้อย่างเต็มศักยภาพ

ในระดับสังคมและประชาชน แม้การสร้างการรับรู้ด้านภัยคุกคามไซเบอร์จะเข้าถึงประชาชนในวงกว้างมากขึ้น แต่พฤติกรรมการใช้งานดิจิทัลที่ยังขาดความระมัดระวัง ทำให้ประชาชนจำนวนไม่น้อยยังคงตกเป็นเหยื่อของอาชญากรรมไซเบอร์อย่างต่อเนื่อง สะท้อนให้เห็นถึงความท้าทายในการเปลี่ยนการรับรู้ให้กลายเป็นพฤติกรรมที่ปลอดภัยอย่างยั่งยืน

Throughout Fiscal Year 2025, Thailand has continued to face increasingly severe and complex cybersecurity threats, both in scale and in the variety of attack methods. These threats have evolved alongside rapid advances in digital technology-particularly the adoption of artificial intelligence and psychological manipulation techniques-expanding the risk landscape across the public sector, private sector, critical information infrastructure, and the general public.

Although many sectors have became more aware and have begun strengthening cybersecurity measures, the level of preparedness among agencies and organizations remains uneven. In particular, small agencies, regional organizations, and small and medium-sized enterprises (SMEs) continue to face limitations in personnel, expertise, and resources. As a result, cybersecurity prevention and incident response capabilities are not yet comprehensive or equitable nationwide.

Challenges at the National Integration Level
While mechanisms for information sharing and inter-agency coordination have become clearer, challenges persist in terms of trust, legal constraints, and differences in operational processes among agencies. These factors hinder the ability to develop a complete and unified national-level cybersecurity situational awareness framework.

Challenges at the Societal and Public Level
Despite broader public awareness of cyber threats, unsafe digital behaviors remain widespread. A significant number of citizens continue to fall victim to cybercrime, highlighting the ongoing challenge of transforming awareness into sustainable, secure digital behaviors.

ข้อเสนอแนะ
RECOMMENDATIONS

จากภาพรวมของปัญหาและอุปสรรคดังกล่าว เห็นควรให้ประเทศมุ่งเน้นดำเนินการดังนี้
Based on the overall assessment of challenges and obstacles, Thailand should prioritize the following actions:

ข้อเสนอแนะเชิงยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์
Strategic Recommendations for Cybersecurity

1 ยกระดับความมั่นคงปลอดภัยไซเบอร์เชิงระบบและบูรณาการ
Strengthen Systemic and Integrated Cybersecurity

- มุ่งเน้นการพัฒนาศักยภาพของทุกภาคส่วนอย่างสมดุล
  Focus on balanced capacity development across all sectors
- สร้างความร่วมมือระดับประเทศ เพื่อรับมือภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็ว
  Enhance nationwide collaboration to respond effectively to rapidly evolving cyber threats

2 เสริมสร้างความเข้มแข็งของกลไกการประสานงานระดับประเทศ
Reinforce National Coordination Mechanisms

- แลกเปลี่ยนข้อมูลภัยคุกคามได้อย่างทันท่วงที มีมาตรฐาน และบนพื้นฐานความเชื่อมั่นร่วมกัน
  Enable timely, standardized cyber threat information sharing
- ใช้ข้อมูลข่าวกรองภัยคุกคามเชิงลึกเป็นฐานในการตัดสินใจเชิงนโยบาย
  Utilize in-depth threat intelligence data to support policy-level decision-making

3 พัฒนาศักยภาพบุคลากรและประชาชน
Develop Human Capacity for Both Professionals and the Public

- ยกระดับความรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์ของรัฐ เอกชน และประชาชน
  Enhance cybersecurity knowledge and skills across government, private sector, and citizens
- พัฒนาบุคลากรเชิงลึกในสาขาที่สำคัญต่ออนาคต
  Develop advanced expertise in future-critical cybersecurity domains
- สร้างความตระหนักรู้และเปลี่ยนพฤติกรรมอย่างเป็นรูปธรรม
  Promote awareness and encourage sustainable behavior change

4 ปรับปรุงกรอบกฎหมายและมาตรการที่เกี่ยวข้อง
Improve Legal and Regulatory Frameworks

- ให้สอดคล้องกับบริบทเทคโนโลยีที่เปลี่ยนแปลง
  Align laws and regulations with evolving technological landscapes
- สนับสนุนการดำเนินมาตรการด้านความมั่นคงปลอดภัยไซเบอร์เชิงป้องกันและเชิงรุก
  Support both preventive and reactive cybersecurity measures
- ยึดหลักธรรมาภิบาลและการคุ้มครองสิทธิของประชาชน
  Uphold ethical principles and protect citizens' rights

บทสรุปเชิงภาพรวม
CONCLUSION

จากผลการดำเนินงานในปี พ.ศ. 2568 ปัญหาและอุปสรรคที่เกิดขึ้นสะท้อนให้เห็นว่า ความท้าทายด้านความมั่นคงปลอดภัยไซเบอร์มิได้เป็นเพียงประเด็นเชิงเทคนิค แต่เป็นประเด็นเชิงโครงสร้างที่เกี่ยวข้องกับคน ระบบ กระบวนการ และความร่วมมือในทุกระดับ การรับมือกับความท้าทายดังกล่าวจึงจำเป็นต้องอาศัยการพัฒนาองค์กรอย่างต่อเนื่องควบคู่ไปกับการยกระดับความพร้อมของประเทศ เพื่อมุ่งสู่การสร้าง **“พื้นที่ไซเบอร์ที่ปลอดภัย มั่นคง และน่าเชื่อถือ”** อย่างยั่งยืน

The results of operations in Fiscal Year 2025 demonstrate that cybersecurity challenges are not merely technical issues, but structural challenges involving people, systems, processes, and multi-level collaboration. Addressing these challenges requires continuous organizational development alongside national readiness enhancement, with the goal of building a **cyberspace that is safe, secure, and trustworthy in a sustainable manner.**

ความท้าทายเชิงโครงสร้าง
Structural Challenges

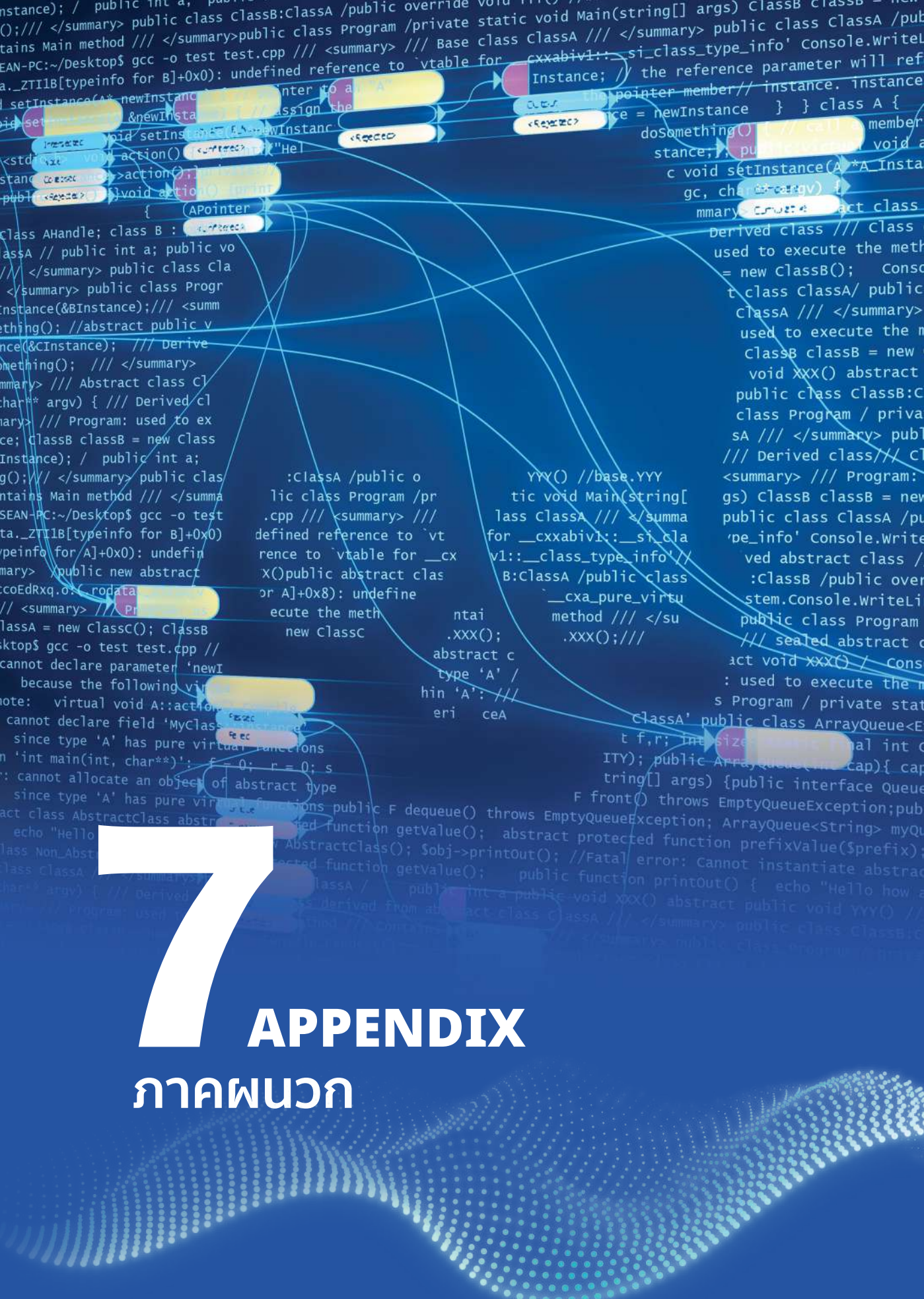
- ครอบคลุมคน ระบบ กระบวนการ และความร่วมมือทุกระดับ
  Covering people, systems, processes, and collaboration at all levels

ความจำเป็นในการพัฒนาอย่างต่อเนื่อง
Need for Continuous Development

- ยกระดับองค์กร หน่วยงาน และประเทศไปพร้อมกัน
  Strengthening organizations, agencies, and national readiness in parallel
- เตรียมความพร้อมรับมือภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็ว
  Enhancing preparedness to address rapidly evolving threats

เป้าหมายเชิงยุทธศาสตร์
Strategic Goal

- สร้างพื้นที่ไซเบอร์ที่ปลอดภัย มั่นคง และเชื่อถือได้
  Building a cyberspace that is safe, secure, and trustworthy
- มุ่งความยั่งยืนและความเชื่อมั่นร่วมกันของทุกภาคส่วน
  Promoting sustainability and shared trust across all sectors



7 APPENDIX
ภาคผนวก

คำศัพท์ทางไซเบอร์
GLOSSARY OF CYBERSECURITY TERMS

คำศัพท์	ความหมาย
Agentic AI	ปัญญาประดิษฐ์ที่สามารถตัดสินใจและดำเนินการได้เองโดยอัตโนมัติ แตกต่างจาก AI ทั่วไป ที่ต้องรอคำสั่งก่อนถึงจะทำงาน Agentic AI สามารถวิเคราะห์ข้อมูล ตั้งเป้าหมาย วางแผน และปรับกลยุทธ์ให้เหมาะสมกับสถานการณ์โดยไม่ต้องพึ่งพามนุษย์ทุกขั้นตอน
AI - Driven Social Engineering Attacks	การโจมตีเชิงจิตวิทยาที่ใช้ปัญญาประดิษฐ์ช่วยวิเคราะห์พฤติกรรมและสร้างเนื้อหาที่สมจริง เช่น ข้อความ เสียง หรือวิดีโอ เพื่อหลอกลวงให้เหยื่อหลงเชื่อและดำเนินการตามที่ผู้โจมตีต้องการ เช่น เปิดเผยข้อมูลหรือโอนเงิน
Attack Surface Management (ASM)	กระบวนการบริหารจัดการและลดจุดที่อาจถูกโจมตีในระบบสารสนเทศขององค์กร โดยมุ่งเน้นการระบุ วิเคราะห์ และติดตามสินทรัพย์ดิจิทัลที่เปิดเผยต่อภายนอก เช่น เว็บไซต์ โดเมน ซับโดเมน แอปพลิเคชัน API ระบบคลาวด์ รวมถึงระบบภายในที่เชื่อมต่อเครือข่าย เพื่อป้องกันไม่ให้ถูกใช้เป็นช่องทางในการโจมตีจากผู้ไม่หวังดี
Cloud & SaaS Hardening	กระบวนการปรับตั้งค่าและเสริมความปลอดภัยของระบบคลาวด์ และ SaaS หรือ Software as a Service การให้บริการระบบซอฟต์แวร์ผ่านอินเทอร์เน็ต เช่น การกำหนดสิทธิ์การเข้าถึง การปิดการตั้งค่าที่ไม่จำเป็น และการเฝ้าระวังการใช้งาน เพื่อลดความเสี่ยงจากการโจมตีและการรั่วไหลของข้อมูล
Cyber Threat Intelligence (CTI)	ระบบข่าวกรองภัยคุกคามไซเบอร์ ที่จัดการรวบรวมข้อมูลจากแหล่งข่าว โดยตรวจสอบภัยคุกคาม มุ่งเน้นการตรวจสอบจากแหล่งข้อมูลภายนอก เช่น เครือข่ายสังคมออนไลน์, Surface web, Deepweb, หรือดาร์กเว็บ (Darkweb) เพื่อค้นหาข้อมูลที่เกี่ยวข้องกับองค์กรเพื่อเพิ่มประสิทธิภาพของข่าวกรองในการรับรู้ถึงภัยคุกคาม และวิเคราะห์ข้อมูลภัยคุกคามในเชิงลึก และลดความเสียหายที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์
Data Poisoning	การโจมตีที่จงใจป้อนข้อมูลที่ผิดพลาด บิดเบือน หรือเป็นอันตรายเข้าสู่ระบบหรือโมเดลปัญญาประดิษฐ์ โดยมีเป้าหมายเพื่อทำให้ผลการวิเคราะห์ การเรียนรู้ หรือการตัดสินใจของระบบคลาดเคลื่อน ส่งผลให้ระบบทำงานผิดพลาดหรือให้ผลลัพธ์ที่ไม่ถูกต้อง

คำศัพท์	ความหมาย
Deception Technologies	เทคโนโลยีที่ช่วยป้องกันภัยคุกคามทางไซเบอร์ ด้วยการใช้ “เหยื่อล่อ” (Decoy) กระจายไว้ภายในเครือข่ายขององค์กร เพื่อหลอกล่อให้ผู้ไม่หวังดี (Hacker) หลงเข้าไปในเส้นทางหรือระบบปลอม แทนที่จะเข้าถึงข้อมูลสำคัญจริงขององค์กร
Generative AI	เทคโนโลยีปัญญาประดิษฐ์ที่สามารถสร้างเนื้อหาใหม่ขึ้นมาได้เองจากข้อมูลที่เรียนรู้ เช่น ข้อความ ภาพ เสียง วิดีโอ หรือเขียนโค้ด โดยอาศัยรูปแบบและความสัมพันธ์ของข้อมูลเดิมที่ถูกนำมาฝึกฝน และสามารถนำไปใช้ได้ทั้งในเชิงสร้างสรรค์และการประยุกต์ใช้งานในภาคธุรกิจ รวมถึงอาจถูกนำไปใช้ในทางที่ก่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ได้หากไม่มีการกำกับดูแลที่เหมาะสม
Harvest - now, Decrypt - later	ภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ที่ผู้โจมตีทำการรวบรวมและจัดเก็บข้อมูลที่ถูกเข้ารหัสไว้ตั้งแต่วันนี้ เพื่อรอถอดรหัสในอนาคต เมื่อคอมพิวเตอร์ควอนตัมมีความสามารถเพียงพอที่จะทำลายการเข้ารหัสที่ใช้อยู่ในปัจจุบัน
Indicators of Compromise (IoCs)	ตัวบ่งชี้การบุกรุกที่ใช้แสดงให้เห็นว่าระบบ เครือข่าย หรืออุปกรณ์อาจถูกโจมตีหรือถูกบุกรุกแล้ว โดยมักเป็นข้อมูลหรือร่องรอยผิดปกติที่เกิดจากกิจกรรมของผู้ไม่หวังดี เช่น IP Address หรือโดเมนที่เป็นอันตราย แฮชของไฟล์มัลแวร์ พฤติกรรมการใช้งานที่ผิดปกติ หรือบันทึกเหตุการณ์ที่ผิดจากปกติ
Info stealer	มัลแวร์ประเภทหนึ่งที่ออกแบบมาเพื่อแอบขโมยข้อมูลสำคัญจากอุปกรณ์ของผู้ใช้งานหรือองค์กร โดยมักปลอมตัวเป็นซอฟต์แวร์หรือไฟล์ที่ดูน่าเชื่อถือ โดยข้อมูลที่ถูกขโมยอาจรวมถึงชื่อผู้ใช้ รหัสผ่าน คุกกี้ ข้อมูลบัตรเครดิต กระเป๋าเงินคริปโต และข้อมูลการเข้าสู่ระบบต่าง ๆ จากนั้นข้อมูลเหล่านี้จะถูกส่งต่อหรือจำหน่ายในตลาดมืด เพื่อนำไปใช้ในการเข้ายึดบัญชี การโจมตีทางไซเบอร์ในขั้นต่อไป
OT / IoT & Machine Identity	การกำหนดและบริหารจัดการตัวตนดิจิทัลของอุปกรณ์ OT และ IoT เพื่อให้สามารถยืนยันตัวตนของเครื่องจักรหรืออุปกรณ์ที่เชื่อมต่อเครือข่ายได้อย่างถูกต้อง และป้องกันการเข้าถึงหรือควบคุมโดยไม่ได้รับอนุญาต
Prompt Injection	เทคนิคการโจมตีระบบ AI โดยการแทรกคำสั่งหรือข้อมูลแฝง เพื่อบิดเบือนการทำงานของโมเดล หรือทำให้สร้างผลลัพธ์ที่ไม่ถูกต้องหรือไม่เหมาะสม

คำศัพท์	ความหมาย
Post - Quantum Cryptography (PQC)	การพัฒนาอัลกอริธึมการเข้ารหัสรูปแบบใหม่ที่ออกแบบมาให้สามารถทนทานต่อการโจมตีจากทั้งคอมพิวเตอร์แบบเดิมและคอมพิวเตอร์ควอนตัมได้ โดยใช้หลักการการสร้างปัญหาทางคณิตศาสตร์ที่แม้แต่คอมพิวเตอร์ควอนตัมก็ยังต้องใช้เวลาคำนวณนานจนแทบเป็นไปไม่ได้ที่จะถอดรหัสได้สำเร็จ
Quantum - Risk Readiness	การเตรียมความพร้อมด้านนโยบาย เทคโนโลยี และกระบวนการ เพื่อรับมือความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดจากการพัฒนาของเทคโนโลยีคอมพิวเตอร์ควอนตัม
Ransomware	มัลแวร์เรียกค่าไถ่ประเภทหนึ่งที่อาชญากรไซเบอร์ใช้เพื่อเข้ารหัสหรือล็อกข้อมูลสำคัญ (ไฟล์, ระบบ) ทำให้ผู้ใช้ไม่สามารถเข้าถึงได้ และทำการเรียกเงินค่าไถ่เพื่อแลกกับการปลดล็อกหรือคืนข้อมูล
Shadow AI	การใช้งานเครื่องมือหรือบริการ AI ภายนอกองค์กรโดยบุคลากรที่ไม่ได้รับการอนุญาตหรือการกำกับดูแล ซึ่งอาจทำให้ข้อมูลภายในถูกส่งออกไปโดยไม่ตั้งใจ และก่อให้เกิดความเสี่ยงด้านความมั่นคงและกฎหมาย
Supply Chain Cyber Risk	ความเสี่ยงด้านไซเบอร์ที่เกิดจากระบบหรือหน่วยงานในห่วงโซ่อุปทาน เช่น ผู้ให้บริการซอฟต์แวร์ ฮาร์ดแวร์ หรือบริการภายนอก ซึ่งอาจถูกใช้เป็นช่องทางในการโจมตีองค์กรหลัก
Third - Party Risk	ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เกิดจากบุคคลหรือหน่วยงานภายนอกที่มีสิทธิ์เข้าถึงระบบหรือข้อมูลขององค์กร และอาจมีมาตรการป้องกันที่ไม่เพียงพอ
Zero Trust	รูปแบบการรักษาความปลอดภัยทางไซเบอร์บนหลักการ อุปกรณ์หรือผู้ใช้งานใด ๆ ที่พยายามเข้าถึงเครือข่ายหรือระบบ ล้วนมีความเสี่ยงที่จะเป็นภัยคุกคามได้ ผู้ใช้ทุกคนต้องได้รับการรับรอง อนุญาต และตรวจสอบอย่างต่อเนื่องก่อนที่จะได้รับสิทธิ์เข้าถึงการเข้าถึงทุกครั้งและยืนยันความปลอดภัยก่อนอนุญาตให้ใช้งาน


TEAM THAILAND FOR
CYBERSECURITY

รายชื่อคณะทำงาน

คณะกรรมการกำกับติดตามการดำเนินงานการจัดทำรายงานประจำปี (Annual Report) ปีงบประมาณ พ.ศ. 2568 (Steering Group)

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

คณะทำงานจัดทำรายงานประจำปี (Annual report) ปีงบประมาณ พ.ศ. 2568 (Working group)

1.	นางชไมพร พงศ์พยุหะ	ประธานคณะทำงาน
2.	นายทศพร โขมพัตร	รองประธานคณะทำงาน
3.	นาวาอากาศเอก เนติภัทร ภัทร์กุลชัย	คณะทำงาน
4.	นางสาวบัณฑารีย์ พุ่มกุมาร	คณะทำงาน
5.	นางสาวกมลพรรณ คงไข่	คณะทำงาน
6.	นางสาวยุภาภรณ์ ทุ่มโมง	คณะทำงาน
7.	นายนันทวัฒน์ จตุเกียรติประยูร	คณะทำงาน
8.	นายทักษิณ บุญรอด	คณะทำงาน
9.	นายปรัชญา ผาสุข	คณะทำงาน
10.	นางสาวภลดา น้อมภักดี	คณะทำงาน
11.	นางสาวพวงพลอย สุขสมปอง	คณะทำงาน
12.	นางสาวอัญชลี ร่วมชาติ	คณะทำงาน
13.	นางสาวปัฐมาภรณ์ เข็มมา	คณะทำงาน
14.	นางสาวกนกวรรณ พรศุภปัทมา	คณะทำงาน
15.	นางสาวพรวิภา สระทองขำ	คณะทำงาน
16.	นางสาวธนาวรรณ กลิ่นแพทย์กิจ	คณะทำงาน
17.	ว่าที่ร้อยตรีหญิง กัญจนาภรณ์ ประไพ	คณะทำงาน
18.	นายทรงวุฒิ ทวีแสง	คณะทำงาน
19.	พันตรี ภาณุพงศ์ ม้วนทอง	คณะทำงาน
20.	นางอสิดา สุขสว่าง	คณะทำงาน
21.	นางสาวพลอยมณีภัคช์ รวมภักดี	คณะทำงาน
22.	นางสาวเพชรไพรินทร์ ต้นแก้ว	คณะทำงาน
23.	นางสาววีนัสรา เกตุพ่อค้า	คณะทำงาน

NCSA 2030: The Architects of a Smart Nation

DNA NCSA

N — **Nation-Centric**
ขับเคลื่อนด้วยความมุ่งมั่นเพื่อแผ่นดิน

C — **Customer-Centric | Competent | Collaborative**
เข้าใจผู้รับบริการอย่างลึกซึ้ง เชี่ยวชาญในระดับสากล
และเชื่อมั่นในพลังของทีม

S — **Strong | Synergistic**
พลังแกร่งที่ผสานกันอย่างลงตัว

A — **AI-Augmented | Accountable | Agile**
ทำงานเคียงข้างเทคโนโลยีอัจฉริยะ
ด้วยความรับผิดชอบ โปร่งใส และพร้อมปรับตัวเสมอ

รายงานประจำปี 2568
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

จัดทำและเผยแพร่โดย

สำนักงานคณะกรรมการการรักษา
ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)
The National Cyber Security Agency (NCSA)

เลขที่ 120 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550
(อาคาร C) ชั้น 7 ซอยแจ้งวัฒนะ 7 ถนนแจ้งวัฒนะ เขตหลักสี่ กรุงเทพฯ
120, Building C, 7th Floor, Government Complex Commemorating
His Majesty the King's 80th Birthday Anniversary,
Chaeng Watthana Road, Laksi, Bangkok 10210, Thailand

โทรศัพท์: 02 142 6888
Phone: +66 2 142 6888

Email: saraban@ncsa.or.th

DOWNLOAD

พิมพ์ครั้งที่ 1 จำนวน 1,000 เล่ม
กุมภาพันธ์ 2569
พิมพ์ที่ บริษัท พี ดับบลิว พริ้นติ้ง จำกัด
ISBN 978-616-94218-3-2