



The National Cyber Security Agency



Annual Report



2023



รายงานประจำปี 2566

สำนักงานคณะกรรมการการรักษา
ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ



NCSA
สกมช
สำนักงานคณะกรรมการการรักษา
ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ผลงานเด่น ประจำปีงบประมาณ พ.ศ. 2566

Highlights of 2023



Prime Minister
Awards 2023



THAILAND
CYBER TOP TALENT

Thailand Cyber
Top Talent 2023



Thailand's National
Cyber Exercise 2023
(NCX)



ศูนย์ปฏิบัติการเฝ้าระวัง
ภัยคุกคามทางไซเบอร์
สำหรับการประชุม APEC 2022
และการเลือกตั้ง



นโยบายและแผนปฏิบัติการว่าด้วย
การรักษาความมั่นคงปลอดภัยไซเบอร์
(พ.ศ. 2565 – 2570)
“บริการที่สำคัญของประเทศไทย
ที่มีความมั่นคงปลอดภัยไซเบอร์
เพื่อความยั่งยืนทางเศรษฐกิจและสังคม”



Women Thailand Cyber
Top Talent 2022



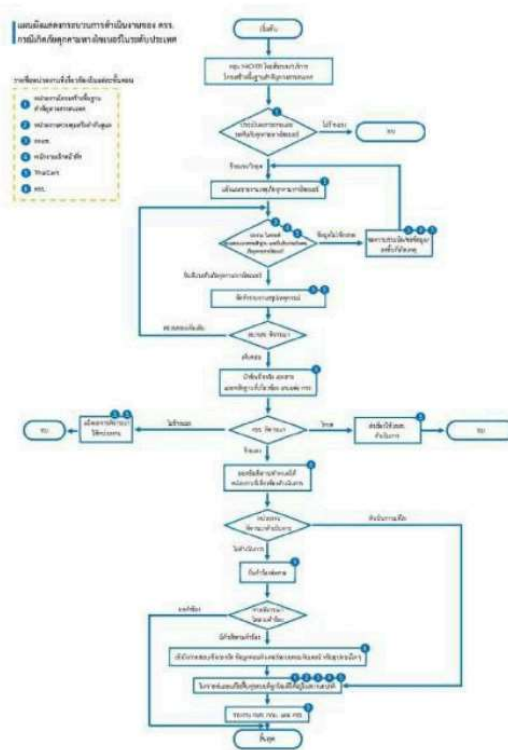
Cyber SEA Game 2023



ASEAN-Japan Capacity Cybersecurity Capacity Building Centre (AJCCBC)



กิจกรรมประชาสัมพันธ์
สร้างความตระหนักรู้ การรักษา
ความมั่นคงปลอดภัยไซเบอร์
สู่ภาคประชาชน



คณะกรรมการรับมือกับภัยคุกคาม
ทางไซเบอร์ในระดับร้ายแรง (คสร.)



ส่งเสริมกลุ่มเปราะบาง
(มูลนิธิพระมหาไถ่เพื่อการพัฒนา
คนพิการ)



สมาคมเวชสารสนเทศไทย
(Thai Medical Information
Association – TMI)



สัปดาห์วิชาการด้านความมั่นคง
ปลอดภัยไซเบอร์
Thailand National Cyber Week 2023



สารถายกรัฐมนตรี

เทคโนโลยีมีบทบาทสำคัญต่อการบริหารและการดำเนินงานของหน่วยงานทุกภาคส่วน ทั้งภาครัฐและภาคเอกชน ตลอดจนเกี่ยวข้องกับการดำเนินชีวิตของพี่น้องประชาชนในหลากหลายมิติ รัฐบาลจึงมีนโยบายพัฒนาเศรษฐกิจและสังคมด้วยการนำเทคโนโลยีและระบบดิจิทัลมาใช้ส่งเสริมให้หน่วยงานและองค์กรต่าง ๆ ใช้ประโยชน์จากเทคโนโลยี เพื่อพัฒนาประสิทธิภาพ การดำเนินงาน การอำนวยความสะดวกและการให้บริการประชาชน ขณะเดียวกันก็ให้ความสำคัญในการขับเคลื่อนเศรษฐกิจดิจิทัล เพื่อให้เป็นเครื่องยนต์สำคัญในการยกระดับขีดความสามารถในการแข่งขันของประเทศ

ควบคู่ไปกับการเปลี่ยนผ่านสู่การเป็นรัฐบาลดิจิทัลและสังคมเศรษฐกิจยุคดิจิทัล รัฐบาลได้ให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งถือเป็นภัยคุกคามด้านความมั่นคงรูปแบบใหม่ในศตวรรษที่ 21 โดยมีแนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ (Cyber Security) เพื่อให้หน่วยงานในทุกภาคส่วนสามารถนำไปใช้ในการบริหารจัดการในการป้องกันและแก้ไขได้อย่างมีมาตรฐาน

นอกจากนี้ รัฐบาลได้สนับสนุนให้มีการเสริมสร้างองค์ความรู้ในเรื่องการใช้เทคโนโลยีในโลกยุคใหม่ได้อย่างปลอดภัย

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นหน่วยงานที่มีบทบาทสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์มิให้เกิดผลกระทบต่อความมั่นคงของรัฐ ซึ่งในการดำเนินงานต้องอาศัยความร่วมมือจากทุกภาคส่วนเพื่อให้การดำเนินงานบรรลุเป้าหมาย ผมหวังว่ารายงานผลการดำเนินงานประจำปีงบประมาณ พ.ศ. 2566 ฉบับนี้ จะช่วยให้หน่วยงานในภาคส่วนต่าง ๆ และประชาชนทั่วไปได้รับรู้และเข้าใจในบทบาทและภารกิจ รวมถึงการดำเนินการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รวมทั้งตระหนักถึงการมีส่วนร่วมในการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

(เศรษฐา ทวีสิน)

นายกรัฐมนตรี

Message from the Prime Minister

Technology plays a vital role in the administration and functioning of both governmental and private entities including, extending its influence into various facets of people's lives. Consequently, the government has formulated policies aimed at fostering economic and social development through the utilization of technology and digital systems. This is intended to motivate diverse agencies and organizations to utilize technology for enhanced efficiency, streamlined operations, and improved delivery of public services. Simultaneously, there is an emphasis on advancing the digital economy to serve as a pivotal driver in elevating the nation's competitiveness.

In the context of transitioning towards a digital government and a digitalized economic society, cybersecurity has emerged as a critical national priority. Recognized as a novel security challenge of the 21st century, the government has undertaken the development of a standardized cybersecurity plan. This plan will equip agencies across all sectors with the necessary tools and protocols for managing cyber threats,

implementing preventative measures, and tackling problems using standardized approaches. Furthermore, the government actively promotes the enhancement of knowledge and skills related to the safe and responsible use of technology in the contemporary world.

The National Cyber Security Agency serves as a crucial agency in safeguarding national security from cyber threats. Its operations necessitate collaborative efforts across all sectors to ensure successful outcomes. This report, encompassing the fiscal year 2023, aims to raise awareness and understanding among various government agencies and the public regarding their roles and responsibilities in cybersecurity. It also details the NCSA's operations in maintaining national cyber resilience and highlights its contributions to effective prevention and mitigation of cyberattacks.



Mr. Srettha Thavisin

Prime Minister



สารรองนายกรัฐมนตรี

ปฏิบัติหน้าที่ประธานกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

ปัจจุบันภัยคุกคามทางไซเบอร์มีรูปแบบที่หลากหลายและมีแนวโน้มที่ทวีความรุนแรงเพิ่มมากขึ้น ส่งผลกระทบต่อประเทศและประชาชนเป็นวงกว้าง โดยเฉพาะอย่างยิ่งการที่รัฐบาลให้ความสำคัญในเรื่องการขับเคลื่อนเศรษฐกิจดิจิทัล ยังเป็นสิ่งกระตุ้นให้เกิดความจำเป็นที่ต้องเร่งเสริมสร้างความมั่นคงปลอดภัยไซเบอร์อย่างมีระบบและเป็นรูปธรรม ทั้งนี้การแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ไม่สามารถดำเนินการได้โดยหน่วยงานใดหน่วยงานหนึ่ง หากแต่รูปแบบที่ดีที่สุดคือการดำเนินการแบบบูรณาการซึ่งมีความสำคัญอย่างยิ่งที่ต้องใช้ความร่วมมือจากหน่วยงานภาครัฐ เอกชน องค์กรอิสระ และประชาชนในทุกภาคส่วน

บทบาทที่สำคัญของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้แก่ การขับเคลื่อน ผลักดัน ติดตามและประเมินผลการปฏิบัติตามนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) เพื่อก่อให้เกิดการดำเนินงานแบบบูรณาการ ส่งเสริมให้หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญ

ทางสารสนเทศ และหน่วยงานของรัฐ ยกระดับและพัฒนารักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยในภาพรวมที่ครอบคลุมทุกมิติ ประสานสอดคล้อง เป็นไปตามแนวทางอันจะก่อให้เกิดการยกระดับในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร สังคม และของประเทศอย่างเป็นรูปธรรม

ในนามของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ผมจึงหวังเป็นอย่างยิ่งว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จะสามารถเร่งรัดการดำเนินการขับเคลื่อนและบูรณาการความร่วมมือทุกภาคส่วนในการเสริมสร้างความมั่นคงปลอดภัยไซเบอร์อย่างมีระบบ นำไปสู่การป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพและยั่งยืนต่อไป

(ภูมิธรรม เวชยชัย)

รองนายกรัฐมนตรี

Message from the Deputy Prime Minister

Acting Chairman of the National Cyber Security Committee (NCSC)

The frequency and severity of cyber threats are on the rise across different fronts, impacting individuals and the nation at large. With the government prioritizing the advancement of the digital economy, it's essential to enhance cybersecurity in a coordinated and inclusive manner. Strengthening cyber security requires cooperation among government agencies, private enterprises, independent organizations, and every member of the society.

The National Cyber Security Agency holds a crucial responsibility in overseeing and assessing the execution of the Cyber Security Policy and Action Plan B.E. 2565-2570 (2022-2027), aimed at upholding cyber security, and promoting comprehensive solutions to cyber threats. Additionally, it fosters collaboration among Regulators,

organizations of Critical Information Infrastructure (CII), and government agencies to oversee and bolster Thailand's cyber security landscape.

On behalf of the National Cyber Security Committee, I earnestly urge the National Cyber Security Agency to accelerate its efforts and foster collaboration across all sectors to systematically enhance cyber security. By doing so, we aim to implement effective prevention and response measures, thereby mitigating the risks posed by cyber threats.



Mr. Phumtham Wechayachai

Deputy Prime Minister,
Acting Chairman of NCSC



สารรัฐมนตรีว่าการกระทรวง ดิจิทัลเพื่อเศรษฐกิจและสังคม

ประธานกรรมการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ (กทม.)
และประธานกรรมการบริหารสำนักงาน
คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)

การรักษาความมั่นคงปลอดภัยไซเบอร์ในแต่ละปีมีความท้าทายแตกต่างกันไป ปี 2566 เป็นอีกปีที่มีความเปลี่ยนแปลงทั้งการจัดตั้งรัฐบาลและผู้บริหารภายในสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่ได้ผู้นำท่านใหม่สามารถบริหารองค์กรได้อย่างมีประสิทธิภาพ ประกอบกับผู้บริหาร พนักงาน ลูกจ้างทุกคน มีส่วนร่วมผลักดันให้หน่วยงานมีพัฒนาการอย่างก้าวกระโดดในการดำเนินงาน ส่งผลให้การประเมินองค์กรจากบุคคลภายนอก ตามมาตรา 39 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีผลการประเมินอยู่ที่ 97.50 จัดอยู่ในระดับดีมาก ซึ่งเมื่อเปรียบเทียบกับปีงบประมาณ 2565 ได้คะแนน 91.75 เพิ่มขึ้นคิดเป็นร้อยละ 5.75 ซึ่งเป็นจุดเปลี่ยนสำคัญที่จะสามารถเป็นองค์กรนำในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศได้ และเป็นหน่วยงานสำคัญที่จะเป็นส่วนช่วยให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานควบคุมหรือกำกับดูแลของประเทศสามารถป้องกัน รับมือ

ลดความเสี่ยงภัยคุกคามทางไซเบอร์ รวมถึงการสร้างการรับรู้และความตระหนักรู้ให้กับประชาชนได้ ตามกรอบแนวทางนโยบายและแผนปฏิบัติการการรักษาความมั่นคงปลอดภัยไซเบอร์ จึงขอให้รักษามาตรฐานการทำงานไว้

ในฐานะที่กระผมกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์และการกำกับการบริหารงาน สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาตินั้น กระผมมีความเชื่อมั่นว่าการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศจะสามารถป้องกัน รับมือ และลดความเสี่ยงตามเจตนารมณ์ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้อย่างมีประสิทธิภาพและเกิดประสิทธิผลสูงสุดกับประเทศชาติต่อไป

(ประเสริฐ จันทรรวงทอง)

รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

Message from the Minister of Digital Economy and Society

Chairman of the Cybersecurity Regulating Committee (CRC)
and Chairman of the Committee Managing the Office
of the National Cybersecurity Committee (CMO)

Every year, the task of maintaining cyber security presents unique challenges. In 2023, significant changes took place, including the formation of a new government and leadership within the National Cyber Security Agency. The new leadership has been effectively managing the organization, leading to substantial progress. Through the dedication and efforts of its executives and employees, the agency has achieved significant progress, attaining an impressive assessment score of 97.50 from external assessors, as stipulated in Section 39 of the Cybersecurity Act B.E. 2562 (2019). This places NCSA in the ‘excellent’ category, marking a notable improvement from the previous year’s score of 91.75, representing a 5.75 percent increase. This milestone solidifies NCSA position as a leader in the nation’s cyber security efforts and a crucial supporter

of organizations of Critical Information Infrastructure and Regulators to effectively prevent, manage, and mitigate cyber threats, while also enhancing public awareness and understanding. The agency’s endeavors are fully aligned with the policy framework and operational plans for cyber security, ensuring the maintenance of high operational standards.

In my role overseeing cyber security and directing the management of NCSA, I am confident that the nation’s cyber security efforts, guided by the provisions of the Cybersecurity Act B.E. 2562 (2019), will effectively prevent, address, and mitigate risks with utmost efficiency and effectiveness for the nation.



Mr. Prasert Jantararuangtong
Minister of Digital Economy and Society



สารเลขาธิการ คณะกรรมการการรักษาความมั่นคง ปลอดภัยไซเบอร์แห่งชาติ

ในโอกาสที่กระผมได้ดำรงตำแหน่งเลขาธิการ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นปีแรกและได้ขับเคลื่อนสำนักงาน คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งเป็นองค์กรที่มีความสำคัญต่อการพัฒนาประเทศด้านความมั่นคงปลอดภัยไซเบอร์ และเป็นองค์กรที่มีบทบาทนำในการขับเคลื่อนแบบบูรณาการทั้งหน่วยงานภาครัฐ ภาคเอกชน และหน่วยงานต่าง ๆ ที่เกี่ยวข้องทั้งภายในประเทศและต่างประเทศ กระผมรู้สึกเป็นเกียรติอย่างยิ่งที่ได้รับมอบหมายให้หลักภารกิจสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์ประจำปีงบประมาณ พ.ศ. 2566 มีคำสำคัญ (Key Words) ที่ผมได้วางแนวทางไว้ คือ Proactive Protection (การป้องกันเชิงรุก) ซึ่งหมายถึง การป้องกันก่อนเกิดเหตุเปรียบได้กับการล้อมคอกก่อนวัวหาย ซึ่งเป็นหน้าที่และภารกิจหลักของการดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และ Total Defense (การผนึกกำลังในการป้องกัน) ซึ่งหมายถึงการเสริมความแข็งแกร่งให้ทุกหน่วยงานมีความพร้อมป้องกัน รับมือ และลดความเสี่ยงอย่างมีประสิทธิภาพ

การดำเนินการที่สำคัญที่สามารถทำให้หลักภารกิจที่กล่าวไว้ มีประสิทธิภาพสูงสุดนั้น ทุกคนและทุกหน่วยงานต้องร่วมมือกันเป็นกลไกในการขับเคลื่อน

แบบบูรณาการให้ภาพรวมของประเทศมีความพร้อมในการรับมือต่อภัยคุกคามไซเบอร์ที่กระทบระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศเกิดความเสียหายหรือใช้งานได้ไม่เต็มที่ รวมถึงประชาชนจำนวนมากที่ได้รับความเดือดร้อนจากการต้องพึ่งพาระบบโครงสร้างพื้นฐานสำคัญที่มีความเชื่อมโยงต่อการพึ่งพาระบบสำคัญต่าง ๆ

กระผมขอขอบคุณอย่างยิ่งสำหรับการบูรณาการความร่วมมือของบุคลากรจากหน่วยงานควบคุมหรือกำกับดูแล (Regulator) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (หน่วยงาน CII) และหน่วยงานของรัฐ ตลอดจนบุคลากรจากสถานศึกษาต่าง ๆ ทั่วประเทศ และหน่วยงานที่เกี่ยวข้อง และกระผมหวังเป็นอย่างยิ่งว่า บุคลากรของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจะสามารถปฏิบัติหน้าที่ของตนเองอย่างเต็มที่และร่วมกันพัฒนา ผลักดัน และส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์ให้เข้มแข็งและยั่งยืนตอบสนองนโยบายรัฐบาลที่มุ่งผลประโยชน์ต่อประชาชนและประเทศชาติอย่างแท้จริง

พลอากาศตรี 
(อมร ชมเชย)

เลขาธิการคณะกรรมการการรักษาความมั่นคง
ปลอดภัยไซเบอร์แห่งชาติ

Message from the Secretary-General of the National Cyber Security Committee

In my first year as Secretary-General of the National Cyber Security Agency (NCSA), I've had the privilege of leading the agency's executive team. The NCSA plays a crucial role in our country's cyber security landscape, fostering collaboration among government agencies, the private sector, and various related entities on both domestic and international fronts. It's been a profound honor to serve in this capacity, contributing to the agency's mission and vision.

In the fiscal year of 2024, cyber security is centered on two key principles: Proactive Protection and Total Defense. Proactive Protection involves preventing incidents before they occur, like the saying 'securing the barn door before the horse can escape', emphasizing the importance of taking precautionary measures. This approach forms the primary duty and mission of implementing the Cybersecurity Act B.E. 2562 (2019), emphasizing prevention as the first line of defense.

Total Defense, on the other hand, involves joining forces for protection, fostering collaboration among all agencies to enhance readiness in protecting, responding to, and mitigating risks effectively. By implementing these crucial actions, we maintain fundamental principles and maximize efficiency in safeguarding against cyber threats. It is crucial for all individuals and agencies

to collaborate effectively as a united front to tackle cyber threats that could potentially cause harm or disruption to critical information infrastructure systems. This integrated approach ensures that the country is collectively prepared to counter such threats. Many individuals have already experienced the consequences of their reliance on interconnected infrastructure systems, highlighting the urgent need to engage all agencies comprehensively in safeguarding against cyber threats.

I am grateful for the collaborative efforts and integration of personnel from Regulators, organizations of Critical Information Infrastructure (CII), and government agencies, along with personnel from educational institutions across the nation and other associated agencies. Furthermore, I sincerely hope that the staff of the National Cyber Security Agency (NCSA) will be empowered to fulfill their responsibilities, advance cyber security sustainability, and align with government policies that truly benefit the people and the nation.



AVM. Amorn Chomchoey

Secretary-General of the National Cyber
Security Committee

สารบัญ

- 2 ผลงานเด่นประจำปี 2566
- 4 สารนายกรัฐมนตรี
- 6 สารรองนายกรัฐมนตรี
- 8 สารรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
- 10 สารเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

01

13 เกี่ยวกับองค์กร

Organizational Structure Overview

- 14 ประวัติความเป็นมา
- 16 วิสัยทัศน์และการขับเคลื่อนองค์กร
- 18 คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)
- 20 คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กทม.)
- 22 คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)
- 24 การปฏิบัติงานของ กบส. ประจำปีงบประมาณ 2566
- 26 คณะกรรมการและคณะกรรมการที่ กทม. และ กบส. แต่งตั้ง
- 28 คณะผู้บริหาร สกมช.
- 30 ผู้อำนวยการสำนัก
- 32 โครงสร้างองค์กร

02

34 ผลการดำเนินงาน

Operational Performance Highlights

- 35 การวางรากฐานความมั่นคงปลอดภัยไซเบอร์ของประเทศ
- 43 การพัฒนาขีดความสามารถการรักษาความมั่นคงปลอดภัยไซเบอร์ทุกมิติ
- 44 การป้องกันภัยคุกคามทางไซเบอร์
- 63 การรับมือภัยคุกคามทางไซเบอร์
- 70 การลดความเสี่ยงจากภัยคุกคามทางไซเบอร์
- 89 การรักษาความมั่นคงปลอดภัยไซเบอร์อย่างยั่งยืน

03

107 การพัฒนา สกมช.สู่องค์กรสมรรถนะสูง

Developing NCSA into a High-Performance Organization

- 108 รางวัลแห่งความภาคภูมิใจ
- 111 การพัฒนาบุคลากร สกมช.สู่มาตรฐานสากล
- 112 การฝึกอบรมยกระดับศักยภาพและทักษะผู้ปฏิบัติงานของ สกมช.
- 114 กิจกรรมประชาสัมพันธ์สร้างความตระหนักรู้การรักษาความมั่นคงปลอดภัยไซเบอร์สู่ภาคประชาชน ภายในปี 2566
- 115 สร้างเกราะป้องกันภัยไซเบอร์ในกิจกรรมเพื่อสังคม (CSR)
- 116 NCSA Highlighted News
- 117 รายงานผลการดำเนินงานของคณะกรรมการตรวจสอบ

04

119 รายงานทางการเงิน

Financial Report

05

125 การประเมินผลการดำเนินงาน

Performance Evaluation

06

128 ปัญหาอุปสรรคการดำเนินงานที่ผ่านมา

Challenges and Obstacles in Past Operations

- 129 ปัญหา อุปสรรค และข้อเสนอแนะ
- 130 บทสรุปส่งท้าย

07

132 ภาคผนวก

Annex



ประวัติความเป็นมา History

- 01 **28 พฤษภาคม 2562** พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ได้ประกาศในราชกิจจานุเบกษา เล่ม 136 ตอนที่ 69 ก ลงวันที่ 27 พฤษภาคม 2562 และมีผลบังคับใช้ตั้งแต่วันที่ 28 พฤษภาคม 2562 เป็นต้นไป จึงมีการจัดตั้งคณะกรรมการและหน่วยงาน ดังนี้
- 01 **May 28, 2019** The Cybersecurity Act 2019 was announced in the Royal Gazette, Volume 136, Chapter 69 A, on May 27, 2019 and entered into force on May 28, 2019. Subsequently, committees and agencies were formed as follow:
- “คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” เรียกโดยย่อว่า “กมช.” หรือเรียกเป็นภาษาอังกฤษว่า “National Cyber Security Committee” (NCSC) โดยมีนายกรัฐมนตรีหรือผู้ที่นายกรัฐมนตรีมอบหมาย เป็นประธานกรรมการ
 - The “National Cyber Security Committee” abbreviated as “NCSC,” with the Prime Minister or a person assigned by the Prime Minister being the chairman of the committee
 - “คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์” เรียกโดยย่อว่า “กกม.” โดยมีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ
 - The “Cybersecurity Regulating Committee” abbreviated as the “CRC” with the Minister of Digital Economy and Society being the chairman of the committee
 - “คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์” เรียกโดยย่อว่า “กบส.” โดยมีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ
 - The “Committee Managing the Office of the National Cybersecurity Committee “ abbreviated as the “CMO” with the Minister of Digital Economy and Society being the chairman of the committee
 - “สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” เรียกโดยย่อว่า “สกมช.” หรือเรียกเป็นภาษาอังกฤษว่า “National Cyber Security Agency” (NCSA) ซึ่งเป็นหน่วยงานของรัฐในรูปแบบองค์การมหาชนอยู่ภายใต้การกำกับดูแลของนายกรัฐมนตรี
 - The “National Cyber Security Agency,” abbreviated as “NCSA”, is a government agency in the form of public organizations under the regulation of the Prime Minister.
- 02 **1 มกราคม 2564** กมช. ได้แต่งตั้ง พลโท ดร.ปรัชญา เฉลิมวัฒน์ (ยศในขณะนั้น) เป็นเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติคนแรก
- 02 **January 1, 2021** The NCSC appointed Lieutenant General Dr. Prachaya Chalermwat (at the time) as the first Secretary-General of the NCSA.
- 03 **18 พฤษภาคม 2564** คณะรัฐมนตรีมีมติให้ข้าราชการ พนักงาน เจ้าหน้าที่ หรือผู้ปฏิบัติงานอื่นใด ในหน่วยงานของรัฐ จำนวนทั้งสิ้น 42 ราย มาปฏิบัติงานที่ สกมช. เป็นการชั่วคราวภายในระยะเวลาหนึ่งร้อยแปดสิบวัน ซึ่งถือว่าเป็นพนักงานชุดแรกของ สกมช.
- 03 **May 18, 2021** The cabinet decided to permit a total of forty-two civil servants, officials, or any other government personnel to be temporarily assigned to work at the NCSA for 180 days, forming the initial group of NCSA employees.

- 04 18 สิงหาคม 2564 สกมช. ได้เปิดสำนักงานอย่างเป็นทางการโดยมีที่ตั้งชั่วคราวอยู่ที่ อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น 6 และ 7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ
- 04 August 18, 2021 NCSA is temporarily located at Ratthaprasasanabhakti Building (Building B), on the 6th and 7th floor at the Government Complex Commemorating His Majesty the King's 80th Birthday Anniversary, December 5, 2007, Chaengwattana Road, Thung Song Hong Sub district, Lak Si District, Bangkok.
- 05 1 ตุลาคม 2565 กมช. ได้แต่งตั้ง พลอากาศตรี อมร ชมเชย เป็นเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (คนที่สอง)
- 05 October 1, 2022 NCSC appointed Air Vice Marshal Amorn Chomchoey as the Second Secretary-General of the National Cyber Security Committee.
- 06 9 ธันวาคม 2565 คณะรัฐมนตรีได้มีมติเมื่อวันที่ 20 กันยายน 2565 เห็นชอบนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) ตามที่ กมช. เสนอ ซึ่งนโยบายและแผนปฏิบัติการดังกล่าว ได้ประกาศในราชกิจจานุเบกษา เล่ม 139 ตอนพิเศษ 288 ง ลงวันที่ 9 ธันวาคม 2565 และมีผลบังคับใช้ตั้งแต่วันที่ 10 ธันวาคม 2565 เป็นต้นไป ซึ่งถือว่าเป็นนโยบายและแผนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศฉบับแรก
- 06 December 9, 2022 The Cabinet approved the Cybersecurity Policy and Action Plan B.E. 2565 - 2570 (2022 - 2027) proposed by the NCSC on September 20, 2022. This Policy and Action Plan was published in the Royal Gazette, Volume 139, Special Chapter 288 D, on December 9, 2022, and entered into force on December 10, 2022. So, this is considered to be the first National Cybersecurity Policy and Action Plan of Thailand.
- 07 3 มกราคม 2566 พลอากาศตรี อมร ชมเชย เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้มอบค่านิยมองค์กรและการขับเคลื่อนองค์กรของ สกมช. หรือที่เรียกว่า DNA ของ สกมช. (NCSA's DNA) ซึ่งประกอบด้วย.N – National, C – Competency, S – Strong/Synergy, A – Agility
- 07 January 3, 2023 Air Vice Marshal Amorn Chomchoey, Secretary-General of the National Cyber Security Agency, presented the organizational values and driving force of the NCSA, also known as NCSA's DNA, which consists of N – National, C – Competency, S – Strong/Synergy, A – Agility.
- 08 5 กรกฎาคม 2566 พลอากาศตรี อมร ชมเชย เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้กำหนดวันสถาปนาของ สกมช. เป็นวันที่ 28 พฤษภาคม ของทุกปี
- 08 July 5, 2023 Air Vice Marshal Amorn Chomchoey, Secretary-General of the National Cyber Security Agency, set the founding date of NCSA on May 28 every year.
- 09 25 กันยายน 2566 คำสั่งสำนักนายกรัฐมนตรีที่ 246/2566 มอบหมายและมอบอำนาจให้ นายภูมิธรรม เวชยชัย รองนายกรัฐมนตรี ปฏิบัติหน้าที่เป็นประธาน กมช.
- 09 September 25, 2023 Order of the Office of the Prime Minister No. 246/2023 assigned and granted authority to Mr. Phumtham Wechayachai, Deputy Prime Minister, to perform duties as chairman of NCSC.

วิสัยทัศน์และการขับเคลื่อนองค์กร

VISION

วิสัยทัศน์ Vision

เป็นผู้นำในการขับเคลื่อนในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ ที่มีประสิทธิภาพพร้อมตอบสนองต่อภัยคุกคามไซเบอร์ทุกมิติ

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

DNA ของ สกมช.



National :

เป็นองค์กรระดับชาติมีหน้าที่ขับเคลื่อนและสร้างความมั่นคงปลอดภัยไซเบอร์ของประเทศและเป็นศูนย์กลางความร่วมมือหน่วยงานภาครัฐและเอกชน ทั้งภายในและต่างประเทศ

Acting 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 เกิดความประทับใจเกินความคาดหวัง

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 :

ต้องเข้มแข็งด้วยความสามัคคี ผนึกกำลังในการปฏิบัติหน้าที่ Showing strength and synergy to fulfill responsibilities.

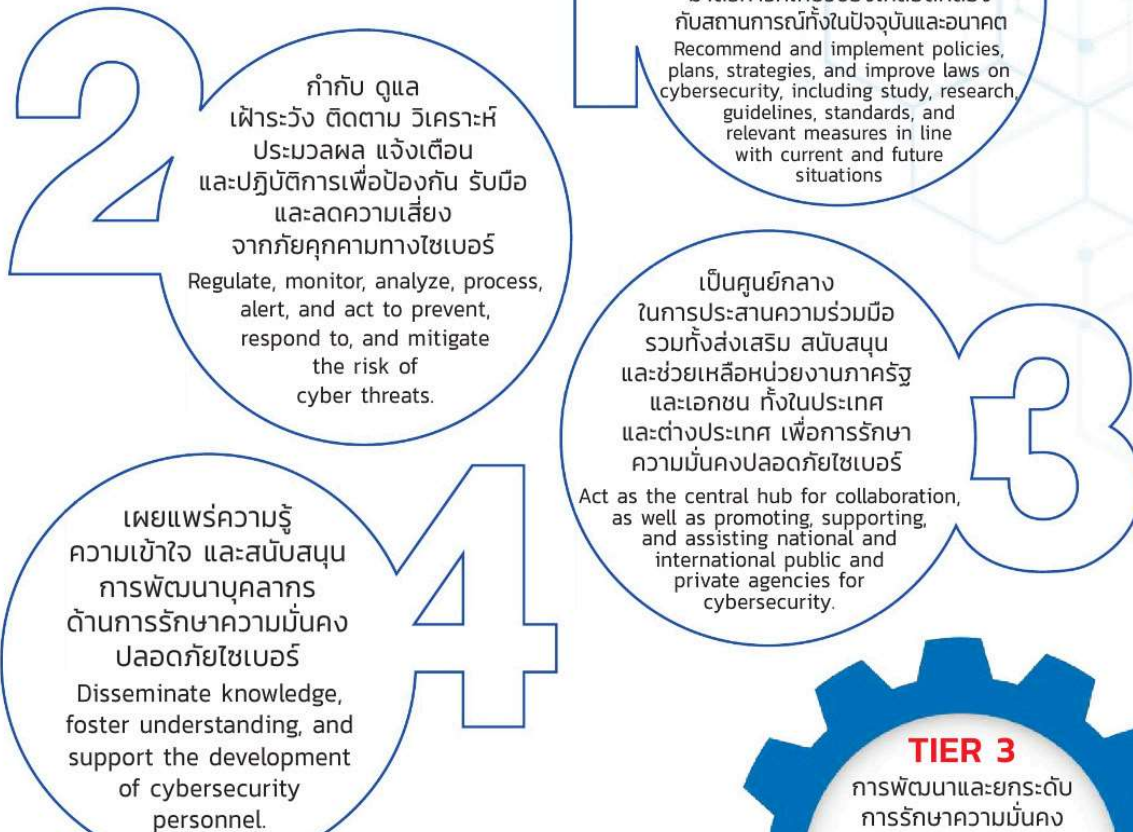


Agility :

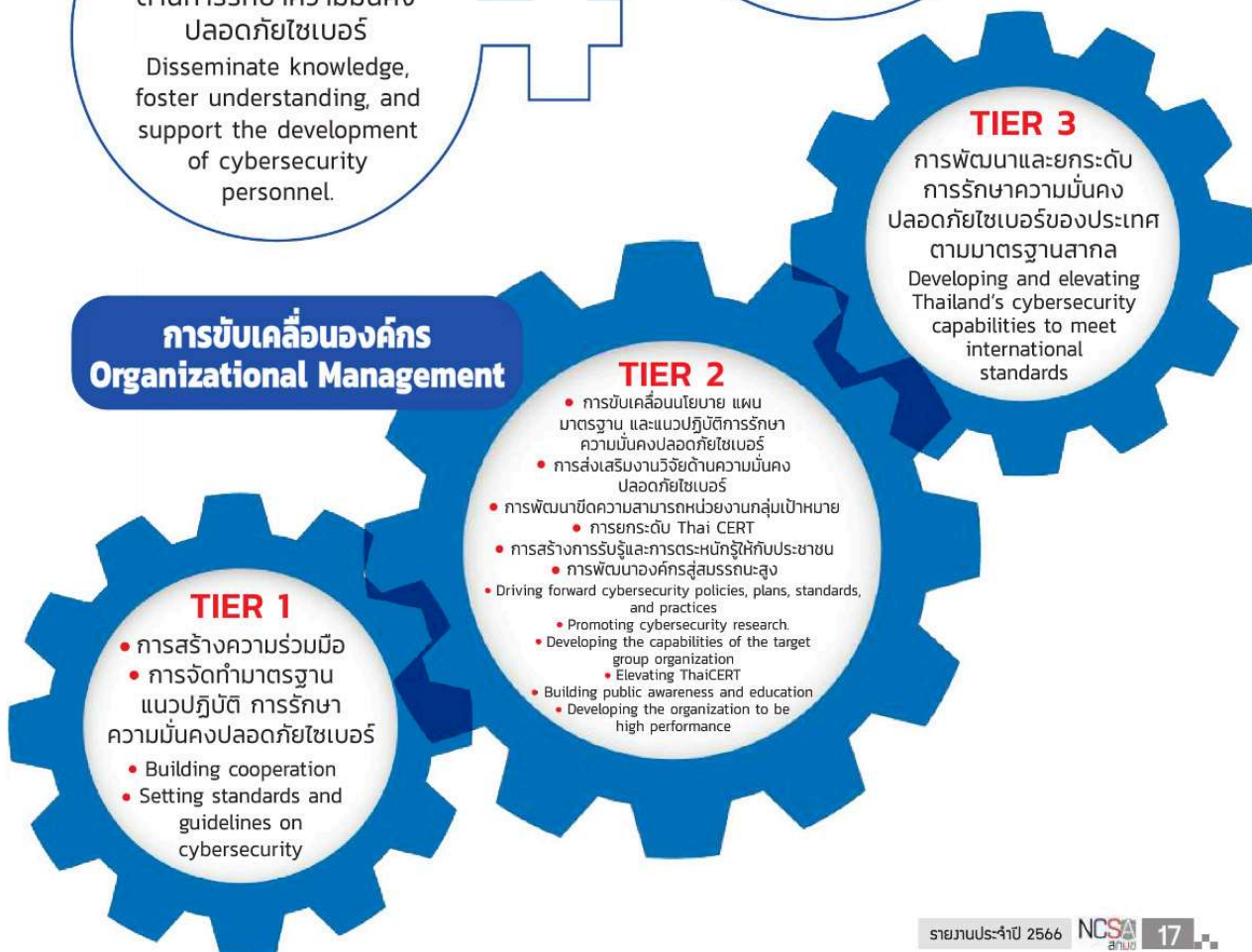
ต้องมีความคล่องตัวพร้อมรับมือทุกความเปลี่ยนแปลงและทุกความท้าทาย

Operating with agility, adapting to changes and challenges for any change and challenge.

พันธกิจ Mission



การขับเคลื่อนองค์กร Organizational Management



ประธานกรรมการ Chairman



นายภูมิธรรม เวชยชัย
รองนายกรัฐมนตรี
ปฏิบัติหน้าที่ประธานกรรมการ
Mr. Phumtham Wechayachai
Deputy Prime Minister
Acting Chairman

กรรมการโดยตำแหน่ง Committees by Position

นายสุทิน คลังแสง
รัฐมนตรีว่าการ
กระทรวงกลาโหม
Mr. Sutin Klungsang
Minister of Defence



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



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



พลตำรวจเอก ดำรงศักดิ์ กิตติประภัสร์
ผู้บัญชาการตำรวจแห่งชาติ
Police General Damrongsak Kittiprapat
Commissioner General,
Royal Thai Police



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



พลเอก สุพจน์ มลานิยม
เลขาธิการสภาความมั่นคงแห่งชาติ
General Supot Malaniyom
Secretary-General,
National Security Council



พลอากาศตรี อมร ชมเชย
เลขาธิการคณะกรรมการการรักษาความมั่นคง
ปลอดภัยไซเบอร์แห่งชาติ
กรรมการและเลขานุการ
AVM Amorn Chomchoey
Secretary-General, National Cyber Security Committee
Acting as Committee member and Secretary

คณะกรรมการการรักษาความมั่นคงปลอดภัย ไซเบอร์แห่งชาติ (กมช.) Nation Cyber Security Committee (NCSC)

กรรมการผู้ทรงคุณวุฒิ Honorary Committees

ดร.ปริญญ์ หอมเอนก
ด้านการรักษาความมั่นคง
ปลอดภัยไซเบอร์
Dr. Prinya Hom-anek
Expert Committee on
Cyber Security



นายไพบูลย์ อมรปัญญาเกียรติ
ด้านกฎหมาย
Mr. Paiboon Aamonpinyokeat
Expert Committee on
Legal Affairs



พลเอก มโน นุชเกษม
ด้านเทคโนโลยีสารสนเทศ
และการสื่อสาร
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
ความสัมพันธ์ระหว่างประเทศ
Associate Professor
Dr. Panitan Wattanayagorn
Expert Committee on
International Relations





คณะกรรมการกำกับดูแล ด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) Cybersecurity Regulating Committee (CRC)

กรรมการผู้ทรงคุณวุฒิ Honorary Committees

พลตรี ปนิวัตร ทรัพย์รุ่งเรือง
ด้านการรักษาความมั่นคง
ปลอดภัยไซเบอร์
Major General Paniwat Subrungruang
Expert Committee on Cyber Security



ดร.พันธ์ศักดิ์ ศิริรัชตพงษ์
ด้านเทคโนโลยีสารสนเทศ
และการสื่อสาร
Dr. Pansak Sirirattaphong
Expert Committee on Information
Technology and Communication



ดร.รอม หิรัญพฤกษ์
ด้านวิทยาศาสตร์
หรือด้านวิศวกรรมศาสตร์
Dr. Rom Hiranpruk
Expert Committee on
Science or Engineering



พลตำรวจตรี พิสิทธิ์ เปาอินทร์
ด้านกฎหมาย
Police Major General Pisit Pao-in
Expert Committee on Legal Affairs



นายเศรษฐพุฒิ สุทธิวาทนฤพุฒิ
ผู้ว่าการธนาคารแห่งประเทศไทย
Mr. Sethaput Suthiwartnarueput
Governor of the Bank of Thailand



พลอากาศตรี อมร ชมเชย
เลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัย
ไซเบอร์แห่งชาติ



กรรมการและเลขานุการ
AVM Amorn Chomchoey
Secretary-General, National
Cyber Security Committee
Acting as Committee member
and Secretary

นางสาวรื่นวดี สุวรรณมงคล
เลขาธิการคณะกรรมการกำกับหลักทรัพย์
และตลาดหลักทรัพย์
Ms. Ruenwadee Suwanmongkol
Secretary – General Office of the
Securities and Exchange Commission



นายไตรรัตน์ วิริยะศิริกุล
รองเลขาธิการ รักษาการแทนเลขาธิการ
คณะกรรมการกิจการกระจายเสียง
กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ



Mr. Trairat Viriyasirikul
Deputy Secretary – General NBTC
Acting Secretary – General NBTC

ประธานกรรมการ Chairman



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

กรรมการโดยตำแหน่ง Committees by Position

ศาสตราจารย์พิเศษ
วิศิษฐ์ วิศิษฐ์สรอรรถ
ปลัดกระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

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



นายปิยวัฒน์ ศิวรักษ์
เลขาธิการคณะกรรมการ
ข้าราชการพลเรือน
Mr. Piyawat Sivaraks
Secretary General,
Office of the Civil Service Commission

นางสาวกุลยา ตันติเตมิท
อธิบดีกรมบัญชีกลาง
Ms. Kulaya Tantitemit
Comptroller – General,
The Comptroller General's Department



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



พลอากาศตรี อมร ชมเชย
เลขาธิการคณะกรรมการการรักษาความมั่นคง
ปลอดภัยไซเบอร์แห่งชาติ
กรรมการและเลขานุการ
AVM Amorn Chomchoey
Secretary-General, National Cyber Security Committee
Acting as Committee member and Secretary

คณะกรรมการบริหารสำนักงานคณะกรรมการ การรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)

Committee Managing the Office of the
National Cybersecurity Committee (CMO)

กรรมการผู้ทรงคุณวุฒิ Honorary Committees

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



พลเอก ภูษพงศ์ พงษ์ศิริ
ด้านสังคมศาสตร์
General Pushpong Pongsiri
Expert Committee
on Social Sciences



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



นายฤทธิญา บุญยสมิต
ด้านกฎหมาย
Mr. Krisda Punyasmita
Expert Committee on Legal Affairs



รองศาสตราจารย์ ดร.เสาวณีย์ ไทยรุ่งโรจน์
ด้านเศรษฐศาสตร์
Assoc. Prof. Dr. Sauwanee Thairungroj
Expert Committee on Economics



นางแก้วใจ นาคสกุล
ด้านการบริหารจัดการองค์กร
Mrs. Kaewjai Nacsakul
Expert Committee
on Organizational Administration



การปฏิบัติงานของ กบส.ประจำปีงบประมาณ พ.ศ. 2566

Committee Managing the Office of the National Cybersecurity
Committee (CMO) Performance for Fiscal Year 2023

การเข้าร่วมประชุมของคณะกรรมการบริหารสำนักงาน คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.) ประจำปีงบประมาณ พ.ศ. 2566

Committee Managing the Office of the National Cybersecurity
Committee (CMO) Meeting Attendance for Fiscal Year 2023





หมายเหตุ

- จำนวนกรรมการทั้งหมด 12 คน
(ยกเว้นการประชุมครั้งที่ 6/2565 และ 7/2565
มีจำนวนกรรมการทั้งหมด 11 คน เนื่องจาก
กรรมการผู้ทรงคุณวุฒิว่าง 1 ตำแหน่ง)



คณะกรรมการและคณะอนุกรรมการ

กกบ. 1 คณะ

คณะอนุกรรมการด้านกฎหมาย

1. พลตำรวจตรี พิสิษฐ์ เปาอินทร์
2. พลตำรวจตรี อติศักดิ์ คุณพันธ์
3. ดร.รอม หิรัญพฤกษ์
4. ดร.พันธ์ศักดิ์ ศิริรัชตพงษ์
5. พลตรี ปณิธาน ทรัพย์รุ่งเรือง
6. นายสมญา พัฒนารพันธ์
7. นางจุไรรัตน์ จุลจักรวัฒน์
8. นายมนต์ ครุฑกุล
9. นายปรนนต์ ชูติธรรมโน
10. นายเทอดพงษ์ หงส์หิรัญเรือง
11. นางสาวพัชรี ไชยเรืองกิตติ
12. พลอากาศตรี อมร ชมเชย
13. พลอากาศตรี จเด็จ คูหะก้องกิจ
14. นางสาวตรุณี พิกุลทอง
15. ว่าที่ร้อยตรี อธิปไตย อางสาริการ

ประธานอนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการและเลขานุการ

ผู้ช่วยเลขานุการ

กกบ. 5 คณะ

1. คณะกรรมการตรวจสอบ

1. รองศาสตราจารย์ ดร.เสาวณีย์ ไทยรุ่งโรจน์
2. พลเอก ภูษพงศ์ พงษ์ศิริ
3. นางพิลาสลักษณ์ ยุคเกษมวงศ์
4. นางสาวศินี ธรรมศิริ
5. นางสาวณิชา ธนภัทรโชติศิริ

ประธานกรรมการตรวจสอบ

กรรมการตรวจสอบ

กรรมการตรวจสอบ

กรรมการตรวจสอบ

เลขานุการ

2. อนุกรรมการด้านยุทธศาสตร์

1. ศาสตราจารย์พิเศษวิศิษฎ์ วิศิษฎ์สรอรรถ
2. รองศาสตราจารย์สุรศักดิ์ สงวนพงษ์
3. นางสาวณิชากาญจน์ กัลยรัตน์ศิริ
4. นายธีรเดช ถิรพร
5. ดร.ชัยชนะ มิตรพันธ์
6. นายกำพล ศรีธนรัตน์
7. พลอากาศตรี อมร ชมเชย
8. นางมัตติกา จงพิริยะอนันต์
9. นางสาวสุกิสรา กุติอราม

ประธานอนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการและเลขานุการ

อนุกรรมการและผู้ช่วยเลขานุการ

3. อนุกรรมการประเมินผลการปฏิบัติงาน ของเลขาธิการคณะกรรมการการรักษา ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

1. ศาสตราจารย์พิเศษวิศิษฐ์ วิศิษฐ์สรอรรถ
2. นางสาววิริยา เนตรน้อย
3. นางแก้วใจ นาคสกุล
4. นางมัตติกา จงพิริยะอนันต์
5. นางสาวสุภิสรา กุติอราแม

4. อนุกรรมการด้านกฎหมาย

1. นายกฤษฎา บุญยสมิต
2. นายพัชโรดม ลิมปิหะญีร์
3. นายตามพ์ สุนทรทรัพย์
4. นายวรรณวิทย์ อาชุนบุตร
5. นางสาวกอบสิริ เอี่ยมสุรีย์
6. นางสาวตรุณี พิกุลทอง
7. นายสิริโชค ศิริโสภณ

5. อนุกรรมการด้านการบริหารงานบุคคล

1. นางแก้วใจ นาคสกุล
2. นายบรรณันท์ ทองกัลยา
3. นางสาววิภาดา ลีเฉลิมวงศ์
4. นางมุกดา เลิศลักษณ์พร
5. นางนิธินุช จรุงเกียรติ
6. นางกิงนภา บางขวด
7. นายปรภากร วงษ์จำรัส

ประธานอนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการและเลขานุการ

อนุกรรมการและผู้ช่วยเลขานุการ

ประธานอนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการและเลขานุการ

อนุกรรมการและผู้ช่วยเลขานุการ

ประธานอนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการ

อนุกรรมการและเลขานุการ

อนุกรรมการและผู้ช่วยเลขานุการ

คณะผู้บริหาร สกมช. NCSA Executives



พลอากาศตรี อมร ชมเชย
เลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัย
ไซเบอร์แห่งชาติ

AVM Amorn Chomchoey
Secretary-General
of the National Cyber Security
Committee

พลตรี วีรวุฒิ วิทยากรณ์
รองเลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัย
ไซเบอร์แห่งชาติ 4

Maj. Gen. Teerawut Wittayakorn
Deputy Secretary-General (4)





ผู้อำนวยการสำนัก NCSA Executives



นางพัชฎิชา ไกรแสงศรี
รักษาการผู้อำนวยการสำนักบริหารกลาง

Phatchicha Kraisansri
Acting Director of Central
Administration Office



นางมัตติกา จงพิริยะอนันต์
ผู้อำนวยการสำนักการเงิน
และกลยุทธ์องค์กร

Mattika Jongpiriyaanant
Director of Finance and
Organization Strategy Office

นายภาณุพงษ์ ธนุทอง
รักษาการผู้อำนวยการ
สำนักเทคโนโลยีสารสนเทศ

Panupong Thanutong
Acting Director of Information
Technology Office



พลอากาศตรี ดร.วุฒิกัทร จันทร์สาร
ผู้อำนวยการสำนักนโยบายยุทธศาสตร์
การรักษาความมั่นคงปลอดภัยไซเบอร์

AVM Vuthibhatra Chansarn, Ph.D.
Director of Cyber Security Strategy
and Policy Office



นางชไมพร พงศ์พยุหะ
รักษาการผู้อำนวยการศูนย์วิจัย
ความมั่นคงปลอดภัยไซเบอร์

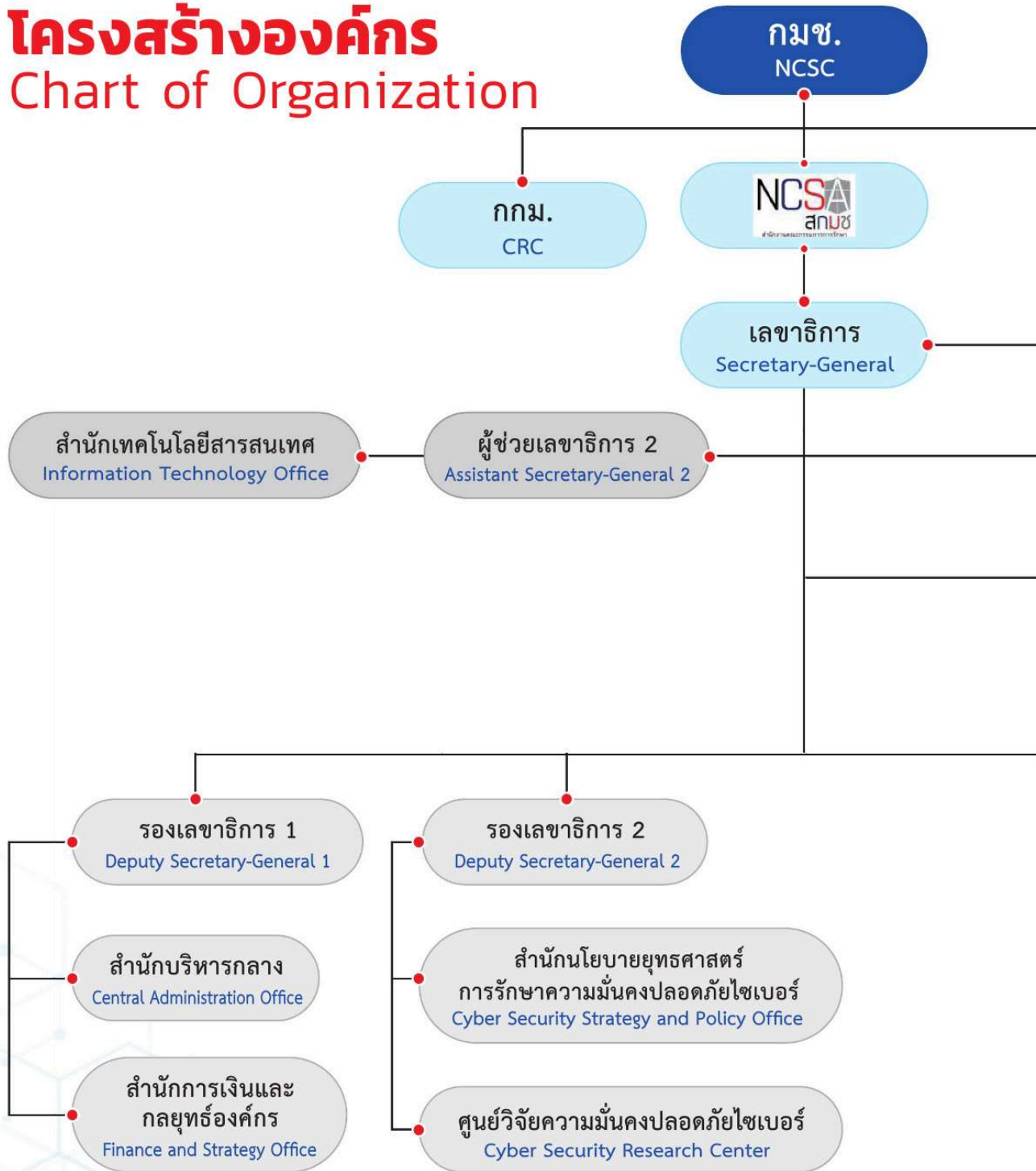
Chamaiporn Pongpayuha
Acting Director of Cyber
Security Research Center

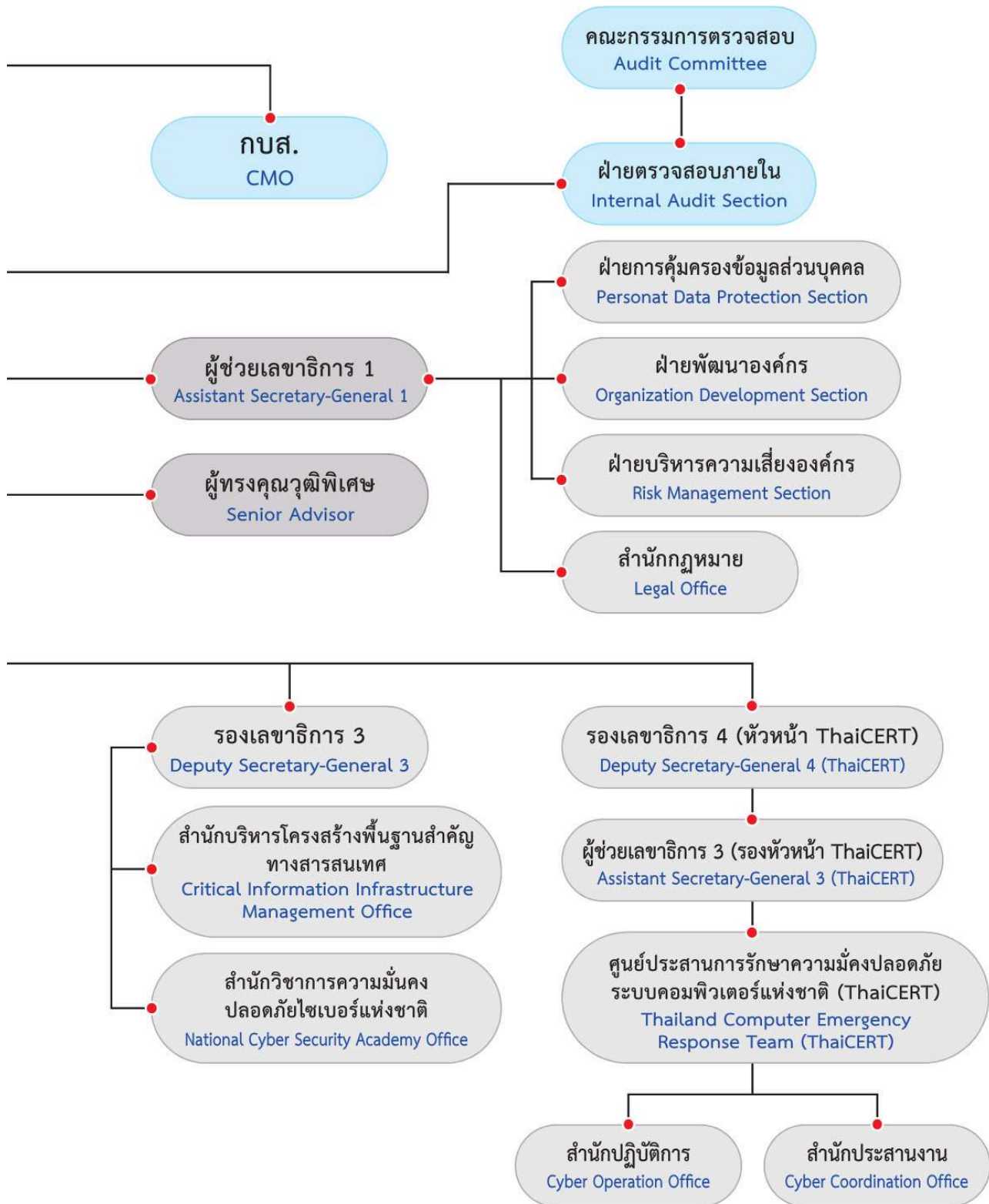




โครงสร้างองค์กร

Chart of Organization







PART : 1

การวางรากฐาน ความมั่นคงปลอดภัย ไซเบอร์ของประเทศ

Establishing the Cybersecurity
Foundation of the Country

“กว่าทศวรรษที่ผ่านมา สถานการณ์ภัยคุกคามทางไซเบอร์ทั้งภายในประเทศและระหว่างประเทศ มีเหตุการณ์โจมตีทางไซเบอร์ต่อระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ส่งผลกระทบต่อความมั่นคงของรัฐและประชาชนเป็นวงกว้าง ตัวอย่างกรณีการโจมตีประเทศ Estonia ด้วย DDoS ที่ใหญ่ที่สุด ที่ส่งผลกระทบต่อระบบคอมพิวเตอร์ของประเทศทุกระบบทั้งเว็บไซต์ และการให้บริการทางการเงินต้องหยุดชะงัก ไม่สามารถให้บริการได้หลายสัปดาห์ เหตุการณ์ดังกล่าว แสดงให้เห็นว่า ความมั่นคงปลอดภัยไซเบอร์เป็นเรื่องที่ต้องเร่งกระทำ และพัฒนาขีดความสามารถด้านการรับมือภัยคุกคามทางไซเบอร์ที่เกิดขึ้น หรือคาดว่าจะเกิดขึ้น”

“Over the past decade, the cybersecurity landscape, within the country and abroad, has been marked by cyber incidents targeting critical information infrastructure, which affects the security of the nation and its citizens. For example, the cyber attack on Estonia through a massive DDoS (Distributed Denial of Service) disrupted the country’s computer systems. Websites and other financial services were interrupted and remained inaccessible for several weeks. This incident shows the urgent need to enhance and develop capabilities to respond and anticipate both present and future cyber threats.”

บทเรียนภัยคุกคามทางไซเบอร์ Cyber Threat Lessons Learned

ภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงของประเทศ
Cyber threats affecting the national security



กรณีการโจมตีประเทศ Estonia ด้วย DDoS ที่ใหญ่ที่สุด ที่ส่งผลกระทบต่อระบบคอมพิวเตอร์ของประเทศทุกระบบทั้งเว็บไซต์ และการให้บริการทางการเงินหยุดชะงัก ไม่สามารถให้บริการได้หลายสัปดาห์

The largest DDoS attack incident in Estonia's history affected all of the country's computer systems, including websites and financial services, causing disruptions that lasted for several weeks.



เหตุการณ์แฮกเกอร์เข้ายึดคอมพิวเตอร์ที่ใช้ควบคุมระบบไฟฟ้าของทั้ง 3 บริษัทไฟฟ้าของยูเครน ส่งผลให้ไฟฟ้าดับเป็นวงกว้างส่งผลกระทบต่อผู้ใช้ไฟฟ้าประมาณ 250,000 ครัวเรือน

Hackers gained control of the computers that managed the electrical systems of three Ukrainian power companies. This resulted in widespread power outages, affecting roughly 250,000 households.



รวมไปถึงเหตุการณ์โจมตีระบบการให้บริการที่สำคัญต่าง ๆ ภายในประเทศไทย ที่ส่งผลให้เกิดการรั่วไหลของข้อมูลส่วนบุคคล และเป็นต้นตอของสาเหตุอาชญากรรมทางไซเบอร์ ไม่ว่าจะเป็นการหลอกลวงผ่านสื่อสังคมออนไลน์ เป็นต้น สิ่งเหล่านี้แสดงให้เห็นถึงผลกระทบต่อเศรษฐกิจ และสังคมที่ประชาชนได้รับผลกระทบ และมีแนวโน้มทวีความรุนแรงเพิ่มมากขึ้น

There were attacks on critical infrastructure in Thailand, leading to personal data leaks. These attacks are the major root cause of cybercrime, manifesting in various forms like social media scams. The impact is far-reaching, affecting both the economy and society, with a concerning upward trend in its severity.



ด้วยความจำเป็นเร่งด่วนในเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างเป็นทางการประเทศไทย จึงได้มีการตราพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และมีผลบังคับใช้เมื่อวันที่ 28 พ.ค. 62 เป็นต้นไป

Recognizing the critical needs for cybersecurity, Thailand implemented the Cybersecurity Act B.E. 2562 (2019), which entered into force on May 28, 2019.

จุดเริ่มต้น พ.ร.บ. การรักษาความมั่นคง ปลอดภัยไซเบอร์ พ.ศ. 2562

ICT เสนอ (ร่าง) พ.ร.บ.
ต่อ ครม.

The MICT submitted
the draft Cybersecurity
Act to the Cabinet.

29 ธันวาคม 2557

December 29, 2014

คณะกรรมการกฤษฎีกา ตรวจสอบพิจารณา
(ร่าง) พ.ร.บ. แล้วเสร็จ (เรื่องเสร็จที่ 1490/2561)

The Council of State concluded its
review of the draft Cybersecurity Act.
(Finished Case No. 1490/2018)

26 กันยายน 2561

September 26, 2018

6 มกราคม 2558

January 6, 2015

ครม. มีมติอนุมัติหลักการ
(ร่าง) พ.ร.บ.

The Cabinet approved
the draft Cybersecurity
Act in principle.

13 ธันวาคม 2561

December 13, 2018

MDES เสนอ (ร่าง) พ.ร.บ.
ฉบับปรับปรุง
ต่อ ครม.

The MDES submitted the
revised draft Cybersecurity
Act to the Cabinet.

Starting Points of the Cybersecurity Act B.E. 2562 (2019)

ครม. มีมติอนุมัติ
หลักการ (ร่าง) พ.ร.บ.
ฉบับปรับปรุง

The Cabinet approved
the draft Cybersecurity
Act in principle.

18 ธันวาคม 2561
December 18, 2018

พ.ร.บ. ประกาศ
ในราชกิจจานุเบกษา

The Cybersecurity
Act was published in the
Royal Gazette.

27 พฤษภาคม 2562
May 27, 2019

28 กุมภาพันธ์ 2562
February 28, 2019

สภานิติบัญญัติ มีมติ
เห็นชอบ (ร่าง) พ.ร.บ.

The National
Legislative Assembly of
Thailand passed the
Cybersecurity Act.

28 พฤษภาคม 2562
May 28, 2019

พ.ร.บ. มีผลใช้บังคับ

The Cybersecurity
Act entered into force.

การวางรากฐานและก้าวไปข้างหน้าอย่างมั่นคง

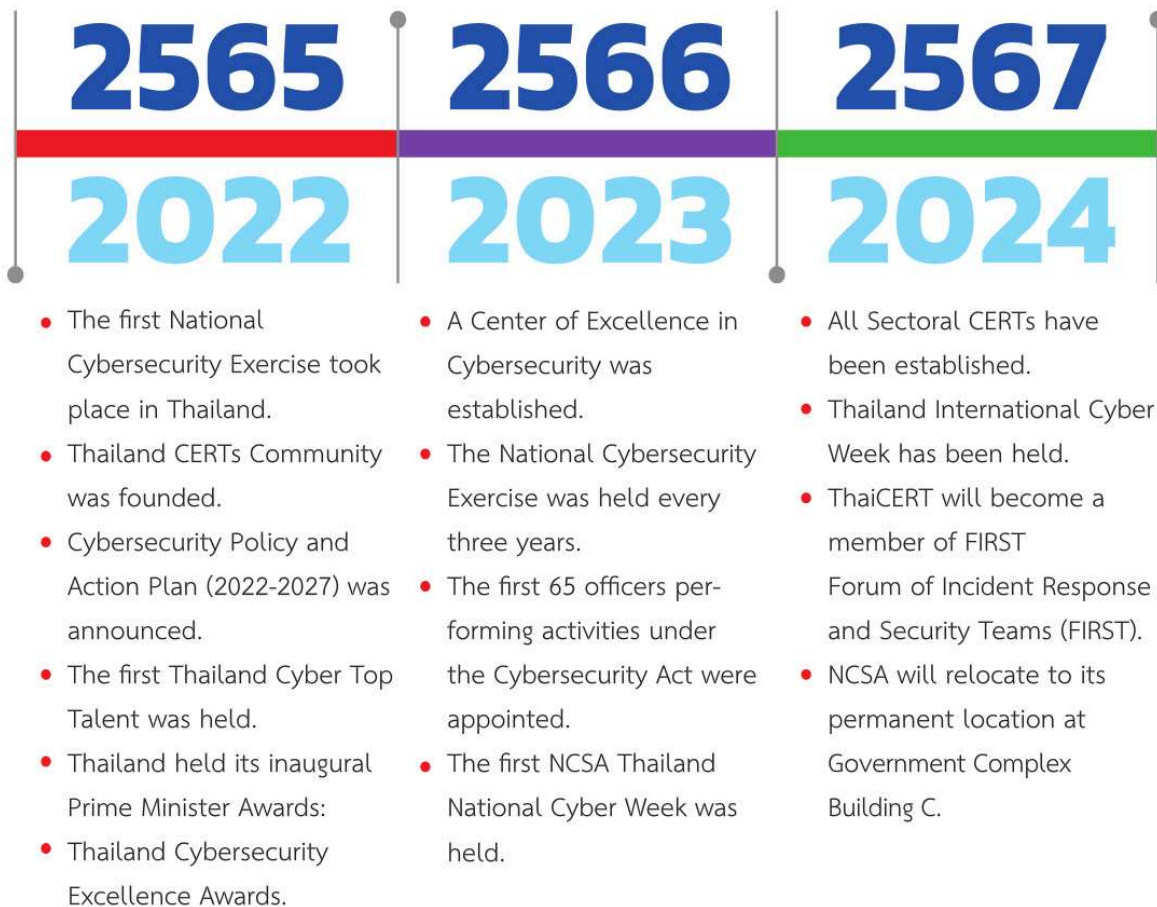
Enhancing Cybersecurity

- พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีผลใช้บังคับ
- มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
- มีคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)
- มีคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)
- มีคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)
- มีการจัดตั้ง National CERT
- กมช. กำหนด Regulator 7 ด้าน และกำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็น CII เป็นครั้งแรก
- มีการแต่งตั้ง ลธ.กมช. คนแรก (พลเอก ประยุทธ์ เฉลิมวัฒน์)
- ครม. มีมติอนุมัติให้มีผู้มาปฏิบัติงานที่ สกมช. จำนวน 42 ราย



- The Cybersecurity Act 2019 entered into force.
- The National Cyber Security Agency (NCSA) was established.
- The National Cyber Security Committee (NCSC) was created.
- The Cybersecurity Regulating Committee (CRC) was created.
- The Committee Managing the Office of the National Cybersecurity Committee (CMO) was created.
- The National CERT was established.
- The NCSC identified 7 regulators and established, for the first time, the characteristics of Critical Information Infrastructure (CII) entities.
- General Pratchaya Chalermwat was named the first Secretary-General of the NCSA.
- The Cabinet approved the appointment of 42 officers to the NCSA.

- มีการฝึก National Cybersecurity Exercise เป็นครั้งแรกของประเทศไทย
- มีการจัดตั้งกลุ่ม Thailand CERTs Community
- มีการประกาศใช้นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)
- มีการจัด Thailand Cyber Top Talent ครั้งแรก
- มีการจัด Prime Minister Awards: Thailand Cybersecurity Excellence Awards เป็นครั้งแรก (รางวัลด้านความมั่นคงปลอดภัยไซเบอร์ดีเด่นระดับชาติ)
- มีการจัดตั้ง Center of Excellence ด้านวิชาการความมั่นคงปลอดภัยไซเบอร์
- มีการฝึก National Cybersecurity Exercise วงรอบ 3 ปี
- มีการแต่งตั้งพนักงานเจ้าหน้าที่ตาม พ.ร.บ. รุ่นแรก จำนวน 65 ราย
- มีการจัด NCSA Thailand National Cyber Week เป็นครั้งแรก
- มีการจัดตั้ง Sectoral CERT ครบทุกด้าน
- มีการจัด Thailand International Cyber Week
- ThaiCERT เข้าร่วมเป็นสมาชิกของ FIRST
- ย้ายสำนักงานไปที่ตึกถาวร ณ ศูนย์ราชการ อาคาร C





ศูนย์ประสานการรักษาความมั่นคงปลอดภัย ระบบคอมพิวเตอร์แห่งชาติ

(Thailand Computer Emergency Response Team (ThaiCERT))



เดิม Thailand Computer Emergency Response Team (ThaiCERT) เป็นหน่วยงานภายใต้การดูแลของ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ หรือ Electronic Transactions Development Agency (ETDA) ตั้งแต่ปี พ.ศ. 2554 โดยมีภารกิจในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

ปัจจุบัน ด้วยพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีผลบังคับใช้ กำหนดให้มีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ Thailand Computer Emergency Response Team (ThaiCERT) ขึ้น โดยเป็นหน่วยงานภายใน สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และมติคณะรัฐมนตรี วันที่ 21 กุมภาพันธ์ 2566 ให้โอน ThaiCERT (เดิม) พร้อมบรรดาภารกิจที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ มาเป็นหน่วยงานภายใต้ สกมช. แล้ว

Previously, Thailand Computer Emergency Response Team (ThaiCERT) was a unit operated under the supervision of Electronic Transactions Development Agency (ETDA) since 2011, with the mission of maintaining the country's cyber security.

Currently, with the Cybersecurity Act 2019 taking effect, Thailand Computer Emergency Response Team (ThaiCERT) was established as an internal unit of the National Cyber Security Agency (NCSA) Furthermore, by the resolution of the Cabinet on February 21, 2023 ThaiCERT (previously) along with all missions related to maintaining the country's cyber security to be a unit under the NCSA.

02

01

03

04

05

06

07

PART : 2

การพัฒนา ขีดความสามารถการรักษา ความมั่นคงปลอดภัย ไซเบอร์ทุกมิติ

- การป้องกัน
- การรับมือ
- การลดความเสี่ยง

Development of Cybersecurity
Capabilities in All Dimensions

- Cyber threats prevention
- Cyber Incident Response
- Mitigation of cyber threats

“อยู่ในช่วงการเสริมสร้างขีดความสามารถของหน่วยงานที่มีหน้าที่รักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมทั้งการสร้างการรับรู้และความตระหนักรู้ให้กับสังคมไทยโดยทั่วไป โดยการมุ่งเน้นกับการสร้างความเข้มแข็งให้กับ สกมช. หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานของรัฐ”

“Thailand is in the process of strengthening the capabilities of agencies responsible for maintaining national cybersecurity. This includes raising awareness and understanding of cybersecurity within Thai society at large. The focus is on strengthening the National Cyber Security Agency, Regulators, organizations of Critical Information Infrastructure, as well as government agencies.”

การป้องกันภัยคุกคามทางไซเบอร์

Enhance Personal Skills and Expertise in Cybersecurity

การยกระดับทักษะบุคลากรผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ การสร้างการรับรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานเป้าหมาย (Cyber Clinic)

Enhancing the skills of cybersecurity officers
cybersecurity awareness training for target agencies (Cyber Clinic)

การสัมมนาเชิงปฏิบัติการสำหรับหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ประจำปีงบประมาณ พ.ศ. 2566 (NCSA Cyber Clinic 2023) มีการจัดสัมมนา 10 ครั้ง ผ่านสื่ออิเล็กทรอนิกส์ Zoom Cloud Meeting โดยมีผู้สนใจเข้าร่วมตลอดปีกว่า 1,600 คน โดยเป็นหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานของรัฐ และหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ จำนวน 74 หน่วยงาน และหน่วยงานเอกชน จำนวน 17 หน่วยงาน

The National Cyber Security Agency (NCSA) has organized a seminar on the NCSA Cyber Clinic for government agencies, regulators, and Critical Information Infrastructure (CII) in 2023. There were 10 seminars organized through online meetings. There were 10 seminars via online meetings with approximately 1,600 participants throughout the year, including participants from 74 Government Agencies, Regulators, and CII and 17 private agencies.

ผู้สนใจเข้าร่วม
ตลอดปีกว่า **1,600 คน**

โครงสร้างพื้นฐานสำคัญ
ทางสารสนเทศ **74 หน่วยงาน**

หน่วยงาน
เอกชน **17 หน่วยงาน**





การฝึกอบรมเชิงปฏิบัติการด้านภัยคุกคามทางคอมพิวเตอร์และระบบสารสนเทศ
หน่วยงานของรัฐ และหน่วยงานปกครองส่วนท้องถิ่นทุกแห่งทั่วประเทศ

NCSA

CYBER CLINIC 2023

ครั้งที่ 10/2566

📅 วันพุธที่ 27 กันยายน 2566 ⌚ 13.00 – 14.00 น.

📍 โรงแรมอเรียต้าพลาซ่า อาคาร 54 เขตวัฒนา กรุงเทพมหานคร
พร้อมพิธีเปิด ณ พ.ศ.2562

📞 ติดต่อสอบถาม : 02-2552-7921 | 📧 training@ncsa.go.th



“ประกาศคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมินปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564”

โดย พ.ต.อ.ณัทฤช พรหมจันทร์ ผู้อำนวยการสำนักปฏิบัติการ สกมช.

Notification of NCSC Re: Characteristics and Measures for Prevention, Response, Assessment, Eradication, and Containment of Cybersecurity Incidents at Each Level B.E. 2564 (2021)



“การประเมินความเสี่ยงและการจัดทำผลสรุปตามมาตรา 54”

โดย รองศาสตราจารย์ ดร.พงษ์พิสิฐ วุฒิวิชชุโขติ

Section 54 Compliance : Risk Assessment and Reporting



“การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ และการจัดทำผลสรุป ตามมาตรา 54”

โดย นายเมธา สุวรรณสาร

Section 54 Compliance : Cyber Security Audit and Reporting



“การรับ-ส่งอีเมลด้วยวิธีการ PGP”

โดย พ.ต.อ.ณัทฤช พรหมจันทร์ ผู้อำนวยการสำนักปฏิบัติการ สกมช.

Receiving and Sending Emails with PGP Encryption



“การจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ”

โดย รองศาสตราจารย์ ดร.พงษ์พิสิฐ วุฒิวิชชุโขติ หัวหน้าภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ คณะเทคโนโลยีสารสนเทศ และนวัตกรรมดิจิทัล มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

Developing Code of Practices and Standard Frameworks for Government Agencies and Organizations of Critical Information Infrastructure



การประเมินระดับความพร้อมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตาม NIST Cybersecurity Framework (ผู้แทน บริษัท Time consulting)

โดย ดร.ธัชพล โปษยานนท์ อนุกรรมการยุทธศาสตร์ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) และคุณจิรนนท์ แก้วดี ผู้จัดการโครงการ TIME consulting

Assessment of Readiness Level in Cybersecurity According to NIST Cybersecurity Framework



การขับเคลื่อนนโยบายและแผนปฏิบัติการด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570)

โดย นางชไมพร พงศ์พยุหะ ผู้อำนวยการฝ่ายนโยบายและแผนยุทธศาสตร์
รักษาการผู้อำนวยการสำนักนโยบายยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ สกมช.
Implementing Organizational Cyber Security Policy and Plans (2022 – 2027)

การขับเคลื่อนยุทธศาสตร์ชาติสู่การปฏิบัติผ่านแผนสามระดับ การจัดทำโครงการและการติดตามประเมินผล

โดย นางสาวศศิธร พลัดเดช ที่ปรึกษาด้านนโยบายและแผนงาน
สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ
Driving National Strategy into Implementation through Three-Level
Planning, Project Development, and Outcome Monitoring

การขับเคลื่อนแผนแม่บทฯ ประเด็นความมั่นคง และนโยบายและแผนระดับชาติ ว่าด้วยความมั่นคงแห่งชาติ

โดย นายจิรายุ ฉัตระทิน นักวิเคราะห์นโยบายและแผนปฏิบัติการ
กองนโยบายและยุทธศาสตร์ความมั่นคง สำนักงานสภาความมั่นคงแห่งชาติ
Implementing the National Master Plan on Security Issues
and National Security Policy and Planning



ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ แห่งชาติ เรื่อง การกำหนดระดับความรู้ความชำนาญ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อแต่งตั้ง เป็นพนักงานเจ้าหน้าที่ พ.ศ. 2564

โดย เรืออากาศเอก นพรัตน์ สุจินดา
ผู้อำนวยการฝ่ายปฏิบัติการทางไซเบอร์ สำนักปฏิบัติการ สกมช.
Notification of NCSC Re: Cybersecurity Knowledge and
Expertise Requirements for Competent Official Appointment
B.E. 2564 (2021)



ระเบียบคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยการมอบอำนาจในการดำเนินการเพื่อรับมือ กับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง พ.ศ. 2565

โดย นางสาวตรุณี พิกุลทอง ผู้อำนวยการสำนักกฎหมาย สกมช.
Regulations of CRC on the Assignment of Powers to Perform Tasks
on behalf of the Cybersecurity Regulating Committee B.E. 2565 (2022)



เตรียมการจัดทำรายงานมาตรา 54 ของพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

โดย พลอากาศตรี จเด็จ คูหะก้องกิจ ผู้ช่วยเลขาธิการ 3 สกมช.
Cybersecurity Act B.E. 2562 (2019) Section 54 Compliance :
Report Preparation

การอบรม Cyber Bootcamp Project

สกมช. ร่วมกับ Australian National University (ANU) และสถานเอกอัครราชทูตออสเตรเลีย ประจำประเทศไทย จัดอบรมให้กับบุคลากรผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ จากหน่วยงานภาครัฐและเอกชน จำนวน 20 คน เพื่อยกระดับความรู้และเพิ่มพูนทักษะให้กับบุคลากรทางด้านไซเบอร์ ในประเทศ เมื่อวันที่ 12-14 กันยายน 2566 ณ โรงแรมคิมป์ตัน มอลล์ กรุงเทพฯ

On September 12 - 14, 2023, the National Cyber Security Agency (NCSA) cooperate with the Australian National University (ANU) and the Australian Embassy in Thailand conducted training for 20 cyber security personnel from government and private agencies to improve skills in cyber security at the Kimpton Malai Hotel in Bangkok.



โครงการพัฒนาขีดความสามารถกระบวนการปฏิบัติงานด้านไซเบอร์ ตามมาตรฐานสากลของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Lead Implementer Lead Auditor)

Project to develop the capability of cyber operations processes according to international standards of the organizations of critical information infrastructure.

เพื่อเผยแพร่และสร้างความเข้าใจให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานเอกชน ในด้านนโยบายและกฎระเบียบที่เกี่ยวข้องด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงมาตรการ มาตรฐาน และแนวปฏิบัติขั้นต่ำ และแนวทางการส่งเสริมในการปกป้องและรักษาความมั่นคงปลอดภัยไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ตามมาตรฐาน NIST Cybersecurity Framework หรือ ISO/IEC 27001

To promote the development of cyber security policies and regulations for government agencies, regulators, Critical Information Infrastructure (CII), and private agencies, including Minimum Standards for Data or Information Systems and Standards and Guidelines for Promoting the Development of Cybersecurity Service Systems in accordance with the Cybersecurity Act 2019 and the NIST Cybersecurity Framework or ISO/IEC 27001 standards.



กิจกรรมการอบรมเชิงปฏิบัติการพัฒนาขีดความสามารถผู้ปฏิบัติงานตามมาตรฐานสากล ภายใต้โครงการการยกระดับทักษะบุคลากรภาครัฐเพื่อตอบสนองความต้องการของประเทศ Workshop to improve competence in accordance with international standards to improve government personnel abilities to accommodate the requirements of the nation.

มีวัตถุประสงค์เพื่อพัฒนาศักยภาพบุคลากรผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ในหน่วยงานภาครัฐทั้งในส่วนกลางและส่วนภูมิภาค และมีกลุ่มเป้าหมายเป็นบุคลากรภาครัฐ ได้แก่ ผู้ปฏิบัติงาน หน่วยงานท้องถิ่น ผู้ปฏิบัติงานหน่วยงานด้านสาธารณสุข ผู้ปฏิบัติงานหน่วยงานด้านการศึกษา และผู้ปฏิบัติงาน หน่วยงานภาครัฐ และมีผู้สมัครเข้าร่วมโครงการกว่า 3,000 คน จากทั่วประเทศ โดยคัดเลือกจากผู้มีคุณสมบัติ ตรงตามวัตถุประสงค์จำนวน 450 คน นำไปสู่การคัดเลือกกลุ่มเป้าหมายที่มีศักยภาพทางด้านความมั่นคงปลอดภัย ไซเบอร์ จำนวนไม่น้อยกว่า 225 คน เข้ารับการพัฒนางานองค์ความรู้เพื่อเข้ารับการประเมินทักษะตามมาตรฐาน ในระดับสากล ซึ่งได้ดำเนินการจัดอบรมพัฒนาศักยภาพบุคลากรผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัย ไซเบอร์ จำนวน 9 รุ่น ดังนี้

The workshops aim to develop skills and knowledge in cybersecurity for personnel of central and provincial government agencies. Among the 3,000 people who registered, 450 qualified individuals were selected to join the program. From this group, 250 participants were further filtered to enter an international assessment program. Nine batches of workshops were conducted before the conclusion of the program.

- รุ่นที่ 1** ณ กรุงเทพมหานคร
- รุ่นที่ 2** ณ จังหวัดเชียงใหม่
- รุ่นที่ 3** ณ จังหวัดพิษณุโลก
- รุ่นที่ 4** ณ จังหวัดอุดรธานี
- รุ่นที่ 5** ณ จังหวัดมหาสารคาม
- รุ่นที่ 6** ณ จังหวัดสุราษฎร์ธานี
- รุ่นที่ 7** ณ จังหวัดสงขลา
- รุ่นที่ 8** ณ จังหวัดชลบุรี
- รุ่นที่ 9** ณ จังหวัดกาญจนบุรี



ด้านการสร้างความตระหนักรู้ ด้านความมั่นคงปลอดภัยไซเบอร์ให้กับประชาชน Raising Public Awareness of Cybersecurity

โครงการอบรม NCSA Cybersecurity Knowledge Sharing ประจำปีงบประมาณ พ.ศ. 2566 เพื่อเป็นการเสริมความรู้ให้กับบุคลากรผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ นักเรียน นักศึกษา ครู/อาจารย์ ผู้ปกครอง คนพิการ ผู้สูงอายุ และประชาชนทั่วไปให้มีความรู้ความเข้าใจ เพื่อสร้างความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ ให้ทราบถึงข้อมูลรายงานทิศทางของภัยคุกคามในระดับประเทศและระดับโลก ให้กับผู้เข้าร่วมรับฟังเพื่อเตรียมรับมือให้เท่าทันภัยคุกคามทางไซเบอร์ ตลอดปี 2566 ให้ทันต่อการเปลี่ยนแปลงและภัยคุกคามใหม่ ๆ อยู่ตลอดเวลา โดยมีการจัดอบรมทั้งหมด 10 ครั้ง ในรูปแบบ Onsite และ Online มีผู้สนใจเข้าร่วมกว่า 62,000 คน ซึ่งมีหัวข้อที่น่าสนใจดังนี้

มีผู้สนใจเข้าร่วมกว่า | **62,000 คน**

NCSA's Cybersecurity Knowledge Sharing 2023, seminars on various cybersecurity-related topics, were organized to enhance the knowledge and understanding of cybersecurity for cybersecurity professionals, students, teachers, parents, persons with disabilities, the elderly, and the public. The primary goal of the workshops is to equip participants with awareness and understanding of cyber threats, encompassing both domestic and international threat landscapes. Through this knowledge enhancement, our objective is to enable the public to effectively confront cybersecurity challenges throughout the year 2023.

หัวข้อ Topic

แนวคิดการประเมิน Cyber Risk Scoring

"Cyber Risk Scoring"





101 OT Security : กับการวางแผนด้านความปลอดภัยไซเบอร์ในระดับองค์กร

"OT Security 101 and How to Prepare Cybersecurity Plans for your Organization"

หัวข้อ Topic

หัวข้อ
Topicภัย Call Center : กลลวงออนไลน์
บทเรียนราคาแพง"Call Center Scams and Online
Fraud : Lessons Learned the Hard Way"หัวข้อ
Topic

"I use cloud, can it be Hacked"

หัวข้อ
Topic"สถาปัตยกรรม Zero Trust
ตามรูปแบบของ NIST SP 800-207""Zero Trust architecture based on
NIST SP 800-207"หัวข้อ
Topic"แนวปฏิบัติการทดสอบเจาะระบบ
(Penetration Testing Best Practices)
& Breach Attack Simulation""Penetration Testing Best Practices &
Breach Attack Simulation"หัวข้อ
Topic

ผู้สูงวัยกับภัยออนไลน์

"The Elderly and the Danger
of Online Scams"หัวข้อ
TopicRomance Scam
รู้ทัน ไม่ซ้ำรัก"Love Bites: Unveiling
Online Romance Scams"

ด้านการประสานความร่วมมือทางวิชาการ

สกมช. ได้มีการแลกเปลี่ยนองค์ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ร่วมกับหน่วยงานพันธมิตรภาคเอกชน ในการอบรมให้กับบุคลากรผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ทั้งภาครัฐและเอกชน ดังนี้



“การคาดการณ์แนวโน้มและทิศทางของภัยคุกคามทางไซเบอร์ในปี พ.ศ.2566”

kaspersky

- “Cyber Immunity for a Secure Digital World”
- NCAS : National SOC Workshop with Kaspersky



- “Thailand Future Cyber Thought Leader 2023”
- Windows System Security Basics and Reinforcement Training
- Linux System Security Basics and Reinforcement Training
- Penetration Testing Technology Training
- HCIA Security Certificate Training
- Global Cybersecurity Trends (CLMV)



ISC2 Bangkok Chapter : August 2023 Event

Guardians of the Clouds: Ensuring Security in a Multi-Cloud Era



เกษียณอย่างมีความสุข อย่าให้มีทุกข์จากภัยไซเบอร์

โครงการพัฒนากำลังคนด้าน Cybersecurity ระดับอุดมศึกษา

สกมช. ได้ตระหนักถึงความสำคัญในการผลิตกำลังคนด้าน Cybersecurity เพื่อฝึกพื้นฐานในการพัฒนาศักยภาพของกำลังคนให้ตอบโจทย์ความต้องการของภาคอุตสาหกรรมด้าน Cybersecurity และ สกมช. ได้คัดเลือกนิสิต/นักศึกษา สังกัดมหาวิทยาลัย/สถาบัน สมาชิก ทปอ. และ สอ. ประเทศไทย ที่ต้องการฝึกประสบการณ์วิชาชีพ ในสาขาวิชา Computer science, Cyber security และสาขาอื่นๆ ที่เกี่ยวข้อง จำนวน 20 คน เข้ารับการฝึกประสบการณ์วิชาชีพ ณ สกมช.



โครงการเสริมสร้างความรู้ความเข้าใจและสร้างความตระหนักเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

เพื่อเสริมสร้างความรู้ความเข้าใจเกี่ยวกับกฎหมาย กฎ ระเบียบ แผน นโยบาย มาตรฐาน และมาตรการต่าง ๆ ที่เกี่ยวข้อง ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อสร้างความตระหนักรู้เกี่ยวกับการป้องกัน การรับมือ ภัยคุกคามด้านไซเบอร์ และสามารถนำความรู้ที่ได้รับไปถ่ายทอดให้บุคคลในหน่วยงาน หรือบุคคลในครอบครัวได้ โดย สกมช. ร่วมกับ กอ.รมน. และ AIS สร้างความตระหนักรู้ด้าน Cybersecurity ให้กับผู้นำหน่วยงานและประชาชน ในรูปแบบ onsite ใน 3 จังหวัด ได้แก่ จังหวัดขอนแก่น จังหวัดเชียงใหม่ และจังหวัดภูเก็ต กว่า 180 คน

online จำนวน 4 ครั้ง | **8,200 คน**
มีผู้เข้าร่วมมากกว่า

กิจกรรม Industrial Based Skill Day

ภายใต้แนวคิด “สร้างตนเองให้มีค่า พัฒนา ให้ตลาดต้องการ” ผ่านสื่ออิเล็กทรอนิกส์ เมื่อวันที่ 11 กรกฎาคม 2566 เพื่อเป็นการส่งเสริมการพัฒนาทักษะด้าน Cybersecurity ให้กับนิสิต นักศึกษาของมหาวิทยาลัย ให้ตรงกับความต้องการของตลาดแรงงานในปัจจุบัน และมีการแลกเปลี่ยนองค์ความรู้ด้านการจัดหลักสูตรความมั่นคงปลอดภัยไซเบอร์ วิทยาลัยการคอมพิวเตอร์มหาวิทยาลัยขอนแก่น โดย ดร.เพชร อิมทองคำ ประธานหลักสูตร วท.บ. ความมั่นคงปลอดภัยไซเบอร์ วิทยาลัยการคอมพิวเตอร์ มหาวิทยาลัยขอนแก่น และแนวทางสอบใบ Certification จากหน่วยงานพันธมิตร โดยมี นิสิต นักศึกษา อาจารย์ และผู้ที่สนใจเข้าฟังเป็นจำนวนมาก



การให้บริการทางวิชาการ

ในปีงบประมาณ พ.ศ. 2566 สกมช. ได้จัดวิทยากรบรรยายตามคำเชิญจากหน่วยงานของรัฐและเอกชน เพื่อสร้างความตระหนักรู้และสร้างภูมิคุ้มกันบนโลกออนไลน์ให้กับบุคลากรของหน่วยงานทั่วประเทศ ทั้งในรูปแบบ Online และ Onsite







สกมช. จัดกิจกรรม และจัดการแข่งขัน CTI-CTF ผ่านโจทย์ที่ท้าทายโดยใช้ระบบ Cyber Threat Intelligence (CTI) ในรูปแบบ Capture the Flag (CTF) โดยมีวัตถุประสงค์ ดังนี้

- เพื่อถ่ายทอดความรู้ และเสริมสร้างความเข้าใจเกี่ยวกับระบบ CTI
- เพื่อเพิ่มพูนความรู้ความเข้าใจ รวมไปถึงการประยุกต์ใช้ระบบ CTI ให้เกิดประโยชน์สูงสุดและสามารถตอบสนองต่อความต้องการของหน่วยงานได้อย่างแท้จริงต่อระบบ CTI
- เพื่อยกระดับมาตรฐานการเฝ้าระวัง ติดตาม และป้องกันภัยคุกคามทางไซเบอร์ ตลอดจนการเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ให้กับหน่วยงานในประเทศไทยอย่างมีระบบและยั่งยืน สามารถรับมือกับภัยคุกคามทางไซเบอร์ในรูปแบบใหม่ได้ทันต่อเหตุการณ์

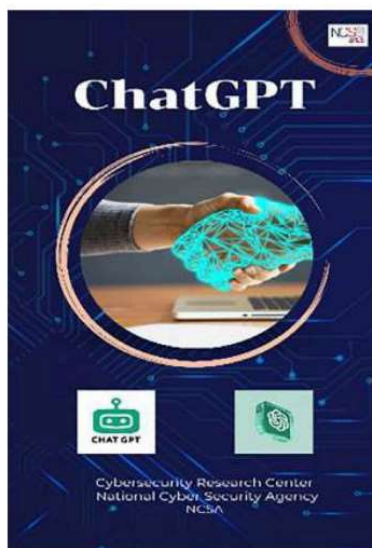
NCSA organized activities and competitions CTI-CTF, presenting challenging questions using the Cyber Threat Intelligence (CTI) system in a Capture the Flag (CTF).

- Increase knowledge and understanding about the CTI system for government and private agencies interested in the NCSA CTI system.
- Increase knowledge and understanding including how to use the CTI system to its full potential and effectively handle the agency's requirements for it.
- Raise the standard for monitoring, detecting, and preventing cyber threats. as well as strengthen cyber security for agencies in Thailand systematically and sustainably able to deal with new cyber threats promptly.

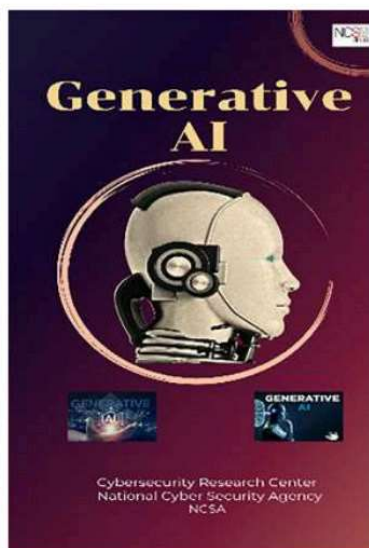
วิชาการงานวิจัย Academic Research

หนึ่งในภารกิจสำคัญของ สกมช. คือ การสร้างความตระหนักรู้ให้แก่ทุกภาคส่วนในสังคมไทยให้รู้เท่าทันถึงเทคโนโลยีที่กำลังก้าวหน้าขึ้นและภัยไซเบอร์ที่พร้อมเข้าคุกคามทุกขณะ ศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์ได้ทำการรวบรวมข้อมูลวิจัย ข่าวสาร รายงานต่าง ๆ ทั้งภายในและนอกประเทศ มาเรียบเรียงเป็นบทความเพื่อเผยแพร่ความรู้ความเข้าใจด้านความมั่นคงปลอดภัยไซเบอร์ด้านต่าง ๆ เพื่อเสริมสร้างภูมิคุ้มกันและการตระหนักรู้ด้านไซเบอร์ หัวข้อบทความวิชาการในรอบปีที่ผ่านมา “ChatGPT” “Generative-AI” และ “Post-Quantum Cryptography”

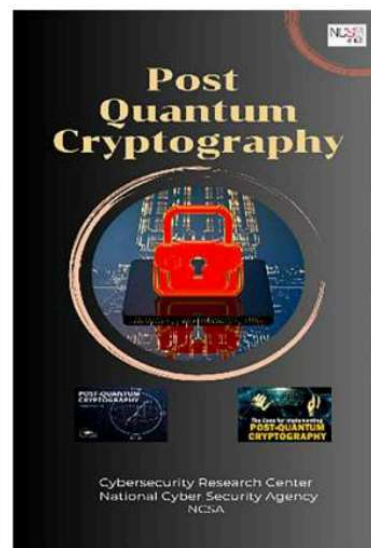
The National Cyber Security Agency (NCSA) primary goal is to raise awareness in all sectors of Thai society about the latest technological developments and cyber threats. The Cyber Security Research Center has gathered research data, news, and reports from both inside and outside the country and compiled them into articles to share knowledge and understanding of various aspects of cyber security to strengthen immunity and cyber awareness. The topics of academic articles in previous years included “ChatGPT”, “Generative- AI,” and “Post-Quantum Cryptography.”



Chat GPT



Generative-AI



Post-Quantum
Cryptography

สกมช. ร่วมกับ อว. แลกเปลี่ยนความรู้ด้านไซเบอร์ ผู้บริหารมหาวิทยาลัยทั่วประเทศกว่า 600 คน

NCSA Partners with Ministry of Higher Education for Cybersecurity Knowledge Exchange with 600 University Management Representatives Nationwide

เมื่อวันที่ 4 สิงหาคม 2565 สกมช. ร่วมกับ กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (อว.) จัดการประชุมเชิงปฏิบัติการ เรื่อง การดำเนินกิจกรรมบนระบบเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา ครั้งที่ 41 (41st WUNCA) มีวัตถุประสงค์เพื่อนำเสนอและแลกเปลี่ยนความรู้ กับผู้บริหารเครือข่ายสารสนเทศของมหาวิทยาลัยทั่วประเทศกว่า 600 คน โดยมี พลอากาศตรี อมร ชมเชย เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และ รศ.สุรศักดิ์ สงวนพงษ์ กรรมการผู้ทรงคุณวุฒิ ใน กบส. จากมหาวิทยาลัยเกษตรศาสตร์ ร่วมเป็นวิทยากร ณ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี วิทยาเขตวังไกลกังวล ซึ่งเป็นการเสริมสร้างความเข้าใจ ตลอดจนสร้างความร่วมมือกับ UniNet ในประเด็น ดังต่อไปนี้

On August 4, 2022, the National Cyber Security Agency (NCSA), collaborating with the Office of the Ministry of Higher Education, Science, Research and Innovation (MHESI) organized the 41st Workshop on UniNet and Computer Application (41st WUNCA). The objective is to present and exchange knowledge with 600 university information network administrators across the country, including Air Vice Marshal Amorn Chomchoey, Secretary-General of the National Cyber Security Agency, and Assoc. Prof. Surasak Sanguanpong, Committee Managing the Office of the National Cybersecurity Committee from the Kasetsart University participated as a lecturer at the Rajamangala University of Technology Rattanakosin Wang Klai Kangwon Campus, which enhances understanding and creates cooperation with UniNet as follows:

- 1 เสริมสร้างพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์**
Strengthen and develop cyber security personnel.
- 2 สร้างเครือข่ายในการป้องกันภัยไซเบอร์**
Create a network to protect against cyber threats.
- 3 นำเสนอและรับฟังข้อปัญหาในการดำเนินการด้านต่าง ๆ ของงานสารสนเทศด้านการศึกษา**
Present and listen to problems in various aspects of educational information work.
- 4 ร่วมพิจารณาแนวทางในการแก้ปัญหา**
Participate in considering solutions to problems.

สัปดาห์วิชาการด้านความมั่นคงปลอดภัยไซเบอร์ Thailand National Cyber Week 2023

งานนิทรรศการสัปดาห์วิชาการด้านความมั่นคงปลอดภัยไซเบอร์ ปี 2566 (Thailand National Cyber Week 2023 – THNCW 2023) จัดขึ้นในวันที่ 17 – 18 ก.พ. 2566 ณ สามย่านมิตรทาวน์ กรุงเทพฯ มีวัตถุประสงค์ในการจัดเพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานภาครัฐ และภาคเอกชน สถาบันการศึกษา ตลอดจนประชาชนที่สนใจได้มีโอกาสแลกเปลี่ยนองค์ความรู้ และประสบการณ์ด้านเทคโนโลยีและการรักษาความมั่นคงปลอดภัยไซเบอร์รวมถึงส่งเสริมการสร้างความตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์

Thailand National Cyber Week 2023 was held on February 17 – 18, 2023 at Samyan Mitrtown, Bangkok. The exhibition was organized for infrastructure agencies, government agencies, private sectors, educational institutions, and general public to have the opportunity to exchange knowledge and experience, as well as to promote cybersecurity awareness.

มีผู้เข้าร่วมทั้งสิ้น | **15,152 คน**

A total of **15,152** people participated in this event.





การพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ Platform Online MOOC และ NCSA e – Learning Developing Cybersecurity Personnel, Platform Online MOOC, and NCSA e-Learning

เพื่อเป็นการยกระดับและเปิดโอกาสการเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ให้กับ ผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์และผู้ที่สนใจได้เข้าเรียนรู้ในทุกที่ ทุกเวลา โดยปัจจุบัน มีผู้เข้าใช้ระบบแล้วกว่า 5,000 คน ทาง www.national-cyber-academy.ncsa.or.th/open-elearning และ www.mooc.ncsa.or.th

The platform was developed to enhance cybersecurity capacity and provide opportunities to practitioners and those who are interested in this field to learn more from this platform, which is available anytime anywhere. Currently, the platform has already got more than 5,000 registrations.

ปัจจุบันมีผู้เข้าใช้ระบบแล้วกว่า

5,000 คน



เริ่มต้นการพัฒนากำลังคน
ด้านความมั่นคงปลอดภัยไซเบอร์

MOOC
cybersecurity learning platform

สำนักงานคณะกรรมการการอุดมศึกษา กระทรวงศึกษาธิการ (สอศ.)

ได้ฟรี ที่ NCSA MOOC

THINCA THAILAND NATIONAL CYBER ACADEMY MOOC.NCSA.OR.TH WWW.NCSA.OR.TH

BASIC CYBERSECURITY

เริ่มต้น!! การพัฒนาทักษะ ด้านความมั่นคงปลอดภัยไซเบอร์

เรียนฟรี!! มี CERTIFICATE

หลากหลายด้วย MODULE บทเรียน การเรียนรู้การรับมือภัยทางไซเบอร์ จะช่วยให้คุณได้ฝึกซ้อมแบบทดสอบ ผ่านการเรียนรู้และลงมือปฏิบัติจริง

เรียนจบพร้อมรับ ประกาศนียบัตร ด้านความมั่นคงปลอดภัยไซเบอร์ (CYBER SECURITY E-CERTIFICATE)

STEPS CONNECT NCSA MOOC

5 1. เข้าแพลตฟอร์ม NCSA MOOC <http://mooc.ncsa.or.th> หรือ QR CODE

2. กด SIGN UP เพื่อสมัครสมาชิก กรอกรายละเอียดส่วนตัว

3. ยืนยันตัวตนทางอีเมล

4. LOGIN เข้าสู่ระบบ NCSA MOOC

5. เรียนรู้วิชา BASIC CYBER SECURITY

หลักสูตร “อุนใจไซเบอร์” “Aunjai Cyber”



สกมช. ร่วมกับ บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน) ได้ร่วมมือกันดำเนินโครงการส่งเสริมการเรียนรู้หน้าที่พลเมืองดิจิทัล ด้วยสื่อการเรียนรู้ดิจิทัล หลักสูตร “อุนใจไซเบอร์” ในรูปแบบ e-Learning สำหรับครู บุคลากรทางการศึกษา นักเรียน และประชาชนทั่วประเทศ เพื่อให้สามารถเข้าถึงสื่อการเรียนรู้ดิจิทัลออนไลน์บนแพลตฟอร์ม LearnDi for Thai ในทุกที่ทุกเวลาและได้เริ่มมีการประชาสัมพันธ์ผ่านสื่อเพื่อให้สถานศึกษานำไปใช้ประโยชน์ต่อไป ทาง www.learndiaunjaicyber.ais.co.th

NCSA and Advanced Info Service Public Company Limited have collaborated to carry out a project to promote learning about digital citizenship duties. The “Aunjai Cyber” course is available in an e-learning format for teachers, educational personnel, students, and citizens across Thailand. It can be accessed through digital learning media on the LearnDi for Thai platform, allowing users to learn online anytime and anywhere. The course has been publicized through various media channels to encourage educational institutions to use it, and you can find more information about it at www.learndiaunjaicyber.ais.co.th.



คลังความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ Cyber Knowledge Center

สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้ดำเนินการรวบรวมองค์ความรู้และจัดทำในรูปแบบสื่อต่าง ๆ อย่างเป็นหมวดหมู่เพื่อให้ผู้ที่สนใจสามารถเข้าถึงและศึกษาเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างเป็นระบบ โดยได้จัดทำเป็นคลังความรู้ด้านไซเบอร์เพื่อเป็นช่องทางให้สามารถเข้าถึงได้อย่างสะดวกและรวดเร็ว ทาง <https://linktr.ee/thnca>

The Cyber Knowledge Center has collected knowledge and distributed it in various media formats. Categorized so that interested people can systematically search and learn about cybersecurity. It has been created as a cyber knowledge repository as a channel for convenient and quick.



เรียนฟรี! ได้ CERTIFICATE!

SCAN ME

LINK : [HTTPS://LINKTR.EE/THNCA](https://linktr.ee/thnca)

สแกนได้แล้ววันนี้
เรียนรู้ได้อย่างไร้ขีดจำกัด

สำนักวิชาการคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

CYBER KNOWLEDGE CENTER

"คลังความรู้ด้านไซเบอร์"

สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ส่งเสริมสังคมการเรียนรู้และเผยแพร่คลังความรู้ด้านไซเบอร์ เพื่อพัฒนาทักษะและการเรียนรู้ได้อย่างไร้ขีดจำกัด เข้าใจถึงความสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์

✓ CYBERSECURITY AWARENESS

- ความเข้าใจของ CYBERSECURITY
- ภัยคุกคามทางเทคโนโลยี
- นโยบาย ความมั่นคงปลอดภัยไซเบอร์
- กฎหมายที่เกี่ยวข้องกับ CYBERSECURITY
- แนวคิดความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework)
- นโยบายความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานในสังกัด (ส.อ. 2555 - 2570)
- นโยบายอื่น

✓ CYBERSECURITY SKILL

- CYBERSECURITY SKILL
- NCSA CYBERSECURITY KNOWLEDGE SHARING สัปดาห์ 2555 สัปดาห์ 2556 สัปดาห์ 2557
- CWS (Cybersecurity Working Space) สัปดาห์ 2555 สัปดาห์ 2556 สัปดาห์ 2557
- CWS (Cybersecurity Working Space) สัปดาห์ 2555 สัปดาห์ 2556 สัปดาห์ 2557

✓ NCSA MOOC CYBER-LEARNING

- BASIC CYBERSECURITY

✓ ศูนย์ไซเบอร์ AIS

- ศูนย์ไซเบอร์ AIS

CYBERSECURITY AWARENESS

CYBERSECURITY KNOWLEDGE SHARING

BASIC

NCSA MOOC CYBER-LEARNING

สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โทรศัพท์ 0-2502-7631 | อีเมล : academic@ncsa.or.th

การรับมือภัยคุกคามทางไซเบอร์

Cyber Incident Response

การแจ้งเตือนเหตุการณ์ภัยคุกคามให้กับหน่วยงานต่าง ๆ อย่างเป็นทางการ
Notification of official cyber threat incidents to various authorities



ภาพรวมภัยคุกคามทางไซเบอร์ที่ ThaiCERT ตรวจพบ และดำเนินการในปี 2566

Thailand's overview of cyber threats in 2023 has been actioned and detected by the Thailand Computer Emergency Response Team (ThaiCERT).



การตรวจสอบช่องโหว่และการทดสอบเจาะระบบ

Vulnerability Assessment (VA) and Penetration Testing (Pentest)



การปฏิบัติการเพื่อประเมินความเสี่ยง
ด้วยการทดสอบเจาะระบบ
เพื่อค้นหาจุดอ่อนในการเข้าถึงระบบต่าง ๆ
โดยใช้ผู้เชี่ยวชาญ

This operation involves a vulnerability assessment (VA) by conducting Pentest into a website to find vulnerable points in accessing the systems by experts



VA scans



Pentests

สนับสนุนการเผชิญเหตุภัยคุกคามทางไซเบอร์

Support for Incident Response



การตอบสนองต่อเหตุการณ์ Incident Response

การปฏิบัติการ เพื่อตรวจสอบหลักฐาน
ให้คำปรึกษาในการช่วยเหลือตอบสนอง และรับมือ
หน่วยงานที่ร้องขอและลงพื้นที่ เข้าช่วยเหลือ ตรวจสอบ
พิสูจน์หลักฐาน จัดทำแผนฟื้นฟูหลังการกำจัดเหตุ
ให้กับหน่วยงานที่ร้องขอและทำการติดตามหลังการ
ให้การช่วยเหลือ

This operation involves verifying evidence, consultation for incident response (IR) to cyber threats, preparation of recovery plans, and follow-up for the units that request support

ปฏิบัติการสนับสนุนทางไซเบอร์
Cyber Support Operations

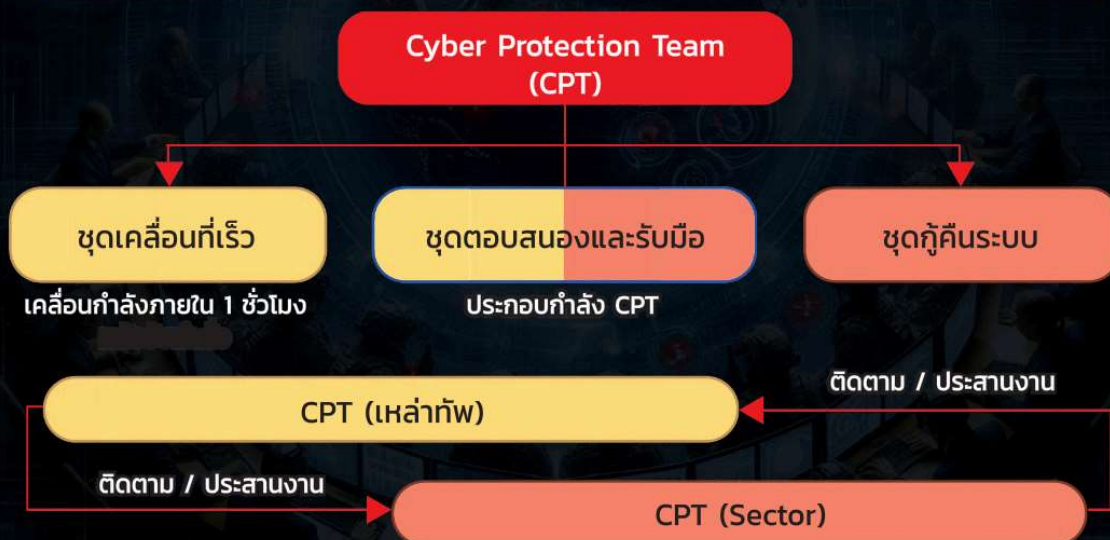


IR Operations

การสร้างทีมปฏิบัติการป้องกันภัยไซเบอร์ (Cyber Protection Team : CPT)

ตามมาตรา 19 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ให้รัฐมนตรีพิจารณาแต่งตั้งจากผู้มีความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้เป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ โดยระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่ฯ เป็นไปตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่องการกำหนดระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่ พ.ศ.2564 ซึ่งผู้ที่ได้รับแต่งตั้งเป็นเจ้าหน้าที่ฯ (Cyber Protection Team : CPT) จะต้องผ่านการอบรมด้านจริยธรรม การสืบสวนสอบสวน ด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) การบริหารจัดการเหตุภัยคุกคามไซเบอร์ (Incident Handling) และการพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics)

Section 19 of the Cybersecurity Act 2019 requires the Minister to consider appointing persons with knowledge and expertise in cybersecurity as officers under the Act. The qualifications of these officials are in accordance with the standards specified in the announcement of the National Cyber Security Committee on the level of knowledge and expertise in cyber security as specified in the Cybersecurity Act 2021, individuals selected for the Cyber Protection Team (CPT) must receive training in forensics, ethics, investigations, and digital security.



“สถิติประเภทยคุกคาม 1 ต.ค. 65 - 30 ก.ย. 66”

Thailand Cyber Threats Landscape from
October 1, 2022 to September 30, 2023

ประเภทยคุกคาม/เดือน Type/month	ต.ค. Oct	พ.ย. Nov	ธ.ค. Dec	ม.ค. Jan	ก.พ. Feb	มี.ค. Mar	เม.ย. Apr	พ.ค. May	มิ.ย. Jun	ก.ค. Jul	ส.ค. Aug	ก.ย. Sep	รวม Total
Application Compromise	0	0	0	0	0	0	0	0	0	0	1	0	1
Command and Control Server	0	0	0	1	0	0	0	0	0	2	1	0	4
Data Breach	4	3	0	3	2	7	0	0	3	6	8	14	50
Data Leak	0	0	0	0	0	3	33	3	0	4	60	0	103
DDoS	0	0	0	0	0	1	0	0	3	20	9	0	33
Fake Website	10	10	18	20	26	49	49	26	26	13	50	13	310
Finance Scam	0	0	0	0	11	8	12	19	17	15	24	5	111
Hacked Website (Defacement)	57	58	54	84	60	80	17	13	20	8	5	19	475
Hacked Website (Gambling)	26	8	35	77	40	73	31	111	42	8	2	69	522
Hacked Website (Phishing)	1	7	3	3	7	7	1	5	4	0	4	5	47
Hacked Website (Malware)	0	0	0	0	0	3	0	5	1	0	3	0	12
Mail Phishing	0	0	0	0	0	1	0	0	0	0	0	0	1
Malware	0	0	0	0	0	0	0	1	0	0	0	0	1
Privileged Account Compromise	0	0	0	0	0	0	1	0	1	1	6	3	12
Ransomware	5	1	0	1	6	2	3	1	4	1	5	1	30
Security Misconfiguration	0	0	0	0	0	0	0	1	0	1	0	0	2
Unauthorised access to information	1	2	0	0	0	1	0	3	0	0	0	0	7
Unauthorised modification of information	0	0	0	0	0	1	0	0	0	0	0	0	1
Vulnerabilities	1	3	1	1	1	4	6	5	10	45	6	1	84
Other	0	0	1	0	1	0	0	0	0	0	0	0	2
Total	105	92	112	190	154	240	153	193	131	124	184	130	1808



การสืบสวนและการขยายผล การป้องกัน แก้ไขปัญหาคูคัมภีร์ทางไซเบอร์

Support the Department of Special Investigation, the Royal Thai Police, and other law enforcement authorities in their investigations, preventative efforts, and efforts to resolve issues of cyber-related crime.

สนับสนุนการสืบสวนขยายผลและป้องกันแก้ไขปัญหาคูคัมภีร์ทางไซเบอร์ออนไลน์ ร่วมกับ สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ และหน่วยงานบังคับใช้กฎหมายอื่น

Investigation and expansion of arrest results, prevention, and resolution of cyber threats
Support the investigation and expansion of cybercrime prevention in cooperation with the Royal Thai Police, the Department of Special Investigation, and other law enforcement agencies.

APEC : เฝ้าระวังและตอบสนองภัยคุกคามทางไซเบอร์ในห้วงการจัดการประชุมผู้นำเขตเศรษฐกิจเอเปค และการประชุมที่เกี่ยวข้องในช่วงที่ประเทศไทยเป็นเจ้าภาพจัดการประชุมเอเปค พ.ศ. 2565 สกมช. จัดตั้ง ศูนย์ปฏิบัติการเฝ้าระวังและตอบสนองภัยคุกคามทางไซเบอร์ (ศปก.ฝตช.) เพื่อปฏิบัติการในการรักษาความปลอดภัยเกี่ยวกับภัยคุกคามทางไซเบอร์ รวมทั้งสนับสนุนการปฏิบัติให้กับหน่วยรักษาความปลอดภัยต่าง ๆ ตลอดห้วงของการประชุมผู้นำเขตเศรษฐกิจเอเปคและการประชุมที่เกี่ยวข้องในช่วงที่ประเทศไทยเป็นเจ้าภาพจัดการประชุมเอเปค พ.ศ. 2565 โดย สกมช. ปฏิบัติการเฝ้าระวัง และตอบสนองภัยคุกคามทางไซเบอร์ ตั้งแต่วันที่ 11-20 พฤศจิกายน 2565

Asia-Pacific Economic Cooperation (APEC) 2022 in Thailand : NCSA has been monitoring and responding to cyber threats at the APEC Economic Leaders' Meeting and related meetings during Thailand's hosting of APEC 2022. During Thailand's hosting of the APEC meeting from November 11 - 20, 2022, the National Cyber Security Agency (NCSA) established the Cyber Threat Surveillance and Response Operations Center to monitor and respond to cyber threats, including providing operational assistance to various security agencies throughout the APEC Economic Leaders' Meeting and related meetings.



กรณีข้อมูลประชาชนรั่วไหล Personal Data Leaked

เมื่อวันที่ 14 มีนาคม 2566 ตรวจพบการประกาศขายข้อมูลส่วนบุคคลของประชาชนในประเทศไทยที่หน้าเว็บไซต์สาธารณะซึ่งบุคคลทั่วไปสามารถเข้าถึงได้ และอ้างว่าข้อมูลดังกล่าว แยกได้จากหน่วยงานรัฐ ประกอบไปด้วยเลขบัตรประจำตัวประชาชน ชื่อ วันเดือนปีเกิด ที่อยู่ และหมายเลขโทรศัพท์ ทั้งนี้ โพสต์ดังกล่าวยังเปิดให้ดาวน์โหลดข้อมูลตัวอย่าง ในการนี้ เมื่อวันที่ 16 มีนาคม 2566 ได้ประสานงานกับกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) เพื่อร่วมกันตรวจสอบข้อมูลและความเกี่ยวข้องกับเหตุการณ์จากการร่วมกันตรวจสอบข้อมูล และร่วมปฏิบัติการจนนำไปสู่การจับกุมผู้กระทำความผิด เมื่อวันที่ 12 เมษายน 2566



On March 14, 2023, an announcement regarding the sale of personal information belonging to Thai citizens was found on a public website and claimed that information was obtained from government agencies. The announcement includes the ID card number, name, date of birth, address, and phone number. Furthermore, the post is still available for download. In this regard, on March 16, 2023, it was

coordinated with the Cyber Crime Investigation Bureau (CCIB) to collaboratively review data and linkages with the event that resulted in the perpetrator's arrest on May 12, 2023.

False Base Station ปลอมเสาสัญญาณโทรศัพท์ส่ง SMS หลอกลวง False base station (FBS) detection and SMS fraud

เนื่องจากปัจจุบันมีผู้เสียหายที่ตกเป็นเหยื่อจากขบวนการส่ง SMS ในลักษณะลิงก์ปลอม โดยอ้างชื่อเป็นหน่วยงานของรัฐและสถาบันการเงิน เพื่อหลอกลวงเงินผู้เสียหาย ซึ่งขบวนการดังกล่าว กำลังแพร่ระบาดเป็นอย่างมาก หากประชาชนหลงเชื่อและกดลิงก์ดังกล่าว จะติดตั้งแอปพลิเคชันควบคุมเครื่องระยะไกล โดยสามารถโอนเงินจากบัญชีธนาคารที่เครื่องโทรศัพท์ผ่าน Mobile Banking

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) เป็นหน่วยงานหลักในการดำเนินการสืบสวน โดยร่วมกับสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช.) ธนาคารแห่งประเทศไทย (ธปท.) ธนาคารกสิกรไทย สมาคมธนาคารไทย และ สกมช. ร่วมปฏิบัติการจนนำไปสู่การจับกุมผู้กระทำความผิด โดยเมื่อวันที่ 24 พฤษภาคม 2566 ได้จับกุมผู้เกี่ยวข้อง จำนวน 6 คน และของกลางเป็นอุปกรณ์ปลอมเสาสัญญาณสื่อสาร (False Base Station) จำนวน 5 เครื่อง รถยนต์ จำนวน 4 คัน สอบสวนได้ข้อเท็จจริงว่าผู้ไม่หวังดีจะใช้วิธีการนำอุปกรณ์ปลอมเสาสัญญาณสื่อสาร ซึ่งใช้รหัสที่เรียกว่าปลากะเบน ใส่ไว้ในรถยนต์และขับออกไปตามสถานที่ต่าง ๆ ในเขตกรุงเทพฯ และปริมณฑล เพื่อส่งสัญญาณไปยังโทรศัพท์มือถือที่อยู่บริเวณใกล้เคียง แล้วส่ง SMS ในลักษณะลิงก์ปลอม โดยอ้างชื่อเป็นสถาบันการเงิน



Currently, some victims receive fake SMS links claiming to be government agencies and financial institutions to deceive money from them. This process is becoming very widespread. If some victims believe and click on the link, they will install a remote-control application and transfer money from your bank account via Mobile Banking.



On 24 May 2023, the Cyber Crime Investigation Bureau (CCIB) was the lead agency conducting the investigation together with The National Broadcasting and Telecommunication Commission (NBTC), Bank of Thailand (BOT), Kasikornbank Public Company Limited (Kbank), Thai Bankers Association (TBA). and the National Cyber Security Agency (NCSA) cooperated in the operations, which resulted in the arrest of 6 perpetrators, 5 communication antenna counterfeiting devices, and 4 cars were arrested. The investigation revealed that malicious actors used a False Base Station method called “Stingray” to enter the car and drive to various places in Bangkok and surrounding areas to send a signal to nearby mobile phones and send fake SMS links using your name as a financial institution.

ลดความเสี่ยงภัยคุกคามทางไซเบอร์

Reducing Risk

ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

Codes of Practice and Standard Frameworks

สกมช. มีการ กำกับ ดูแล และติดตามการดำเนินการตามมาตรา 44 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยในเดือนสิงหาคม พ.ศ. 2566 ได้มีการให้หน่วยงานดังกล่าว จำนวนทั้งสิ้น 426 หน่วยงาน จัดส่งประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน มายัง สกมช. เพื่อเป็นการตรวจสอบการดำเนินการตามมาตรา 44 รวมทั้งช่วยให้หน่วยงานตระหนักถึงความสำคัญของการมีแนวทางในการป้องกัน รับมือ และลดความเสี่ยงต่อภัยคุกคามทางไซเบอร์ โดยประมวลแนวทางปฏิบัติฯ ประกอบด้วย

In accordance with Section 44 of the Cybersecurity Act 2019, the NCSA supervises and audits the activities of governmental agencies, regulator, and organizations of Critical Information Infrastructure. A formal correspondence dated August 25, 2023, requested the submission of cybersecurity codes of conduct by 426 agencies. These codes serve as guidelines for the identification and implementation of preventative, responsive, and risk-mitigation measures in the face of cyber threats. Listed below are the guidelines:

- 1 แนวทางปฏิบัติการ**
ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์
 Guidelines for cybersecurity auditing
- 2 แนวทางปฏิบัติการ**
ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
 Guidelines for cybersecurity risks assessment
- 3 แผนการรับมือภัยคุกคามทางไซเบอร์**
หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล
หน่วยงาน และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
 Cyber incident response plan for government agencies, regulator, and organization of Critical Information Infrastructure

การกำหนดมาตรฐานขั้นต่ำและการตรวจสอบมาตรฐานขั้นต่ำ และการติดตามการประเมินความเสี่ยง กำกับ ดูแล และติดตามการดำเนินการตามมาตรา 54 ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

Establishing the Organizations of Critical Information Infrastructure minimum standards and inspecting, following up on risk assessments, and supervising operations in accordance with Section 54

สกมช. ได้มีการจัดประชุมซักซ้อมความเข้าใจเกี่ยวกับการดำเนินการตามมาตรา 54 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ประจำปี 2566 เมื่อวันที่ 30 สิงหาคม 2566 ผ่านสื่ออิเล็กทรอนิกส์ โดยมี พลตรี ธีรวุฒิ วิทยากรณ์ รองเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นประธานในการประชุม โดยมีผู้เข้าร่วมประชุมจำนวนทั้งสิ้น 235 คน ซึ่งการประชุมครั้งนี้มีวัตถุประสงค์เพื่อให้หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบถึงแนวทางการดำเนินการตามมาตรา 53 การกำหนดมาตรฐานขั้นต่ำและการตรวจสอบมาตรฐานขั้นต่ำ และมาตรา 54 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

On Wednesday, August 30, 2023, the NCSA conducted a comprehension meeting via electronic media to discuss the implementation of Section 53 and 54 of the Cybersecurity Act 2019. The meeting was led by Major General Teerawut Wittayakarn, Deputy Secretary-General of the National Cyber Security Agency. A collective of 235 individuals was in attendance. The purpose of the meeting was to ensure that and regulators and organizations of Critical Information Infrastructure were aware of the operational guidelines outlined in Section 53, establishment of minimum standards and inspection, and Section 54, assessment of cybersecurity risks.

สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ NCSA

การประชุมซักซ้อมความเข้าใจเกี่ยวกับการดำเนินการตามมาตรา 54 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ประจำปี 2566

วันพุธที่ 30 สิงหาคม 2566 เวลา 14.00 – 16.00 น.
ผ่านสื่ออิเล็กทรอนิกส์

โดยมี พลตรี ธีรวุฒิ วิทยากรณ์ รอง สก.มช.
เป็นประธาน

วาระการประชุม

1. ประธานฯ กล่าวเปิดการประชุม
2. เรื่องพิธีกร
3. เรื่องวัตถุประสงค์ของการประชุม
4. เรื่องเนื้อหา (เรื่อง แนวทางปฏิบัติการประเมินความเสี่ยง และการตรวจสอบฯ ฉบับปรับปรุงล่าสุด 4 สิงหาคม 2566 - รายการประเมินความเสี่ยง (Checklist) ในการปฏิบัติงาน พ.ศ. 2566/กฎหมายที่เกี่ยวข้อง - รูปแบบ (Template) แบบฟอร์มเอกสารงานปฏิบัติการตามมาตรฐานฯ - รูปแบบ (Template) แบบฟอร์มเอกสารประเมินความเสี่ยง)
5. ประธานฯ กล่าวสรุปและปิดการประชุม



การฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ การจัดฝึก Thailand's National Cyber Exercise 2023 (NCX)

Cybersecurity Capabilities Staff Exercise Thailand's National Cyber Exercise 2023 (NCX)

สกมช. ได้จัดการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ Thailand's National Cyber Exercise 2023 เมื่อวันที่ 17 - 18 สิงหาคม 2566 เพื่อให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีความรู้ความเข้าใจเพิ่มมากขึ้นเกี่ยวกับการรับมือภัยคุกคามทางไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยมีหน่วยงานเข้าร่วมจำนวน 155 หน่วยงาน มีผู้เข้าร่วมจำนวนทั้งสิ้น 515 คน ผลการประเมินความพึงพอใจต่อการจัดการฝึก ร้อยละ 92.09 อยู่ในเกณฑ์การประเมิน **ระดับดีมาก**

Thailand's National Cyber Exercise 2023 (NCX) was conducted for government agencies, regulators, and organizations of Critical Information Infrastructure from August 17-18, 2023. In accordance with the Cyber Security Act 2019, the Exercise intends to increase knowledge and comprehension of cyber threats. 515 participants and 155 agencies are participating. The Exercise received an outstanding rating of 92.09 percent on the satisfaction evaluation scale, as determined by the criteria.





การประชุมเพื่อพิจารณาสั่งการในสถานการณ์จำลองกรณีเกิดเหตุภัยคุกคามทางไซเบอร์ในระดับร้ายแรงของคณะกรรมการรับมือภัยคุกคามทางไซเบอร์ในระดับร้ายแรง (คสร.)

Critical Incident Response Committee (CIRC)

ด้วยคณะกรรมการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ (กกม.) ได้มอบอำนาจให้คณะกรรมการคณะหนึ่ง เรียกว่า คณะกรรมการรับมือภัยคุกคามทางไซเบอร์ในระดับร้ายแรง (ครร.) ประกอบด้วย (1) รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ (2) ผู้บัญชาการทหารสูงสุด เป็นกรรมการ (3) ผู้บัญชาการตำรวจแห่งชาติ เป็นกรรมการ (4) ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นกรรมการ (5) เลขาธิการสภาความมั่นคงแห่งชาติ เป็นกรรมการ และ (6) เลขาธิการคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นกรรมการและเลขานุการ โดยที่ ครร. มีหน้าที่และอำนาจในการดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ให้มีความรวดเร็วและทันทั่วถึง เพื่อป้องกันหรือลดความเสียหายที่อาจจะเกิดขึ้นจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

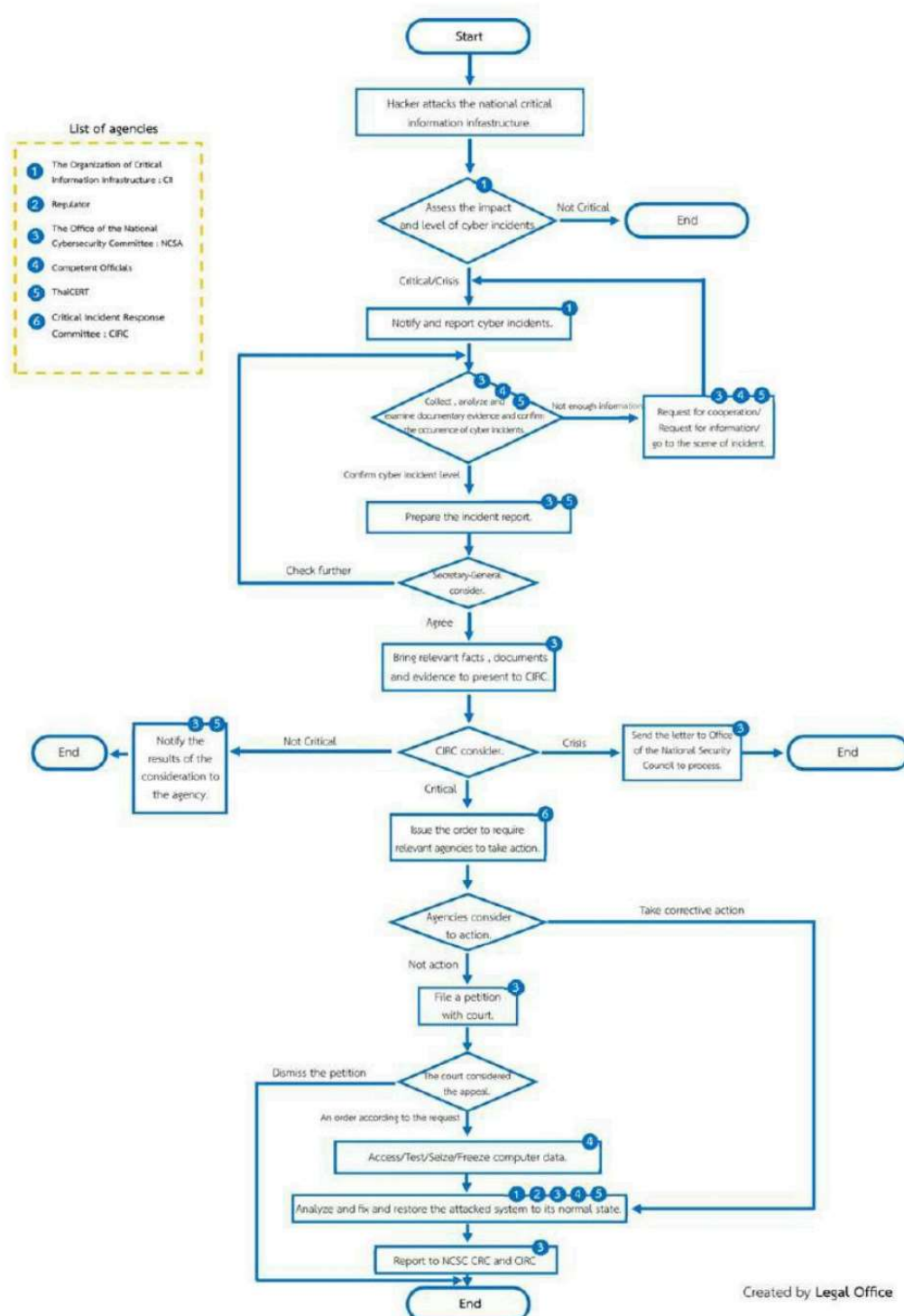
ดังนั้น เพื่อเป็นการซักซ้อมความเข้าใจเกี่ยวกับหน้าที่และอำนาจตามกฎหมาย รวมถึงการพิจารณาสั่งการกรณีเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง สกมช. ได้นำเหตุภัยคุกคามทางไซเบอร์จากการจัดฝึกและทดสอบแผนเผชิญเหตุฯ (Thailand's National Cyber Exercise 2023 : NCX2023) มาเป็นสถานการณ์จำลองประกอบการพิจารณาสั่งการของ ครร. เมื่อวันที่ 25 กันยายน 2566 โดยมี นายประเสริฐ จันทรวงทอง รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่ประธานในการประชุม ซึ่งการซักซ้อมดังกล่าว ยังเป็นการบูรณาการความร่วมมือในการเตรียมความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรงระหว่าง ครร. สกมช. และหน่วยงานอื่น ๆ ที่เกี่ยวข้องอีกด้วย

Cybersecurity Regulating Committee (CRC) granting authority to establish the Critical Incident Response Committee (CIRC), consist of 1) Minister of Digital Economy and Society (Chairman); 2) Chief of Defence Forces, Royal Thai Armed Forces Headquarters (Member); 3) Commissioner-General, Royal Thai Police (Member); 4) Permanent Secretary of the Ministry of Digital Economy and Society (Member); 5) Secretary-General of the National Security Council (Member); and 6) Secretary-General of the National Cyber Security Agency (Member and Secretary). The CTRC - C is entrusted with the responsibility and authority to supervise and respond to cyber threats at a critical level in a timely and effective manner in order to prevent or mitigate potential damage caused by cyber threats.



The NCSA has included cyber threat incidents in its simulation scenario for the CTRC - C meeting on Monday, September 25, 2023, to help understand legal obligations and authorities, especially when dealing with cyber threats at a critical level. The scenario was created as part of Thailand's National Cyber Exercise 2023 (NCX2023). Mr. Prasert Jantararungthong, Minister of Digital Economy and Society, presided over the proceedings. Chairing the meeting rehearsal involves coordinating collaboration between the NCSA and other relevant agencies in order to prepare for addressing cyber threats at a critical level.

แผนผังแสดงกระบวนการดำเนินงานของ คสร.
กรณีเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง
Chart Showing the Operational Process of the Critical
Incident Response Committee for Critical Cyber Threats



Sectoral CERT ด้านสาธารณสุข

Sectoral CERT in Public Health

ความก้าวหน้าของการดำเนินโครงการสนับสนุนการจัดตั้ง Sectoral CERT ด้านสาธารณสุข

Progress of the project to support the establishment of Sectoral CERT in public health

สกมช. ได้จัดทำโครงการสนับสนุนการจัดตั้ง Sectoral CERT ด้านสาธารณสุข และโครงการศูนย์เฝ้าระวัง ป้องกันและรับมือ ภัยคุกคามทางด้านไซเบอร์สำหรับโรงพยาบาลรัฐ ระยะที่ 1 (Healthcare Cyber Defence Center) เพื่อเสริมสร้างความมั่นคงปลอดภัยของระบบสารสนเทศทางด้านสาธารณสุขในการช่วยเฝ้าระวัง ตรวจสอบ รับมือ ป้องกัน แจ้งเตือน บรรเทาสถานการณ์จากภัยคุกคามใหม่ ๆ ที่เกิดขึ้น และจัดการกับช่องโหว่ รวมทั้งตรวจสอบและประมวลผลหลังเกิดเหตุขององค์กรในแต่ละภาคส่วนของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความปลอดภัยตลอด 24/7 มีการแจ้งเตือนล่วงหน้าสำหรับภัยคุกคามที่มีความเสี่ยงสูง โดยให้บริการด้านการตรวจสอบและการแก้ไขปัญหาด้านความมั่นคงปลอดภัยของระบบสารสนเทศภายในกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุข ในการรับมือต่อภัยคุกคามเหล่านั้นได้ ปัจจุบันติดตั้งเรียบร้อยแล้ว จำนวน 15 แห่ง ดังนี้

NCSA has initiated a project to assist in setting up a Sectoral CERT in public health and the Healthcare Cyber Defence Centre for public hospitals, Phase 1. The center's goal is to enhance the security of public health information systems by monitoring, detecting, addressing, preventing, warning about, mitigating new threats, and managing vulnerabilities. It involves inspecting and processing organizations within each Critical Information Infrastructure (CII) sector to maintain security around the clock and alert about high-risk threats. It offers inspection and troubleshooting services to ensure the security of internal information system for CII. The Sectoral CERT is now comprised of 15 established locations.



โครงการสนับสนุนการจัดตั้ง Sectoral CERT ด้านสาธารณสุข

Project to support the establishment of Sectoral CERT in public health



1 โรงพยาบาลลำปาง
Lampang Hospital



2 โรงพยาบาลพุทธชินราช
(จังหวัดพิษณุโลก)
Buddhachinnarat
Hospital (Phitsanulok
Province)



3 โรงพยาบาลกำแพงเพชร
Kamphaeng Phet Hospital



4 โรงพยาบาลสระบุรี
Saraburi Hospital



5 โรงพยาบาลขอนแก่น
Khon Kaen Hospital



6 โรงพยาบาลอุดรธานี
Udon Thani Hospital



7 โรงพยาบาลมหาสารคาม
Maharat Nakhon Ratchasima
Hospital



8 โรงพยาบาลวารินชำราบ
(จังหวัดอุบลราชธานี)
Warin Chamrap Hospital
(Ubon Ratchathani Province)



9 Data Center กรมการแพทย์
Data Center, Department
of Medical Services



10 ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข
Information and Communication Technology Center, Office of the Permanent Secretary,
Ministry of Public Health



โครงการศูนย์เฝ้าระวัง ป้องกัน และรับมือภัยคุกคามทางด้านไซเบอร์ สำหรับโรงพยาบาลรัฐ ระยะที่ 1 (Healthcare Cyber Defense Center, Phase 1)



1 โรงพยาบาลราชบุรี
Ratchaburi Hospital



2 โรงพยาบาลชลบุรี
Chonburi Hospital



3 โรงพยาบาลมหาราช
นครศรีธรรมราช
Maharat Nakhon Si
Thammarat Hospital



4 โรงพยาบาลหาดใหญ่
(จังหวัดสงขลา)
Hat Yai Hospital
(Songkhla Province)



5 สถาบันประสาทวิทยา
(จังหวัดกรุงเทพมหานคร)
Neurological Institute
(Bangkok Province)

ทั้งนี้ สกมช. ได้ดำเนินการเพื่อพัฒนา
ศักยภาพบุคลากรด้านความมั่นคง
ปลอดภัยไซเบอร์ให้กับหน่วยงานทาง
ด้านสาธารณสุข จำนวน 3 หลักสูตร ดังนี้

1

กิจกรรมอบรมหลักสูตร (Course Outline) เพื่อถ่ายทอดความรู้
และประสบการณ์ด้านการบริหาร Security Operation Center (SOC)

กิจกรรมอบรมหลักสูตร “การบริหารจัดการ การใช้งานระบบ Cortex XDR
และระบบ Cortex XSOAR ในรูปแบบการฝึกงาน (On The Job Training)”

2

3

กิจกรรมอบรมหลักสูตร “การถ่ายทอดความรู้และประสบการณ์ด้านการบริหาร
Security Operation Center (SOC) ในรูปแบบการฝึกงาน (On The Job Training)”



โดย สกมช. ได้จัดพิธีลงนามบันทึกความเข้าใจ
ว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัย
ทางไซเบอร์ ระหว่าง สกมช. กับ สำนักงานปลัด
กระทรวงสาธารณสุข เมื่อวันที่ 19 กรกฎาคม 2566
เป็นที่เรียบร้อยแล้ว โดยความร่วมมือดังกล่าว เป็นความร่วมมือ
ในการสนับสนุนการจัดตั้งศูนย์ประสานการรักษา
ความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงาน
โครงสร้างพื้นฐานสำคัญทางสารสนเทศ ด้านสาธารณสุข
สกมช. ได้สนับสนุนให้สำนักงานปลัดกระทรวงสาธารณสุข
ในฐานะหน่วยงานควบคุมหรือกำกับดูแล เป็น Sectoral
CERT ด้านสาธารณสุข ซึ่งสำนักงานปลัดกระทรวง
สาธารณสุขได้ดำเนินการจัดตั้งศูนย์ประสานการรักษา
ความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงาน
โครงสร้างพื้นฐานสำคัญทางสารสนเทศ ด้านสาธารณสุข
(Health CIRT) เรียบร้อยแล้ว โดยสำนักงานปลัดกระทรวง
สาธารณสุขได้มอบหมายให้ศูนย์เทคโนโลยีสารสนเทศ
และการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข
เป็นหน่วยงานรับผิดชอบ

A memorandum of understanding on cyber
security cooperation was signed between the NCSA
and the Permanent Secretary's Office, Ministry of
Public Health, during a signing ceremony organized
by NCSA on July 19, 2023. The goal of this
collaboration is to create a computer system security
coordination centre for organization of critical
information infrastructure. NCSA has provided
support to the Office of the Permanent Secretary
of the Ministry of Public Health as a regulator,
serving as a Sectoral CERT in public health. The
Office of the Permanent Secretary of the Ministry
of Public Health has set up Computer Incident
Response Team for organization of critical
information infrastructure in public health (Health
CIRT), and it is now operational. The Information
and Communication Technology Centre, under
the Office of the Permanent Secretary of the
Ministry of Public Health, has been designated as the
responsible agency.

การพัฒนาแพลตฟอร์มการแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ 10 หน่วยงาน

Development of Malware Information Sharing Platform for ten agencies

สกมช. ดำเนินการนำร่อง 10 หน่วยงาน เปิดใช้แพลตฟอร์มแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ ร่วมพัฒนาแหล่งข่าวกรองที่น่าเชื่อถือระดับประเทศ วันจันทร์ที่ 9 ตุลาคม 2566 สกมช. แถลงข่าวความสำเร็จ “โครงการพัฒนาแพลตฟอร์มการแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์” โดยมีหน่วยงานเข้าร่วมโครงการทั้งหมด 10 หน่วยงาน ได้แก่

Monday, October 9, 2023 marked the beginning of a pilot programme between NCSA and ten agencies to implement a cyber threat information exchange platform with the objective of establishing a reliable source of national-level intelligence. The success of the Malware “Information Sharing Platform Development Project” in which ten agencies participated including the Ministry of Public Health CIRT (HealthCIRT), Ministry of Transport CERT (MOT-CERT), Ministry of Energy CERT (EnergyCERT), Thailand Telecommunications Sector CERT (TTC-CERT), National Intelligence Agency, Thailand Banking Sector CERT (TB-CERT), GovCERT, RTARF, PEA and EGAT was officially announced at a press conference hosted by the NCSA.

- | | | | |
|----|---|--------------------------|---|
| 1 | กระทรวงสาธารณสุข (HealthCIRT) | กระทรวงคมนาคม (MOT-CERT) | 2 |
| 3 | กระทรวงพลังงาน (EnergyCERT) | สำนักข่าวกรองแห่งชาติ | 4 |
| 5 | ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) | | |
| 6 | ศูนย์ประสานงานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT) | | |
| 7 | สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (GovCERT) | | |
| 8 | กองบัญชาการกองทัพอากาศ | การไฟฟ้าส่วนภูมิภาค | 9 |
| 10 | การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย | | |



และมีการเชื่อมต่อระบบกันแบบอัตโนมัติ เพื่อแลกเปลี่ยนข้อมูลให้สามารถเชื่อมโยงข้อมูลภัยคุกคามทางไซเบอร์เชิงเทคนิคต่าง ๆ ไม่ว่าจะเป็นตัวบ่งชี้ที่ระบุถึงกลุ่ม Hacker ต่าง ๆ ที่คาดว่าจะหรือน่าจะมีการโจมตีในประเทศไทยเป็นต้น เพื่อเป็นการแชร์ข้อมูลระหว่างกันแบบเชิงรุก ที่เรียกว่า Proactive Protection ซึ่งมีแผนจะขยายต่อให้ครอบคลุมทั้งประเทศ แนวคิดการออกแบบระบบจะมุ่งเน้นให้รองรับการขยายการเชื่อมต่อในอนาคตได้ (Scalable) และการควบคุมและคัดกรอง (Filtering) ข้อมูลภัยคุกคามทางไซเบอร์ รวมถึงกลไกการแลกเปลี่ยนข้อมูลที่จะสร้างให้เกิดความเชื่อมั่น (Trust) ในการแลกเปลี่ยนข้อมูลระหว่าง สกมช. และหน่วยงานอื่น ๆ ซึ่งจะนำหลักสากลที่เรียกว่า Traffic Light Protocol มาควบคุมการแลกเปลี่ยนข้อมูลระหว่างกัน



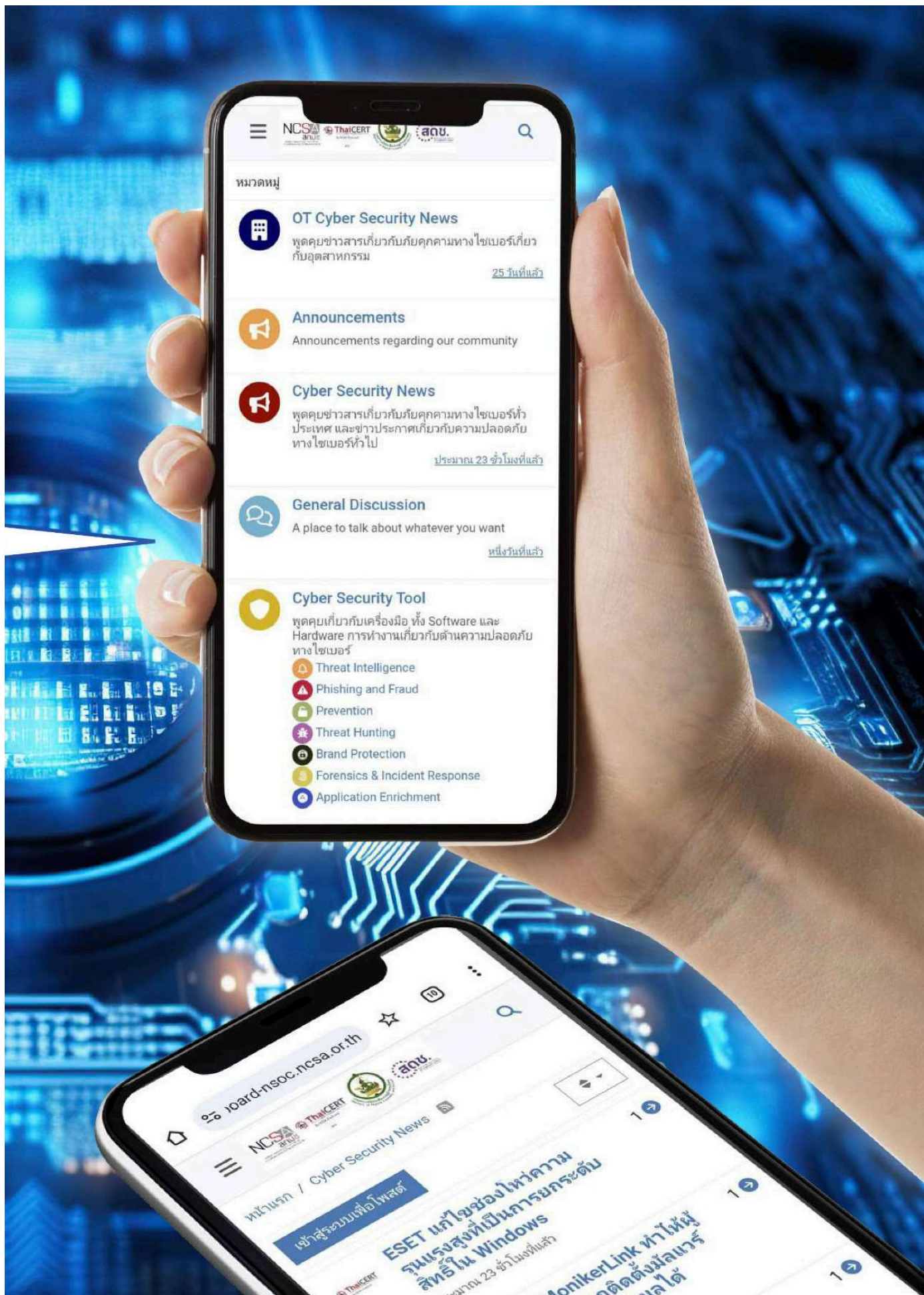
By means of an automated information exchange process, the systems link a variety of technical cyber threat data, including indicators of criminal groups that are probable targets of Thailand. By proactively exchanging information, a programme known as Proactive Protection intends to eventually encompass the entire nation. The primary objectives of the system design concept are scalability to accommodate future connectivity expansion and the filtration and control of cyber threat data. It contains a mechanism for the exchange of information that will foster confidence in the NCSA's interactions with other agencies. The Traffic Light Protocol, an international standard designed to govern the exchange of information between entities, will be implemented as a result.

NCSA แจ้งข่าวภัยคุกคามไซเบอร์

Cybersecurity NEWS
แจ้งข่าวภัยคุกคามไซเบอร์
แพลตฟอร์มบริการสาธารณะ
เพื่อแชร์ข่าวสาร
เกี่ยวกับภัยคุกคามทางไซเบอร์
จากที่มาหลายแหล่งทั่วโลก
เพื่อให้เกิดความตระหนักรู้
ถึงภัยคุกคามทางไซเบอร์
ที่เกิดขึ้น



<https://webboard-nsoc.ncsa.or.th/>



Cyber Range ระบบปฏิบัติการจำลอง Cyber Range Simulation Operating System

Cyber Range Platform เป็นผลผลิตของโครงการพัฒนาเทคโนโลยีดิจิทัลแบบบูรณาการเพื่อยกระดับความสามารถบุคลากรในการป้องกันรับมือภัยคุกคามทางไซเบอร์ พัฒนาศักยภาพขึ้นเพื่อเป็นระบบฝึกซ้อมในการรับมือภัยคุกคามทางไซเบอร์ รับผิดชอบโดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ วัตถุประสงค์หลักของแพลตฟอร์มดังกล่าว เพื่อมุ่งเน้นการเพิ่มขีดความสามารถและศักยภาพของบุคลากรด้านไซเบอร์ขององค์กรได้อย่างหลากหลาย เช่น การวิเคราะห์ภัยคุกคามทางไซเบอร์ การทดสอบเจาะระบบเพื่อประโยชน์ในการตรวจสอบความมั่นคงปลอดภัยของระบบรักษาความปลอดภัย เป็นต้น นอกจากนี้ยังช่วยส่งเสริมขีดความสามารถในการปฏิบัติงานด้านการเฝ้าติดตาม เฝ้าระวัง และตรวจสอบวิเคราะห์สถานการณ์ด้านภัยคุกคามทางไซเบอร์อีกด้วย

โดยได้ดำเนินการจัดอบรม

จำนวน **14** รุ่น | ทั้งหมด **152** คน

The Cyber Range Platform is the outcome of a comprehensive digital technology development initiative that aimed to improve the capacity of personnel to defend against cyber threats. Overseen by ThaiCERT, it functions as a training system for dealing with such threats. In order to evaluate security systems, the platform's principal objective is to enhance the capabilities of the organization's cyber personnel in domains such as penetration testing and cyber threat analysis. Moreover, it contributes to the enhancement of operational capabilities in the realm of cyber threat scenario surveillance and analysis.

The Cyber Range Platform can be incorporated with sectoral SOC's at the technical, tactical, and strategic levels for the purpose of training with cyber security operations centres of various organizations of critical information infrastructure. Therefore, it is a vital component that fulfils the requirements of cyber personnel development, guaranteeing preparedness to efficiently counter cyber threats.



กิจกรรมแข่งขันทักษะทางไซเบอร์ Thailand Cyber Top Talent 2023
Cyber Skills Competition Activity "Thailand Cyber Top Talent 2023"

การแข่งขันรอบคัดเลือก เมื่อวันที่ 16 กันยายน 2566 ผู้เข้าร่วมการแข่งขันทั้งหมด 831 ทีม แบ่งออกเป็น 3 ระดับ ได้แก่ ระดับมัธยมศึกษา ระดับอุดมศึกษา และระดับประชาชนทั่วไป รวมทั้ง 3 ระดับ ผู้สมัครเข้าร่วม จำนวน 2,323 คน

ทั่วทุกภูมิภาคประเทศไทย ได้ทีมแข่งรอบสุดท้าย จำนวน 30 ทีม



The qualifying round was held on September 16, 2023. A total of 831 teams participated in the competition, divided into 3 levels: secondary school level, university student level and general public level. In total there were 3 levels, with 2,323 applicants participating in all regions of Thailand, resulting in 30 teams competing in the final round.



กิจกรรมแข่งขันทักษะทางไซเบอร์ สำหรับผู้หญิง และเพศสภาพเป็นหญิง
"Women Thailand Cyber Top Talent 2022"
 Cyber Skills Competition Activity "Women Thailand Cyber Top Talent 2022"

การแข่งขันรอบคัดเลือกเมื่อวันอาทิตย์ที่ 11 ธันวาคม 2565 ผ่านระบบออนไลน์ มีผู้เข้าแข่งขัน แบ่งออกเป็น 2 ระดับ รวม 132 ทีม ได้แก่ ระดับนักเรียน นิสิต นักศึกษา จำนวน 83 ทีม และระดับประชาชนทั่วไป จำนวน 49 ทีม รอบชิงชนะเลิศ วันอาทิตย์ที่ 18 ธันวาคม 2565 ซึ่งมีทีมผ่านเข้าแข่งขัน จำนวน 30 ทีม ณ Novotel Bangkok on Siam Square เพื่อชิงเงินรางวัลรวมกว่า 200,000 บาท พร้อมเหรียญที่ระลึก โล่รางวัล และเกียรติบัตร

The qualifying round was held on Sunday, December 11, 2022 via the online system. The participants were divided into 2 levels, totaling 132 teams, including 83 teams at the student level and 49 teams at the general public level. The finals was on Sunday December 18, 2022, with 30 teams passing through to compete at Novotel Bangkok on Siam Square to win a total prize money of more than 200,000 baht, along with commemorative medals, plaques and certificates.



การแข่งขัน Cyber SEA Game 2022

Cyber SEA Game 2022 Competition

สกมช. ดำเนินการจัดการแข่งขัน Thailand Cyber Top Talent 2022 ในรอบคัดเลือกซึ่งเป็นการแข่ง Capture The Flag ในรูปแบบ Jeopardy เป็นปีที่ 2 เพื่อคัดเลือกผู้แข่งขันที่ได้รางวัลชนะเลิศให้เป็นตัวแทนประเทศไทยในการเข้าร่วมแข่งขัน Cyber SEA Game 2022 ระหว่างวันที่ 10-11 พฤศจิกายน 2565 ณ ประเทศไทย ซึ่งมีชาติสมาชิกอาเซียนเข้าร่วมแข่งขันทั้งหมด 10 ชาติ รวม 40 คน รางวัลชนะเลิศ ได้แก่ ประเทศเวียดนาม อันดับที่ 2 ได้แก่ ประเทศสิงคโปร์ และรางวัลอันดับที่ 3 ได้แก่ ประเทศไทย



The NCSA has organized the qualifying round of the Thailand Cyber Top Talent 2022 competition. This round takes the form of a Capture the Flag competition in the Jeopardy format, and the winners will be qualified to represent Thailand in the Cyber SEA Game 2022 competition which was held in Thailand from November 10 - 11, 2022. Forty individuals representing ten ASEAN Member States participated in the competition. Thailand was awarded the second runner-up, while Vietnam was announced as winner of the outstanding award. Singapore, in that order, is awarded the first runner-up

กฎหมายลำดับรองที่สำคัญสำหรับบังคับใช้กับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศ

กฎหมายลำดับรองที่สำคัญสำหรับบังคับใช้กับหน่วยงานของรัฐ หน่วยงานควบคุม
หรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

1 ประกาศ กมช. เรื่อง
**การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มี
ภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้าง
พื้นฐานสำคัญทางสารสนเทศฯ**
Notification of NCSC Re: Criteria and Characteristics
for Designating Agencies with Certain Missions or
Services as Organizations of Critical Information
Infrastructure and the Regulation Assignment

2 ประกาศ กมช. เรื่อง
**ลักษณะ หน้าที่และความรับผิดชอบของ
ศูนย์ประสานการรักษาความมั่นคงปลอดภัย
ระบบคอมพิวเตอร์ฯ**
Notification of NCSC Re: Characteristics, Duties,
and Responsibilities of the Coordinating Center
of Computer Emergency Response Team
for Organizations of Critical Information
Infrastructure and Related Missions and Services

3 ประกาศ กมช. เรื่อง
**ลักษณะภัยคุกคามทางไซเบอร์ มาตรการ
ป้องกัน รับมือ ประเมินปราบปราม
และระงับภัยคุกคามทางไซเบอร์แต่ละระดับฯ**
Notification of NCSC Re: Characteristics and
Measures for Prevention, Response, Assessment,
Eradication, and Containment of Cybersecurity
Incidents at Each Level

4 ประกาศ กมช. เรื่อง
**การกำหนดระดับความรู้ความชำนาญ
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่**
Notification of NCSC Re: Cybersecurity
Knowledge and Expertise Requirements for
Competent Official Appointment

5 ประกาศ กกม. เรื่อง
**ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
สำหรับหน่วยงานของรัฐและหน่วยงาน
โครงสร้างพื้นฐานสำคัญทางสารสนเทศฯ**
Notification of the CRC Re: Codes of Practice and
Standard Frameworks for Government Agencies and
Organizations of Critical Information Infrastructure

6 ประกาศ กมช. เรื่อง
**การจัดตั้ง หน้าที่และอำนาจของศูนย์ประสาน
การรักษาความมั่นคงปลอดภัย
ระบบคอมพิวเตอร์แห่งชาติฯ**
Notification of NCSC Re: Establishment, Duties,
and Powers of Thailand Computer Emergency
Response Team (ThaiCERT)

7 ประกาศ กกม. เรื่อง
**หลักเกณฑ์และวิธีการรายงาน
ภัยคุกคามทางไซเบอร์ฯ**
Notification of the CRC Re: Cyber Incident Reporting
Criteria and Procedure

8 ระเบียบ กกม. ว่าด้วย
การมอบอำนาจให้ปฏิบัติราชการแทนฯ
Regulation of the CRC Re: Assignment of Powers
to Perform Tasks on behalf of the CRC

9 ประกาศ กมช. เรื่อง
**นโยบายและแผนปฏิบัติการว่าด้วยการรักษา
ความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)**
Notification of NCSC Re: Cybersecurity Policy and
Action Plan 2022 - 2027

10 ประกาศ สกมช. เรื่อง
**หลักเกณฑ์และอัตราในการเรียกเก็บค่าธรรมเนียม
ค่าบำรุง ค่าตอบแทน หรือค่าบริการฯ**
Notification of NCSA Re: Criteria and Rates of Fees,
Maintenance Fees, Compensation Fees, and Service
Fees for Operations

11 (ร่าง) ประกาศ กมช. เรื่อง
**มาตรฐานการกำหนดคุณลักษณะ
ความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูล
หรือระบบสารสนเทศฯ**
(Draft) Notification of NCSC Re: the Standards for
Defining the Attributes of Cybersecurity for Data or
Information Systems

12 (ร่าง) ประกาศ กมช. เรื่อง
**มาตรฐานขั้นต่ำของข้อมูลหรือ
ระบบสารสนเทศฯ**
(Draft) Notification of NCSC Re: the Minimum
Standards for Data or Information Systems

13 (ร่าง) ประกาศ กมช. เรื่อง
**มาตรฐานและแนวทางส่งเสริมพัฒนา
ระบบการให้บริการเกี่ยวกับการรักษา
ความมั่นคงปลอดภัยไซเบอร์ฯ**
(Draft) Notification of NCSC Re: the Standards and
Guidelines for Promoting the Development of Cybersecurity
Service Systems

14 (ร่าง) ประกาศ กมช. เรื่อง
**มาตรการและแนวทางในการยกระดับทักษะ
ความรู้และความเชี่ยวชาญในการรักษา
ความมั่นคงปลอดภัยไซเบอร์ฯ**
(Draft) Notification of NCSC Re: Measures and
guidelines to enhance the knowledge and expertise
in Maintaining Cybersecurity

การขับเคลื่อนนโยบายและแผนปฏิบัติการ ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

Implementation of Cybersecurity Policy and Action Plan to maintain cybersecurity

สกมช. จัดทำกิจกรรมเผยแพร่และสร้างความเข้าใจในนโยบาย และกฎระเบียบที่เกี่ยวข้องด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ภายใต้โครงการขับเคลื่อนแผนยุทธศาสตร์ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อสนับสนุนการเผยแพร่ประชาสัมพันธ์ สร้างความรู้ ความเข้าใจในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ แก่ทุกภาคส่วนโดยทั่วถึงทั้งภาครัฐ ภาคเอกชน และภาควิชาการ เพื่อสร้างความตระหนักถึงภัยคุกคามทางไซเบอร์ และความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์

NCSA organizes and participates in events that increase knowledge and comprehension of cybersecurity policies and regulations. This endeavour is a component of a larger undertaking that seeks to execute a strategic blueprint with the goals of bolstering cybersecurity, advancing public relations, and disseminating information in the field of cybersecurity throughout diverse academic, private, and public spheres. The objective is to enhance consciousness regarding cyber threats and the criticality of upholding cybersecurity measures to ensure the secure and advantageous operation of digital technologies and cyber activities. Furthermore, the objective is to foster cooperation in the field of cybersecurity by means of diverse partnership models involving both individuals and organizations. This collaborative effort will provide direction for policy and action plan, culminating in concrete execution that optimizes the effectiveness and productivity of cybersecurity maintenance.



การดำเนินงานการขับเคลื่อนนโยบายและแผนปฏิบัติการว่าด้วย การรักษาความมั่นคงปลอดภัยไซเบอร์ ประจำปีงบประมาณ พ.ศ. 2566

Performance Results for Implementing the Cybersecurity Policy and Action Plan to Maintain Cybersecurity in the Fiscal Year 2023 are as Follows:

โดยมีผลการดำเนินงานการขับเคลื่อนนโยบายและแผนปฏิบัติการว่าด้วย
การรักษาความมั่นคงปลอดภัยไซเบอร์ ประจำปีงบประมาณ พ.ศ. 2566 ดังนี้

1

การผลักดันหน่วยงานเป้าหมาย

Ensured alignment of the target agency's plans

ดำเนินการจัดทำแผนงาน/โครงการ/กิจกรรมด้านไซเบอร์ให้สอดคล้องกับยุทธศาสตร์ กลยุทธ์ ตัวชี้วัด
ของนโยบายและแผนปฏิบัติการฯ และบรรจุลงในแผนปฏิบัติการของหน่วยงาน รวมเป็นจำนวน 68 หน่วยงาน

2

การขับเคลื่อนนโยบายและแผนฯ ไปสู่การปฏิบัติ ในระดับนโยบาย Implementing the Policy and Action Plan at policy level

- 2.1 ทหาหรือแนวทางการขับเคลื่อนนโยบายและแผนฯ ร่วมกับกรมการทหาร
- 2.2 ประชุมชี้แจงแนวทางการขับเคลื่อนนโยบายและแผนฯ
- 2.3 ประชุมหารือแนวทางการขับเคลื่อนนโยบายและแผนฯ ร่วมกับหน่วยงาน Regulator
- 2.4 แลกผลผลการขับเคลื่อนนโยบายและแผนฯ เพื่อการแก้ไขปัญหาความมั่นคง
- 2.5 ประชุมชี้แจงส่วนราชการ เรื่อง แนวทางการขับเคลื่อนนโยบายและแผนฯ ไปสู่การปฏิบัติ
- 2.6 ประชุมพิจารณาการจัดทำโครงการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อขับเคลื่อน
นโยบายและแผนฯ และสอดคล้องกับการดำเนินงานตามยุทธศาสตร์ชาติ

3

การขับเคลื่อนนโยบายและแผนฯ ไปสู่การปฏิบัติ ในระดับปฏิบัติการ Implementing the Policy and Action Plan at Operational Level

- 3.1 จัดกิจกรรมสัมมนาเพื่อสร้างความรู้ ความเข้าใจในนโยบายและแผนฯ ใน 3 ภูมิภาค
มีผู้เข้าร่วมทั้ง Onsite และ Online มากกว่า 30,000 คน
 - ครั้งที่ 1 การประชุมประชาคมไซเบอร์แห่งชาติ ณ โรงแรมอัศวิน แกรนด์ คอนเวนชั่น กรุงเทพมหานคร
 - ครั้งที่ 2 ณ โรงแรม เดอะ ไพน์ จังหวัดสงขลา
 - ครั้งที่ 3 ณ โรงแรมแสน จังหวัดเชียงราย
- 3.2 ผลักดันให้เกิดการจัดทำแผนการขับเคลื่อนโดยประกอบด้วยโครงการจำนวน 663 โครงการ
พร้อมทั้งให้หน่วยงานนำโครงการดังกล่าวไปบรรจุลงในแผนปฏิบัติการฯ ของหน่วยงาน
 - จัดประชุมชี้แจงและติดตามการจัดทำข้อมูลโครงการ/กิจกรรม ให้กับกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เมื่อวันที่ 7 กันยายน 2566
 - จัดประชุมชี้แจงและติดตามข้อมูลโครงการ/กิจกรรม ให้กับหน่วยงานที่ยังไม่มีโครงการในการดำเนินการ เมื่อวันที่ 27 กันยายน 2566

พันธมิตรและหน่วยงานดำเนินงานที่สำคัญ Partners of NCSA

ภายในประเทศและต่างประเทศ (กรอบทวิภาคีและพหุภาคี)

Bilateral and Multilateral Collaboration

บันทึกความร่วมมือ



Pentest



การป้องกันภัยคุกคามทางไซเบอร์



ด้านการเงิน



การจัดตั้ง Sectoral CERT ด้านสาธารณสุข



สนับสนุนหน่วยงาน



ความร่วมมือระหว่างประเทศ (พหุภาคี)



ความร่วมมือระหว่างประเทศ (ทวิภาคี)



02

PART : 3

การรักษาความมั่นคง ปลอดภัยไซเบอร์ อย่างยั่งยืน

Sustainable Cybersecurity

มุ่งเป้าสู่การสร้างสังคมดิจิทัล โดยสมบูรณ์แบบที่มีการสร้างเกราะป้องกันและภูมิคุ้มกันให้กับทุกภาคส่วนของประเทศ สกมช. ซึ่งที่มีประสิทธิภาพสูงในทุก ๆ ด้าน เพื่อเป็นแกนกลางในการขับเคลื่อนงานต่าง ๆ ผ่านหน่วยงาน Regulator หน่วยงาน CII หน่วยงานของรัฐ และชุมชน เพื่อมุ่งหวังให้ประชาชนคนไทยปลอดภัยจากภัยคุกคามทางไซเบอร์

The goal is to build a perfect digital society with a defense and immunity system for all sectors in Thailand. The National Cyber Security Agency (NCSA), with its highly effective personnel and operations, will serve as a hub to drive various initiatives through the Regulators, organizations of Critical Information Infrastructure, government agencies, including the community. The ultimate goal is to ensure that Thai citizens are safe from cyber threats.

ทิศทางยกระดับความมั่นคงปลอดภัยไซเบอร์

Directions for Enhancing Cybersecurity

การกำหนดกรอบแนวทางการพัฒนาหน่วยงานเป้าหมาย เพื่อยกระดับความมั่นคงปลอดภัยไซเบอร์

The establishment of a framework to enhance capacity of target agencies

(The inspection report is shown below.)

ตามที่ นายกรัฐมนตรีได้แถลงนโยบายต่อรัฐสภาเมื่อวันที่ 11 กันยายน 2566 ในการเป็นรัฐบาลที่ขับเคลื่อนเศรษฐกิจ การเมือง สังคม ด้วยข้อมูลที่แม่นยำ และทันสมัย พร้อมทั้งให้ความสำคัญกับการป้องกันภัยคุกคามข้ามชาติ และการเพิ่มความปลอดภัยทางไซเบอร์นั้น เพื่อตอบสนองต่อนโยบายดังกล่าว สกมช. จึงได้ดำเนินการจัดประชุมเร่งรัดแผนการดำเนินงานตามพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ประจำปีงบประมาณ พ.ศ. 2567 เมื่อวันที่ 22 พฤศจิกายน 2566 ณ ห้องประชุม NT Auditorium บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) กรุงเทพฯ โดยมี นายประเสริฐ จันทรรวงทอง รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจ และสังคม ในฐานะประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัย ไซเบอร์ (กกม.) โดยเน้นย้ำให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดำเนินการ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565 - 2570 ซึ่งส่งผลต่อการยกระดับความมั่นคงปลอดภัยไซเบอร์ ในภาพรวมของประเทศได้อย่างสัมฤทธิ์ผล



The Prime Minister delivered his policy to the Paliament on September 11, 2023, aiming declaring that the Government will drive the economy, politics, and society with precise and up to date information. It also emphasizes the importance of preventing transnational threats and strengthening cybersecurity. In the light of this policy, Mr. Prasert Jantararungtong, Minister of Digital Economy and Society, Chairman of the Cybersecurity Regulating Committee (CRC), chaired the meeting which was arranged by the NCSA on Wednesday, November 22, 2023, from 1:30 p.m. to 3:30 p.m. at the NT Auditorium, National Telecoms Public Company Limited, Bangkok, to expedite the implementation plan in accordance with the Cybersecurity Act 2019 for the fiscal year 2024. He underscored that government agencies, regulator and organization of critical information infrastructure implementing the Cybersecurity Act 2019 and the Cybersecurity Policy and Action Plan 2022 - 2027 to effectively enhance country's overall cybersecurity.

ตารางสรุปกำหนดการดำเนินการของหน่วยงานภาครัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในห้วงปีงบประมาณ พ.ศ. ๒๕๖๗

นโยบายบริหารจัดการฯ สำหรับ Gov, CII / มาตรการ พสบ.ไซเบอร์	Gov*	Reg	CII	D	E	F	G	H	I	J	K	L	M	N	O	P
นโยบายบริหารจัดการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับ Gov, CII	✓		✓													
ม.๔๓ ดำเนินการตามนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ฯ	✓	✓	✓													
ม.๔๔ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ	✓	✓	✓													
ม.๔๕ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ	✓	✓	✓													
ม.๔๖ แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการไปยัง สกมช.	✓	✓	✓													
ม.๔๗ แจ้งรายชื่อและข้อมูลการติดต่อของเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ ไปยัง สกมช., Reg		✓	✓													
ม.๔๘ Reg ตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของ CII		✓	✓													
ม.๔๙ จัดให้มีการประเมินความเสี่ยงฯ จัดให้มีการตรวจสอบฯ ปีละครั้ง ส่งสรุปผลรายงาน สกมช.			✓													
ม.๕๐ มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์ ตามมาตรฐานที่ Reg กำหนด และเข้าร่วมทดสอบสถานะความพร้อมรับมือภัยคุกคามฯ ที่ สกมช. จัดขึ้น		✓	✓													
ม.๕๑ รายงานเหตุภัยคุกคามฯ ไปยัง สกมช.และ Reg และปฏิบัติตาม พสบ. (รับมือภัยคุกคามฯ)		✓	✓													
ม.๕๒ ตรวจสอบ ประเมิน ป้องกัน รับมือ ลดความเสี่ยง และแจ้งไปยัง สกมช. และ Reg ของตน	✓	✓	✓													

Gov* หมายถึง หน่วยงานของรัฐที่ไม่ได้เป็นหน่วยงาน CII

✓ หมายถึง ไม่ได้เป็นหน่วยงานปฏิบัติโดยตรง แต่เกี่ยวข้องกับการปฏิบัติ

ตารางสีแดง หมายถึง ช่วงเวลาที่หน่วยงานสามารถบูรณาการ



การขยายความร่วมมือระหว่างประเทศ Expanding International Cooperation

สกมช. ผสานความร่วมมือกับ International Telecommunication Union (ITU) ในการจัดส่งวิทยากรเข้าร่วมการเสวนาในเรื่อง Best Practices for Critical Information Infrastructure Protection ร่วมกับผู้แทนจากหน่วยงานด้านไซเบอร์ของประเทศในภูมิภาคเอเชีย ยุโรป ภายใต้การประชุม ITU Europe & Asia-Pacific Interregional CyberDrill ณ เมืองลิมาโซ สาธารณรัฐไซปรัส ระหว่างวันที่ 27 พฤศจิกายน ถึง 1 ธันวาคม 2566 โดย ITU ได้มีความสนใจขยายความร่วมมือด้านการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับนานาชาติ และมีแผนในการดำเนินกิจกรรมในด้านดังกล่าวกับ สกมช. ในปี พ.ศ. 2567 นอกจากนี้ยังได้รับความสนใจเป็นอย่างดีจากผู้แทนประเทศที่ได้รับเชิญจาก ITU เข้าร่วมการประชุม เช่น ราชอาณาจักรภูฏาน และสาธารณรัฐประชาชนบังกลาเทศ ในการแลกเปลี่ยนข้อมูลและมุมมองต่อการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งมีความสนใจร่วมมือกับ ThaiCERT เพื่อพัฒนาและเสริมสร้างขีดความสามารถการตอบสนองต่อภัยคุกคามทางไซเบอร์ และแนวทางการปฏิบัติงานร่วมกันระหว่างศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์



NCSA and the International Telecommunication Union (ITU) collaborated by sending speakers to the ITU Europe & Asia-Pacific Interregional CyberDrill, which was held in Limassol, Republic of Cyprus, from November 27 to December 1, 2023. During this event, speakers shared insights on Best Practices for Critical Information Infrastructure Protection and representatives from cyber agencies in Asian and European countries participated. International cooperation in advancing the field of cybersecurity is an area that the ITU is eager to expand. In 2024, NCSA also intends to conduct activities in this particular domain. Furthermore, representatives of nations (including the People's Republic of Bangladesh and the Kingdom of Bhutan) that were invited by the ITU to participate in the conference have expressed interest in exchanging information and perspectives regarding the protection of critical information infrastructure. Furthermore, they show enthusiasm for establishing a collaborative partnership with ThaiCERT to enhance and refine their capacity to address cyber threats, as well as to develop operational guidelines for joint CERT operations.

สถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

Institute of National Cyber Security

สกมช. ตระหนักถึงการพัฒนากำลังคนและสมรรถนะทางด้านความมั่นคงปลอดภัยไซเบอร์ที่พัฒนาไปอย่างรวดเร็วประกอบกับการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์และองค์ความรู้ด้านไซเบอร์ ยังอยู่ในวงจำกัด ทำให้ภัยคุกคามด้านไซเบอร์ ต่อหน่วยงานและประชาชนทวีความรุนแรงมากขึ้นและส่งผลกระทบในด้านเศรษฐกิจ สังคม และความมั่นคงของประเทศ

ดังนั้น สกมช. จึงมีแนวความคิดในการจัดตั้งสถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อให้เป็นหน่วยงานหลักในการสร้างบุคลากรที่มีความรู้ความเข้าใจและมีประสิทธิภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทั้งจากภายในและภายนอกประเทศ เพื่อยกระดับสมรรถนะของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์และประชาชน ให้เป็นเกิดกระบวนการเรียนรู้ที่สร้างความเชื่อมั่นในการใช้เทคโนโลยี ดิจิทัล ในการขับเคลื่อนเศรษฐกิจและสังคม การเสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัย ไซเบอร์ รวมถึงการสร้างความรู้ความตระหนักด้านสถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ในรูปแบบกิจกรรมที่หลากหลาย ร่วมกันเพื่อให้มีการดำเนินการเชิงปฏิบัติการที่มีลักษณะบูรณาการและเป็นปัจจุบัน ที่เหมาะสมกับกลุ่มเป้าหมาย ได้อย่างยั่งยืน ทั้งในประเทศ และในระดับสากล

NCSA recognizes the rapid growth of cybersecurity competencies and the workforce, as well as the limited number of cybersecurity personnel who have been granted specialized training and have cybersecurity knowledge. However, this also means that the severity of cyber threats against citizens and agencies is increasing, which has far-reaching consequences for the economy, society, and national security.

It is crucial to develop competent and productive personnel capable of preventing, responding to, and mitigating the risks posed by domestic and international cyber threats. This will elevate the proficiency of both cyber security personnel and the general public. The process should help promote confidence in utilizing digital technology to advance society and the economy. Furthermore, it is vital to enhance comprehension of cyber security and generate awareness regarding potential cyber threats across diverse endeavours. A comprehensive understanding and perception will enable individuals to execute integrated and ongoing tasks. The content delivered should serve as appropriate for the intended audience and maintain its relevance over a prolonged period.

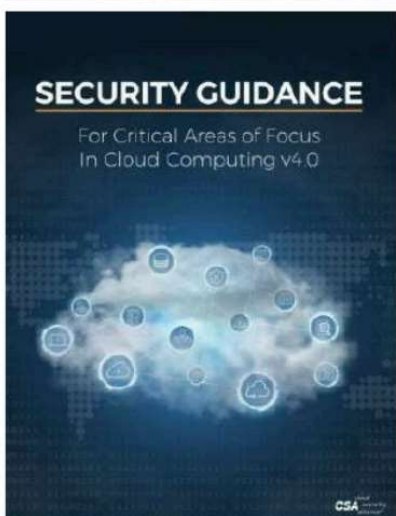


การจัดทำมาตรฐานความมั่นคงปลอดภัย CLOUD Computing สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

The Establishment of Cloud Computing Security Standards for the Organization of Critical Information Infrastructure Agency

ตามที่นายกรัฐมนตรีได้แถลงนโยบายต่อรัฐสภา เมื่อวันที่ 11 กันยายน 2566 ในการเป็นรัฐบาลที่ขับเคลื่อนเศรษฐกิจ การเมือง สังคม และสิ่งแวดล้อม ด้วยข้อมูลที่แม่นยำและทันสมัย ปรับปรุงการทำงานของภาครัฐให้เป็นรัฐบาลดิจิทัล ทำให้ประชาชนได้รับความสะดวกมากยิ่งขึ้น มุ่งเน้นการบริหารประเทศในรูปแบบบูรณาการการทำงานระหว่างหน่วยงานให้ตอบสนองเป้าหมายการพัฒนาประเทศระยะยาว นำไปสู่การกำหนดนโยบาย Go Cloud First โดยรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ที่ต้องการวางกรอบการขยายตลาดเชิงโครงสร้างพื้นฐานให้แก่ทั้งภาครัฐและเอกชน โดยเน้นการสร้าง Public Cloud และ Private Cloud ที่มีมาตรฐานในการดูแลข้อมูลภาครัฐนั้น สกมช. ได้ตอบสนองต่อนโยบายดังกล่าวโดยได้เริ่มดำเนินการพิจารณาร่างมาตรฐานความมั่นคงปลอดภัยคลาวด์คอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยได้เชิญผู้เชี่ยวชาญจากหลายภาคส่วนร่วมกันพิจารณาศึกษามาตรฐานที่เกี่ยวข้องจากหน่วยงานชั้นนำ เช่น International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST) และ Cloud Security Alliance (CSA) เป็นต้น เพื่อนำไปกำหนดมาตรฐานที่เหมาะสมและสอดคล้องกับนโยบายและบริบทของประเทศไทย ซึ่งจะเป็นปัจจัยสนับสนุนที่สำคัญให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการใช้คลาวด์คอมพิวเตอร์ได้อย่างมีประสิทธิภาพ และเป็นไปตามนโยบายดังกล่าว

On September 11, 2023, the Prime Minister delivered his policy to the Parliament, declaring that the Government will drive the economy, politics, and society. with precise and up-to-date information. The proposal also called for the transformation of public sector operations into a digital government, increased accessibility to public services, and an integrated national administration that aligns with long-term national development objectives. The consequence is the Minister of Digital Economy and Society's Go Cloud First Policy. With standards for maintaining government data, this policy seeks to provide a framework for expanding cloud infrastructure to the private and public sectors, with an emphasis on the creation of public and private clouds. NCSA has initiated the development of preliminary cloud computing security standards for organizations of Critical Information Infrastructure with regard to the policy. This is being achieved through the invitation of industry experts to evaluate and analyse relevant standards established by reputable organisations including the National Institute of Standards and Technology (NIST), International Organisation for Standardisation (ISO), and Cloud Security Alliance (CSA). The objective is to establish standards that are suitable and in line with the policy and context of Thailand that will serve as an important foundation of support for the Organisation of Critical Information Infrastructure as it implements cloud computing in a policy-compliant and efficient manner.



NIST
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

PUBLICATIONS

NIST SP 800-144
Guidelines on Security and Privacy in Public Cloud Computing

Author(s)
Nigel E. Jenner (BAK), Tim Grance (NIST)

Date Published: December 2012

Abstract
Cloud computing can and does mean different things to different people. The common characteristics most interpretations share are on-demand scalability of highly available and reliable pooled computing resources, secure access to networked services from nearly anywhere, and displacement of data and services from inside to outside the organization. While aspects of these characteristics have been realized to a certain extent, cloud computing remains a work in progress. This publication provides an overview of the security and privacy challenges pertinent to public cloud computing and points out considerations organizations should take when outsourcing data, applications, and infrastructure to a public cloud environment.

Keywords
Cloud Computing; Computer Security and Privacy; Information Technology Outsourcing

Control Families
Planning

DOCUMENTATION

Publication:
CF <https://nvlpubs.nist.gov/nistpubs/SP800-144.pdf>
Downloadable

Supplemental Material:
SP 800-144 SP800-144a
Final Report

Document History:
12/20/12: SP 800-144 (Final)

TOPICS

Security and Privacy
Authentication, Authorization, Accountability

Technology
Cloud & Virtualization

Laws and Regulations
Federal Information Security Modernization Act (FISMA)
Circular A-130

การรับรองหลักสูตรการรักษา ความมั่นคงปลอดภัยไซเบอร์ จากสถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน)

สกมช. ได้ดำเนินการพัฒนาหลักสูตรพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์ (ระดับพื้นฐาน) (Cybersecurity Foundation Course) เพื่อเป็นการพัฒนาศักยภาพ และเพิ่มสมรรถนะทักษะบุคลากรทางด้านความมั่นคงปลอดภัยไซเบอร์ โดยได้รับการพิจารณาความสอดคล้องของหลักสูตรตามมาตรฐานอาชีพและคุณวุฒิวิชาชีพ จากสถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน) ดังนี้

สอดคล้อง
ตามมาตรฐานอาชีพ
และคุณวุฒิวิชาชีพ สาขาวิชาชีพ
อุตสาหกรรมดิจิทัลอาชีพ
นักบริหารจัดการ
ความมั่นคงปลอดภัย
ระบบเครือข่ายและคอมพิวเตอร์
ระดับ

5-6

**หลักสูตรพื้นฐานด้านความมั่นคง
ปลอดภัยไซเบอร์ (ระดับพื้นฐาน)
(Cybersecurity Foundation Course)**

**หลักสูตรพื้นฐานด้านความมั่นคง
ปลอดภัยไซเบอร์ (ระดับพื้นฐาน)
(Cybersecurity Foundation Course)**

สอดคล้อง
ตามมาตรฐานอาชีพ
และคุณวุฒิวิชาชีพ สาขาวิชาชีพ
อุตสาหกรรมดิจิทัลอาชีพ
นักบริหารจัดการ
ความมั่นคงปลอดภัย
ระบบสารสนเทศ
ระดับ

4-6





ที่ สคช. ๒๖๑๕/๒๕๖๕

สถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน)
๑๑๗๗ อาคารเฟิร์ล แบงก์ค็อก ชั้น ๑๔
ถนนพหลโยธิน แขวงพญาไท เขตพญาไท
กรุงเทพมหานคร ๑๐๔๐๐

๒๓ พฤศจิกายน ๒๕๖๕

เรื่อง แจ้งผลการพิจารณาความสอดคล้องของหลักสูตร

เรียน สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

อ้างถึง หนังสือสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หนังสือเลขที่ สกมช

๐๗๐๐/๑๐๘๒ ลงวันที่ ๑๘ ตุลาคม ๒๕๖๕

สิ่งที่ส่งมาด้วย แบบฟอร์มลงนามยินยอมให้ประชาสัมพันธ์หลักสูตรฝึกอบรมฯ

ตามที่ สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้ขอรับการพิจารณาความสอดคล้องของหลักสูตร ตามมาตรฐานอาชีพและมาตรฐานสมรรถนะตามหนังสืออ้างถึง นั้น สถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน) พิจารณาแล้วเห็นว่าหลักสูตรของท่าน มีความสอดคล้องตามมาตรฐานอาชีพและคุณวุฒิวิชาชีพ ดังรายละเอียดต่อไปนี้

๑) หลักสูตรพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์ (ระดับพื้นฐาน) (Cybersecurity Foundation Course) สอดคล้องตามมาตรฐานอาชีพและคุณวุฒิวิชาชีพ สาขาวิชาชีพอุตสาหกรรมดิจิทัล อาชีพนักบริหารจัดการความมั่นคงความปลอดภัยระบบเครือข่ายและคอมพิวเตอร์ ระดับ ๕ - ๖

๒) หลักสูตรพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์ (ระดับพื้นฐาน) (Cybersecurity Foundation Course) สอดคล้องตามมาตรฐานอาชีพและคุณวุฒิวิชาชีพ สาขาวิชาชีพอุตสาหกรรมดิจิทัล อาชีพนักจัดการความมั่นคงความปลอดภัยระบบสารสนเทศ ระดับ ๔ - ๖

ดังนั้น สถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน) จึงขอแจ้งผลการพิจารณาตามรายละเอียดข้างต้น และขอความกรุณาท่าน กรอกแบบฟอร์มให้ความยินยอมประชาสัมพันธ์หลักสูตรฝึกอบรมที่มีความสอดคล้องตามมาตรฐานอาชีพและมาตรฐานสมรรถนะ บนหน้าเว็บไซต์ของสถาบันฯ ที่ URL: <https://www.tpqi.go.th/> เพื่อเป็นประโยชน์ต่อสาธารณะ หรือประชาชนที่มีความสนใจเข้ารับการฝึกอบรมเตรียมความพร้อมก่อนเข้ารับการประเมินสมรรถนะ หรือพัฒนาตนเองให้มีองค์ความรู้ความเชี่ยวชาญตามมาตรฐานอาชีพและมาตรฐานสมรรถนะต่อไป (รายละเอียดดังสิ่งที่ส่งมาด้วย ๑) และโปรดส่งแบบฟอร์มลงนามยินยอมให้ประชาสัมพันธ์หลักสูตรฝึกอบรมฯ กลับมาทาง E-mail : bussakorn.k@tpqi.go.th ทั้งนี้ สามารถติดต่อประสานงานได้ที่ คุณบุษกร เสนีย์โยธิน นักวิชาการมาตรฐานวิชาชีพ

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

(นายสุรพล พลอยสุข)

ผู้อำนวยการสถาบันคุณวุฒิวิชาชีพ

๒๓ พ.ย. ๒๕๖๕ ๑๖:๒๕:๔๘ Non-PKI Server Sign
Signature Code : 1P5j0-Gc3K4-15gUG-lpNvT

สถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน)

สำนักขับเคลื่อนภารกิจพิเศษ

คุณบุษกร เสนีย์โยธิน

โทร. ๐๖๓-๓๖๐ ๘๔๔๔

ไปรษณีย์อิเล็กทรอนิกส์ saraban@tpqi.go.th

การขับเคลื่อนนโยบายและแผนปฏิบัติการ ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

Implementation of Cybersecurity Policy and Action Plan

การขยายผล ผลักดัน เสริมสร้าง ความร่วมมือ ในการขับเคลื่อนนโยบายและแผน 4 ไปสู่การปฏิบัติ

Implementing the Cybersecurity Policy and Action Plan by enhancing outcomes, promoting collaboration, and bolstering efforts

การติดตามประเมินผลการดำเนินงานภายใต้นโยบายและแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ ดำเนินการติดตามประเมินผลการดำเนินงานภายใต้นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ.2565 – 2570) สำหรับหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และ หน่วยงานของรัฐ เพื่อทราบความคืบหน้าและประเมินผลการปฏิบัติตามนโยบายและแผนปฏิบัติการฯ (พ.ศ.2565 – 2570) นำไปสู่การปฏิบัติอย่างเป็นรูปธรรมและมีประสิทธิภาพ โดยมีแนวทางการดำเนินงาน ดังนี้

In accordance with the Cybersecurity Policy and Action Plan 2022 – 2027, government agencies, regulators, and organizations of critical information infrastructure, will be evaluated and monitored in a manner that facilitates productive and concrete implementation. The guidelines for operation are as follows:



- | | | |
|-----------|--|---|
| ขั้นที่ 1 | การประชุมชี้แจงและกบถวน
นโยบายและแผนปฏิบัติการฯ
(พ.ศ. 2565 – 2570) | Set up a compliance meeting |
| ขั้นที่ 2 | การประชุมติดตามการดำเนินงาน
โครงการของหน่วยงานที่เกี่ยวข้อง
ประจำปี พ.ศ. 2567 ภายใต้นโยบาย
และแผนปฏิบัติการฯ (พ.ศ. 2565 – 2570) | Follow up on the progress
of ongoing projects
for the fiscal year 2024 |
| ขั้นที่ 3 | การติดตามและประเมินผลการดำเนินงาน
โครงการประจำปี พ.ศ. 2567
ภายใต้นโยบายและแผนปฏิบัติการฯ
(พ.ศ. 2565 – 2570) | Monitor and conduct
project performance
assessments
for the fiscal year 2024 |
| ขั้นที่ 4 | การจัดทำรายงานผลการดำเนินงาน
ภายใต้นโยบายและแผนปฏิบัติการฯ
(พ.ศ. 2565 – 2570) | Prepare a compliance
report |

Thailand International Cyber Week

การพัฒนาสัปดาห์วิชาการในระดับสากล

Development of an Academic Week on a Global Scale

สกมช. ได้ส่งเสริมการสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยกำหนดจัดนิทรรศการสัปดาห์วิชาการด้านความมั่นคงปลอดภัยไซเบอร์ (Thailand International Cyber Week) ขึ้นเป็นประจำทุกปี

ในปี 2567 กำหนดจัดงาน Cybersec Asia & Thailand International Cyber Week 2024 ในวันที่ 31 มกราคม - 1 กุมภาพันธ์ 2567 ซึ่งเป็นงานนิทรรศการสัปดาห์วิชาการด้านความมั่นคงปลอดภัยไซเบอร์ระดับสากล เป็นการสร้างโอกาสการเข้าถึงข้อมูลข่าวสาร สามารถเลือกใช้เทคโนโลยีและนวัตกรรมได้อย่างเหมาะสมในการรักษาความมั่นคงปลอดภัยไซเบอร์

Cybersecurity awareness has been promoted by the NCSA. It is planned that Thailand International Cyber Week will be held annually.

CyberSec Asia & Thailand International Cyber Week 2024 took place from January 31 to February 1, 2024. The event was a global cybersecurity academic expo aimed at offering attendees insights into the latest advancements in cybersecurity technology.

CYBERSEC ASIA X **THAILAND INTERNATIONAL CYBER WEEK 2024** **NCSA สกมช.**

CYBERSEC ASIA | SHIELD YOUR CORE

งานแสดงเทคโนโลยีและนวัตกรรมด้านความมั่นคงปลอดภัยทางไซเบอร์ขั้นสูง
สำหรับประเทศไทย และ ภูมิภาคเอเชียแปซิฟิก

31 มกราคม - 1 กุมภาพันธ์ 2567 **09:30 - 17:00 น.**
Plenary Hall 1-2 ศูนย์การประชุมแห่งชาติสิริกิติ์ กรุงเทพฯ

คุณกำลังเผชิญกับความท้าทายเหล่านี้หรือไม่?

- การแทรกแซงความมั่นคงปลอดภัยบนโลกไซเบอร์
- ช่องโหว่บนคลาวด์
- การละเมิดข้อมูล
- การพยายามก่อกวนหน้าอาชญากรรมไซเบอร์ด้วยการป้องกันทางนิติวิทยาศาสตร์ขั้นสูง

ค้นหาคำตอบของทุกปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ พร้อมปรึกษาปัญหาจากผู้เชี่ยวชาญจากแบรนด์ชั้นนำกว่า 50 บริษัท จาก 12 ประเทศทั่วโลก อาทิ ประเทศไทย สิงคโปร์ เกาหลีใต้ ออสเตรเลีย บรูไน จีน มาเลเซีย สหรัฐอาหรับเอมิเรตส์ อินเดีย สหราชอาณาจักรอิสราเอล เป็นต้น

ร่วมอัปเดตข่าวสารข้อมูลทางนวัตกรรมจาก 60 วิทยากรรับเชิญจาก 15 ประเทศ

พร้อมแล้วที่จะเปิดประตูต้อนรับผู้เข้าร่วมงานทุกท่านสู่ Cyber Security Community ของเรา

ลงทะเบียนที่นี่!

แล้วพบกันที่งาน Cybersec Asia 2024 x Thailand International Cyber Week 2024
จัดโดย บริษัท วัชรวิญญู เอเชีย แปซิฟิก และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

จัดโดย **วัชรวิญญู เอเชีย แปซิฟิก** สนับสนุนโดย **JAARBEURE** **CYBERSEC ASIA** **NCSA** **สกมช.**

WWW.CYBERSEC-ASIA.NET

เครือข่ายงานวิจัย Research Network

ขับเคลื่อนเครือข่ายวิจัยและสนับสนุน

การทำวิจัยด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

Facilitate a Research Network and Promote Cybersecurity Research

ศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์ให้ความสำคัญกับการพัฒนาความร่วมมือด้านการวิจัยและพัฒนานวัตกรรม องค์ความรู้ใหม่ ๆ ให้มีการต่อยอดและใช้ประโยชน์จากผลงานวิชาการ และส่งเสริมการพัฒนาบุคลากรสายวิชาการ สายสนับสนุนวิชาการ นักศึกษาและนักวิจัย ให้มีการแลกเปลี่ยนองค์ความรู้และใช้งานทรัพยากรทางวิชาการร่วมกันผ่านกลไกความร่วมมือด้านวิจัยและพัฒนานวัตกรรมและองค์ความรู้ที่เกี่ยวข้องกับการศึกษาวิจัยด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ จึงได้มีการจัดกิจกรรมพัฒนาเครือข่ายการวิจัยด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อกำหนดกรอบการวิจัยและสนับสนุนงานวิจัยและการพัฒนาการวิจัยด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ

The Cyber Security Research Centre focuses on fostering collaboration in research and innovation, advancing academic staff, generating new knowledge, and utilizing academic research to assist students and researchers. A cooperative structure is formed to investigate and develop novel

approaches linked to cybersecurity in the country to facilitate information sharing and educational resource utilization. Thus, initiatives have been arranged to enhance the network. The Cyber Security Research Network intends to create a framework that supports research and development in the country's cybersecurity.



การรับมือหลังยุค Quantum

Responding to Cyber Threats in the Post-Quantum Era

คำแนะนำในการรับมือหลังยุค Quantum

Advice on How to Respond to Cyber Threats in the Post-Quantum Era

ความกังวลเกี่ยวกับควอนตัมคอมพิวเตอร์ที่มีแนวโน้มพร้อมใช้ภายในอีกไม่กี่ปีข้างหน้า คือความสามารถในการถอดรหัสลับข้อมูลสูงกว่าคอมพิวเตอร์ในระบบปัจจุบันอย่างเทียบไม่ได้ คำแนะนำ แนวทางการปฏิบัติการเตรียมความพร้อมสำหรับยุคควอนตัม (Guideline for Post-Quantum Readiness) คือความพยายามของ สกมช. และกลุ่มนักวิชาการด้านควอนตัมคอมพิวเตอร์ นำเสนอแนวทางปฏิบัติให้องค์กร หน่วยงานภายในประเทศได้ตระหนักและเข้าใจถึงความสำคัญในการแสวงหาเทคโนโลยีและองค์ความรู้ใหม่ มาปรับปรุง และเปลี่ยนแปลงเทคโนโลยีการเข้ารหัสลับข้อมูลที่ใช้ในปัจจุบัน ในคำแนะนำประกอบด้วยข้อมูล เกี่ยวกับเทคโนโลยีที่พัฒนาเพื่อป้องกันเหตุ การจัดการสินทรัพย์ด้านข้อมูลขององค์กร รวมไปถึงการประเมิน ความพร้อมและความเสี่ยงว่าองค์กรที่บริหารนั้นต้องปรับตัวไปในทิศทางไหน และจัดการด้านทรัพยากรอย่างไร ให้มีประสิทธิภาพสูงที่สุดภายใต้ข้อจำกัดขององค์กรแต่ละแห่ง



การยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามมาตรฐาน Global Cyber Index (GCI) Enhancement of Cybersecurity according to Global Cybersecurity Index (GCI)

ดำเนินการขับเคลื่อนการยกระดับการพัฒนาดัชนีความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของประเทศไทยในระยะที่ 2 ประจำปี พ.ศ. 2567 ตาม “แผนปฏิบัติการเพื่อยกระดับดัชนีชี้วัดด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี” โดยมีการดำเนินงานที่สำคัญ อาทิ

Conduct a comprehensive operational strategy formulation in accordance with the “Three Years Action Plan to Raise the Global Cybersecurity Index (GCI) of the International Telecommunication Union (ITU) for Thailand” in order to advance the development of the Global Cybersecurity Index (GCI) of Thailand in Phase 2, fiscal year 2024, including critical tasks such as:

- 1** **จัดทำแผนการดำเนินงาน (Project Work Plan) อย่างละเอียด**
Develop a comprehensive operational strategy
- 2** **ศึกษารวบรวมข้อมูล ข้อเท็จจริง หลักฐานที่สอดคล้องกับแบบประเมินภายใต้ดัชนีชี้วัด Global Cybersecurity Index: GCI ของสหภาพโทรคมนาคม (ITU)**
Research and acquire data, facts, and evidence that align with the evaluation criteria of the GCI
- 3** **จัดกิจกรรมคัดเลือก Talent ในกลุ่มเป้าหมาย เพื่อเป็นตัวแทนของประเทศไทยในการแลกเปลี่ยนภายใต้โครงการ “Cyber Security Program Exchange 2024”**
Organize an event to discover talented individuals from the target demographic to serve as representatives for Thailand in the “Cyber Security Program Exchange 2024”
- 4** **จัดทำ MOU เพื่อสร้างความร่วมมือระหว่าง ภาควิชาการ ภาครัฐ ภาคเอกชน ภายในประเทศที่เกี่ยวข้องกับ Cyber Security เพื่อจัดตั้งเป็น “ภาคีเครือข่ายความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย” หรือ Thailand Cyber Security Consortium**
Create a Memorandum of Understanding (MoU) to facilitate collaboration among academia, government, and the corporate sector in Thailand on cybersecurity, with the aim of establishing the “Thailand Cyber Security Consortium”

- 5** ส่งเสริมและสร้างความร่วมมือระหว่าง หน่วยงานกำกับดูแล หน่วยงานภาครัฐที่เกี่ยวข้อง และ "ภาคีเครือข่ายความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย"
Promote collaboration among government agencies, regulator, and Thailand Cyber Security Consortium
- 6** การจัดทำแบบสอบถามด้านมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์
Create a survey on cybersecurity standards
- 7** การประชุมเพื่อกำหนดเกณฑ์และพิจารณาผลการประเมิน หน่วยงานที่มีมาตรฐานความมั่นคงปลอดภัยไซเบอร์ ดีเลิศ
Arrange a meeting to establish criteria and review evaluations of organizations with outstanding cybersecurity standards
- 8** สรุปผลและจัดทำข้อเสนอแนะให้กับ สกมช.
Provide a concise summary of the findings and offer suggestions to NCSA



The table below shows global commitments of specific indicators per pillar.

Legal Measuring the laws and regulations on cybercrime and cybersecurity	107 Countries with some form of cybersecurity legislation 133 Data Protection Regulations 97 Criminal Information Regulations
Technical Measuring the implementation of technical capabilities through national and sectoral agencies	131 Active CERT 104 Engaged in a regional CERT 101 Child Online Protection Reporting mechanisms
Organizational Measuring the national strategies and organizations implementing cybersecurity	127 National Cybersecurity Strategies 136 Cybersecurity Agencies 86 Child Online Protection strategies and initiatives reported
Capacity development Measuring awareness campaigns, training, education, and exercises for cybersecurity capacity development	142 Countries conduct cybersecurity initiatives 94 Countries with cybersecurity R&D programs 98 Countries reported having national cybersecurity industries
Cooperation Measuring partnerships between agencies, firms, and countries	106 Countries engaged in cybersecurity Public-Private Partnerships 90 Countries with cybersecurity bilateral agreements 112 Countries with cybersecurity multilateral agreements



การจัดตั้งประชาคมไซเบอร์แห่งชาติ Establishment of the National Cyber Community

การประชุม กมช. ครั้งที่ 2/2566 เมื่อวันที่ 30 มีนาคม 2566 เห็นชอบการจัดตั้ง “ประชาคมไซเบอร์แห่งชาติ” เพื่อให้สอดคล้องตามมาตรา 9 (6) และมาตรา 42 (4) พ.ร.บ.รักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยต้องมีการประสานความร่วมมือระหว่างภาครัฐ เอกชน และความร่วมมือระหว่างประเทศ เพื่อปิดช่องว่าง ลดความเสี่ยงภัยไซเบอร์ ประกอบนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565 – 2570 กำหนดให้มีการจัดตั้ง “ประชาคมไซเบอร์แห่งชาติ” เพื่อเพิ่มศักยภาพ ส่งเสริมสนับสนุน พัฒนา และการกำกับดูแล (Governance) ด้านความมั่นคงปลอดภัยไซเบอร์

The NCSC Meeting No.2/2023 on March 30, 2023, endorsed the establishment of a “National Cyber Community” in accordance with Section 9 (6) and Section 42 (4) of the Cybersecurity Act 2019. The National Cyber Community requires coordination and cooperation among the government, private sector, and international partners to address the gap and mitigate cyber threats. The establishment of the “National Cyber Community” is in line with the Cybersecurity Policy and Action Plan 2022 - 2027 to enhance the capacity for promoting, supporting, developing, and governing cybersecurity.

เพิ่มศักยภาพในการกำกับดูแล (Governance)			
กำหนดกรอบการประสานความร่วมมือกับหน่วยงาน		กำหนดนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์	
ในประเทศ	ต่างประเทศ	ประมวลแนวทางปฏิบัติ	กรอบมาตรฐาน

โดยมีกลุ่มเป้าหมายหลัก คือ หน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ อาทิ หน่วยงานภาครัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ กลุ่มเป้าหมายรองหน่วยงานภาคเอกชน และประชาชนทั่วไป ที่มีความสนใจและเกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ ผลสรุปข้อคิดเห็นเกี่ยวกับแนวคิดสำหรับการจัดตั้งประชาคมไซเบอร์แห่งชาติ เก็บตัวอย่างข้อมูลแบบสอบถามเพื่อใช้ประกอบในการวิเคราะห์ผลทั้งสิ้น 360 ชุดข้อมูล ประเมินผลสัมฤทธิ์จากแบบสอบถาม ซึ่งเป็นคำถามปลายปิดทั้งแบบเลือกตอบได้ข้อเดียวและเลือกตอบได้หลายข้อ จำนวน 7 ข้อ

The framework aims to construct the National Cyber Community, focusing on agencies responsible for maintaining cybersecurity, including government agencies, regulators, and organizations of Critical Information Infrastructure. The secondary target group comprises individuals from the private sector and the general public who have an interest in computers, computer systems, and computer programmes.

In order to reach a conclusion regarding suggestions for the establishment of the National Cyber Community, 360 datasets of questionnaire data samples were collected for analysis. An assessment was conducted on the achievement outcomes derived from the questionnaires. The survey comprises a total of seven closed-ended questions, comprising both multiple-choice and single-choice responses.

1 **ความคิดเห็นด้านการจัดตั้ง ประชาคมไซเบอร์แห่งชาติ** Establishment of the National Cyber Community

จำนวน **303** คน
คิดเป็นร้อยละ **84.17**

2 **ความคิดเห็นด้านบทบาทและ หน้าที่ของประชาคมไซเบอร์แห่งชาติ** Roles and responsibilities of the National Cyber Community

จำนวน **303** คน
คิดเป็นร้อยละ **84.17**

3 **ความคิดเห็นด้านอำนาจในการขับเคลื่อน งานด้านไซเบอร์ของประเทศ** Authority in driving country's cyber operations

จำนวน **319** คน
คิดเป็นร้อยละ **88.61**

4 **ความคิดเห็นด้านกรอบความร่วมมือ กับหน่วยงานต่าง ๆ ของประชาคม ไซเบอร์แห่งชาติ**

Prospect of engaging in collaborative
efforts with various agencies comprising
the National Cyber Community

จำนวน **319** คน
คิดเป็นร้อยละ **88.61**

5 **ความคิดเห็นด้านแหล่งที่มา ของงบประมาณในการจัดตั้ง และดำเนินงานของประชาคม ไซเบอร์แห่งชาติ**

Sources of funding for the
establishment and operation of
the National Cyber Community

จำนวน **303** คน
คิดเป็นร้อยละ **64.44**

6 **ความคิดเห็นด้านรูปแบบการสื่อสาร ประชาสัมพันธ์ที่จะช่วยสร้างความเข้าใจ** Formats of public relations communications to promote comprehension

จำนวน **305** คน
คิดเป็นร้อยละ **84.72**

7 **ความคิดเห็นด้านกระบวนการ ที่จะทำให้ประชาคมไซเบอร์แห่งชาติ สามารถสร้างภาคีเครือข่าย**

Procedure that would facilitate the
formation of network partnerships
by the National Cyber Community

จำนวน **291** คน
คิดเป็นร้อยละ **80.83**









รางวัลแห่งความภาคภูมิใจ Awards of Pride

ล.กมช. ควา รางวัล CSO30 ASEAN Award 2023

Air Vice Marshal Amorn Chomchoey, Secretary-General of the National Cyber Security Agency won the CSO30 ASEAN Award 2023

สุดยอด 30 ผู้นำด้านความปลอดภัยทางไซเบอร์แห่งอาเซียน โดยรางวัลนี้มอบให้กับผู้นำในด้านความปลอดภัยในโลกไซเบอร์ (Cybersecurity) เพียง 30 คนในภูมิภาคอาเซียน โดย CSO ถือเป็นองค์กรระดับโลกที่ให้บริการข้อมูลข่าวสาร บทวิเคราะห์และงานวิจัยด้านความปลอดภัยและการบริหารจัดการความเสี่ยง โดยพิจารณาจากปัจจัยในการเป็นกำลังสำคัญในการขับเคลื่อนประเทศ ด้วยนวัตกรรม ด้วยการยกระดับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การสนับสนุนการจัดตั้งและยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT) ได้อย่างมีนัยสำคัญ รวมทั้งการขับเคลื่อนด้วยการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์กว่า 5,000 คน การรับรางวัลดังกล่าวเกิดจากการผลักดันและขับเคลื่อนงานของ สกมช. ให้เป็นที่ยอมรับในภูมิภาค



The CSO30 ASEAN Award 2023 is given to the top 30 cybersecurity leaders in the ASEAN region. CSO is a global organization that provides information services, analysis, and research on safety and risk management while being a vital force in driving innovation by upgrading critical information infrastructure units and supporting the establishment of the ThaiCERT for critical information infrastructure agencies (Sectoral CERT) significantly.

Winning the award was attributed to pushing and driving the work of the Office of the National Cyber Security Agency (NCSA) to be recognized in the region and develop more than 5,000 cybersecurity personnel.

การประเมินเว็บไซต์ที่ทุกคนเข้าถึงได้ตามมาตรฐาน WCAG Web Content Accessibility Guidelines (WCAG)



การประเมินเว็บไซต์ที่ทุกคนเข้าถึงได้ตามมาตรฐาน Web Content Accessibility Guidelines (WCAG) เป็นการส่งเสริมและสนับสนุนการพัฒนาเว็บไซต์ที่ทุกคนเข้าถึงได้ (Web Accessibility) เป็นปีแรกที่ สกมช. เข้ารับการประเมินและได้รับรางวัล ซึ่งทำให้ สกมช. จะมีการพัฒนาต่อไป

The evaluation of websites accessible to all by the Web Content Accessibility Guidelines (WCAG) aims to promote and support the development of websites everyone can access, thus promoting web accessibility. This year, NCSA has been evaluated and received an award, allowing it to improve further and develop.



ผลการประเมิน Data Catalog (Data Catalog results)

สกมช. ได้รับ 100 คะแนน ขั้นสูงสุด ในการประเมินการเปิดเผยข้อมูลภาครัฐตามแนวทางที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือ สพร. กำหนด โดย สกมช. ได้ตระหนักถึงความจำเป็นของการพัฒนาองค์กรไปสู่การเป็นองค์กรดิจิทัล เพื่อรองรับการปรับเปลี่ยนเป็นระบบราชการดิจิทัลอย่างเต็มรูปแบบในอนาคต จึงให้ความสำคัญกับการปรับปรุงข้อมูลในความรับผิดชอบให้อยู่ในรูปแบบดิจิทัล เพื่อให้หน่วยงานต่าง ๆ และผู้สนใจ สามารถเข้าถึงได้อย่างสะดวก รวดเร็ว ทุกที่ทุกเวลา โดยไม่เสียค่าใช้จ่าย รวมทั้งสามารถนำไปใช้ต่อยอด และพัฒนานวัตกรรม เพื่อการป้องกัน รับมือ และลดความเสี่ยงภัยคุกคามทางไซเบอร์ของประเทศได้อย่างมีประสิทธิภาพ และทันต่อสถานการณ์

100 highest scores for evaluating government information disclosure according to the Digital Government Development Agency (Public Organization: DGA) guidelines. (Public Organization). NCSA has realized the need to transform the organization into a fully digital entity to support the government system's complete digitalization in the future. As a result, we are committed to improving the information under our responsibility in a digital format that can be easily accessed and used by various agencies and interested parties, free of charge. We aim to facilitate convenient and quick access to this information anytime and anywhere, with the ability to expand and develop innovations. The well-developed innovation will help prevent, manage, and reduce cyber threats in the country promptly and efficiently.

ผลการประเมิน PMQA PMQA Results (PMQA: Public Sector Management Quality Award)

การก้าวสู่ปีที่ 2 ของการประเมินสถานะของหน่วยงานภาครัฐในการเป็นระบบราชการ 4.0 (PMQA 4.0) สกมช. พัฒนานวัตกรรมด้วยผลการดำเนินงานแบบก้าวกระโดดจากปี 2565 ได้รับผลการประเมิน 210.80 คะแนน สู่ 457.53 คะแนน ระดับก้าวหน้า จากคะแนนเต็ม 500 คะแนน ในปี 2566 โดยมี 2 หมวด ที่มีค่าคะแนนสูงที่สุด ได้แก่ หมวด 2 การวางแผนเชิงยุทธศาสตร์ 479.17 คะแนน และหมวด 1 การนำองค์กร 468.75 คะแนน ซึ่งสอดคล้องกับที่ สกมช. เป็นหน่วยงานนโยบายที่มีการขับเคลื่อนประเด็นงานการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ และ สกมช. จะใช้เป็นแนวทางในการวางรากฐานสู่การสมัครรับรางวัลเลิศรัฐ ของ ก.พ.ร. ต่อไป

As NCSA moves into the second year of evaluating the status of government agencies in becoming Bureaucratic System 4.0 (PMQA 4.0), NCSA has made significant strides in improving its performance since 2022. In 2023, NCSA received a total evaluation score of 457.53 out of a possible 500 points, substantially improving from its previous score of 210.80. There are two categories with the highest scores: Category 2 Strategic Planning with 479.17 points and Category 1 Organizational Leadership with 468.75 points. It is consistent with NCSA being a policy agency that the organization has been actively promoting the maintenance of cyber security in the country. In the future, the NCSA will use this as a guideline to establish the foundation for applying for the Public Sector Excellence Award from the Office of the Public Sector Development Commission: OPDC



ผลการประเมิน ITA ITA Results (ITA: Integrity and Transparency Assessment)

อันดับ 3 ของหน่วยงานประเภทองค์กรมหาชน ปีแรกของการประเมินคุณธรรมและความโปร่งใสในการดำเนินงานของหน่วยงานภาครัฐ (ITA) เริ่มต้นด้วย ระดับผ่านดี ด้วยคะแนน 95.13 คะแนน จากคะแนนเต็ม 100 คะแนน โดยมีผลการประเมินคะแนนรายตัวชี้วัดที่มีคะแนนสูงสุดในตัวชี้วัดที่ 1 การปฏิบัติหน้าที่ 98.92 คะแนน และตัวชี้วัดที่ 7 ประสิทธิภาพการสื่อสาร 84.81 ซึ่งมีค่าคะแนนน้อยที่สุด ที่ สกมช. อยู่ระหว่างการพัฒนากระบวนการพัฒนาประสิทธิภาพการสื่อสารต่อสาธารณชน ผ่านช่องทางที่หลากหลาย สามารถเข้าถึงได้ง่ายและไม่ซับซ้อน โดยข้อมูลที่เผยแพร่จะมีความครบถ้วนและเป็นปัจจุบัน รวมทั้งมีการเผยแพร่ข้อมูลข่าวสารที่ประชาชนหรือผู้รับบริการจะได้รับทราบอย่างชัดเจน เพื่อส่งเสริมความโปร่งใสในหน่วยงานต่อไป

NCSA ranked 3rd among agencies in the category of public organizations. In the first year of assessing morality and transparency in the operations of government agencies (ITA), an excellent passing level score of 95.13 out of 100 was achieved. The performance of duties (Indicator 2) received the highest score of 98.92 points, while communication efficiency (Indicator 1) had the lowest score of 84.81 points. NCSA is developing an easily accessible communication process to disseminate complete and up-to-date information for transparency and clarity through various channels for the public and service recipients.

การพัฒนาบุคลากร Personnel Development

การพัฒนาบุคลากร สกมช. สู่มาตรฐานสากล

Developing NCSA Personnel Towards International Standards

พนักงานมี
Core, Managerial,
Functional
Competency

จำนวน คิดเป็นร้อยละ

41 คน **81**

จำนวน คิดเป็นร้อยละ

42 คน **83**

พนักงานมี
Certificate
ด้านไซเบอร์พื้นฐาน
CompTIA Sec+
หรือ CC(ISC)2



การฝึกอบรมยกระดับศักยภาพ และทักษะผู้ปฏิบัติงานของ สกมช. Developing NCSA Personnel

สร้างการมีส่วนร่วมในกิจกรรมการทำงาน โดยมีตัวชี้วัดกำหนดว่า บุคลากรทุกระดับรับรู้และมีส่วนร่วมในกิจกรรมของ สกมช. ร้อยละ 60 ผลที่ได้คือ บุคลากรทุกระดับรับรู้และมีส่วนร่วมในกิจกรรมของ สกมช. ร้อยละ 80 และเน้นการพัฒนาผู้นำให้เป็นผู้นำยุคใหม่ และเพิ่มศักยภาพและความเข้าใจทักษะการทำงานที่จำเป็นในยุคปัจจุบัน

Throughout 2023, NCSA arranges capacity development activities for personnel, with key performance indicators set at 60% staff participation, achieving 80% participation. Emphasis is placed on developing next-generation leaders and enhancing essential skills and understanding for the modern era.

**โครงการเสริมสร้างพัฒนาศักยภาพบุคลากร
ระดับผู้บริหาร NCSA Leadership Program**

"Leadership Capacity Enhancement
Training for the Management"

กิจกรรมพัฒนาบุคลิกภาพ

"Personality Development Workshop"

**กิจกรรมพัฒนาทักษะการประชุม
นำเสนอ และบรรยายสรุป**

"Presentation Skills
Development Program"

**การอบรมเชิงปฏิบัติการเพื่อพัฒนา
การคิดเชิงออกแบบ (Design Thinking)
สำหรับผู้บริหารระดับต้น สกมช.**

"Design Thinking Workshop"

**การอบรมเชิงปฏิบัติการเพื่อสร้างแรงบันดาลใจ
ในการพัฒนาทักษะภาษาอังกฤษสำหรับผู้ปฏิบัติงาน
ของ สกมช.**

"English Communication
Skills Workshop"



การเสริมสร้างองค์ความรู้ ในกิจกรรม KM. ทุกวันศุกร์ KM (Knowledge Management)



KM FRIDAY TALK
"Open Data"
การพัฒนาแบบข้อมูลให้เป็นดิจิทัล เพื่อไปสู่การเปิดเผย

บรรยายโดย
พีท ก๊อป
นายกฯ (พธช.) สมุทรสาคร

วันศุกร์ที่ 10 ก.พ. 66 เวลา 15.00 - 16.00 น.
ผ่านระบบ ZOOM

OPENING SHOW
พบการนำเสนอผลงานนักศึกษาฝึกงาน
เวลา 14.45 - 15.00

(อ.กฤษณะ (พธช.) และ อ.กฤษณะ (พธช.))

Special KM Friday Talk
"Data Analytics"
เปลี่ยนข้อมูล เป็นเครื่องมือทรงพลัง

ได้ความรู้โดย วิชาเอกรับเชิญ
คุณวรพัญญา ระเบียบโลก
Chief Data Scientist
จาก บริษัท เทคโนโลยีสารสนเทศและการสื่อสาร (มหาชน) (พธช.)

ศุกร์ 23 มี.ค. 66 เวลา 13.00 - 14.00 น. ผ่านระบบ Zoom

หากคุณกำลังมีปัญหายุ่งเหยิงแกว่งๆ เตรียมพบกับ
KM FRIDAY TALK
"การแก้ปัญหาที่ยุ่งยาก
ด้วยวิธีการพับผ้าห่ม"

SPEAKER
พลเอก สุชาติ วงษ์มาก
ผู้บัญชาการกองทัพบก

วันศุกร์ เวลา 15.45 เป็นต้นไป
25 พฤศจิกายน 2565
ห้อง CO-WORKING SPACE

รับเกียรติจาก และมาพบกับห้อง CO

KM FRIDAY TALK
E-Saraban Series

NEW UPDATE
Workshop การใช้ระบบ
Saraban Electronic

วันพฤหัสบดี 7 ธ.ค. 66
และ ศุกร์ที่ 15 ธ.ค. 66
เวลา 15.00 - 16.00 น.
ผ่าน Zoom Meeting

กิจกรรมประชาสัมพันธ์สร้างความตระหนักรู้ การรักษาความมั่นคงปลอดภัยไซเบอร์สู่ภาคประชาชน ภายในปี 2566 Creating Awareness of Cybersecurity

ฝ่ายสื่อสารองค์กร ได้ดำเนินการเผยแพร่ข้อมูลข่าวสาร ข่าวประชาสัมพันธ์ ที่มีสาระประโยชน์ต่อการดำเนินชีวิตของประชาชน และเพื่อสร้างภาพลักษณ์ที่ดีให้กับ สกมช. ทั้งการเผยแพร่ประชาสัมพันธ์ภารกิจหน้าที่ข่าวสารเตือนภัย ให้ความรู้ทางด้านไซเบอร์ ตลอดจนวิธีป้องกันภัยคุกคามทางไซเบอร์รูปแบบต่างๆ มาโดยตลอด โดยในปี 2566 ได้ขยายช่องทางการให้ความรู้แก่ประชาชน ผ่านการจัดกิจกรรมออกบูธนิทรรศการประชาสัมพันธ์

The Corporate Communications Department has communicated news and press releases that are useful to the lives of the people, and to create a good image for the NCSA, including publicizing its mission, news, warnings, knowledge regarding cyber awareness, as well as ways to prevent various forms of cyber threats. In 2023, it has expanded channels to provide knowledge to the public through public relations exhibition booth activities.

กลุ่มเป้าหมายกว่า **30,000** คน ทั้งหมด **17** งาน
Target group of more than **30,000** people, totaling **17** events

1. งาน Enterprise IT Infrastructure Day 2022
2. งาน BOT Digital Finance Conference 2022
3. งานการประชุมวิชาการสถาบันพระปกเกล้า ครั้งที่ 24 เรื่อง “ความมั่นคงใหม่กับประชาธิปไตย”
4. งาน DigiTech ASEAN Thailand 2022
5. งาน “Thailand 4.0 ประเทศไทยไปไกลกว่าที่คิด: Thailand 4.0 The Future and Beyond”
6. งานสัมมนา “PDPA Going Forward”
7. งานวันผู้สูงอายุแห่งชาติและวันแห่งครอบครัว ประจำปี 2566
8. งาน Cyber Operations Contest 2023
9. งาน Smart Cyber Security Summit Thailand 2023
10. งาน Privacy & Security Summit 2023
11. งานสัมมนา “ภัยคุกคามด้านไซเบอร์กับ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์”
12. งาน Healthcare Technology Summit 2023
13. งาน HACKaTHAILAND 2023: DIGITAL INFINITY
14. งาน eBiz Expo 2023
15. งาน CyberSecPro
16. งาน MDES FutureScape 2023
17. งานเสวนา เรื่อง “สิทธิของประชาชนเมื่อถูกคุกคามจากภัยไซเบอร์”



สร้างเกราะป้องกันภัยไซเบอร์ในกิจกรรมเพื่อสังคม (CSR) Corporate Social Responsibility (CSR)

ส่งเสริมให้ประชาชนทุกช่วงวัย รู้ทัน ป้องกัน ภัยไซเบอร์ สามารถใช้ชีวิตบนโลกไซเบอร์ได้อย่างมั่นคงและปลอดภัย ผ่านกิจกรรมเพื่อสังคม Corporate Social Responsibility ร่วมติดตามข่าวสารทางปัญญา สร้างการตระหนักรู้ พัฒนาทักษะด้านไซเบอร์จำนวน 5 ครั้ง ดังนี้

1. โครงการ CSR กิจกรรม “พี่ชวนน้อง เรียน เล่น รู้ ภัยไซเบอร์” ณ มูลนิธิพระมหาไถ่เพื่อการพัฒนาคนพิการ
2. โครงการ CSR กิจกรรม “รู้หน้าที่ มีวินัย ใฝ่ความดี มีภูมิคุ้มกันภัยไซเบอร์” ณ พิพิธภัณฑ์กองทัพอากาศและการบินแห่งชาติ
3. โครงการ CSR กิจกรรม “สกมช. ส่งเสริมเด็กไทยรู้ทันภัยไซเบอร์ ขับเคลื่อนการใช้เทคโนโลยี อย่างชาญฉลาด” ณ โรงเรียนอนุบาลสุพรรณบุรี
4. โครงการ CSR กิจกรรม “ชุมชนคลองเตย ตระหนักรู้ ภัยไซเบอร์” ณ มูลนิธิดวงประทีป คลองเตย
5. โครงการ CSR กิจกรรม “พี่อาสาพาน้องรู้ภัยไซเบอร์” ณ มูลนิธิพระมหาไถ่เพื่อการพัฒนาคนพิการ



NCSA Highlighted News รวมข่าวเด่นปี 2566

“สื่อสารองค์กร” เผยแพร่ประชาสัมพันธ์ข้อมูลข่าวสารผ่านช่องทางต่างๆ เพื่อเป็นการส่งเสริมภาพลักษณ์ที่ดีให้แก่องค์กร



สกมช. เพิ่มหา 'นักรบไซเบอร์' เผยไทยมีอัตราค่าจ้างเพียง 0.5%



ฝ่าแนวคิด "สกมช." มือปราบภัยไซเบอร์ รับมือ ภัยคุกคามป่วนหนัก



สกมช. คุมเข้มทุกหน่วยงาน ยกกระดานการป้องกันภัยไซเบอร์



รู้ทันภัยไซเบอร์ ! สกมช. 'อัปสเกล-เสริมทักษะ' ปลุกภูมิคุ้มกันประชาชนทุกช่วงวัย



สกมช. ประเดิม 10 องค์กร ปัน MISP แหล่งข่าวกรองไซเบอร์ของไทย



สกมช. เร่งสร้างภูมิคุ้มกันไซเบอร์ประชาชน "THAILAND NATIONAL CYBER WEEK 2023"



การแถลงข่าวจำนวน 9 ครั้ง Press Conferences

- 1 15 ธันวาคม 2565** แถลงข่าวรายงานผลการประเมินความเสี่ยงและสถานะความพร้อมในการรับมือต่อภัยคุกคามทางไซเบอร์ของประเทศ
- 2 20 มกราคม 2566** แถลงข่าวกรณีแอปดูดเงิน พร้อมเปิดรายชื่อแอปอันตรายกว่า 200 แอปฯ
- 3 30 มกราคม 2566** แถลงข่าวเปิดตัว “Thailand National Cyber Week 2023”
- 4 31 มีนาคม 2566** แถลงข่าวข้อมูลส่วนตัวของประชาชนโดนแฮก 55 ล้านคน
- 5 25 พฤษภาคม 2566** สกมช. ร่วมแถลงข่าวการบุกทลายแก๊งสวมรอย ธนาคารสิริไทย หลอกดูดเงิน
- 6 16 มิถุนายน 2566** สกมช. ร่วมกับ AIS เปิดตัวดัชนีชี้วัดสุขภาพดิจิทัลครั้งแรก เผยคนไทย 44.04% เสี่ยงภัยไซเบอร์
- 7 11 สิงหาคม 2566** สกมช. ร่วมกับ กรมที่ดิน แจงกรณีถูกหลอกติดตั้งแอปดูดเงิน เตือนประชาชนอย่าหลงเชื่อ
- 8 24 สิงหาคม 2566** สกมช. ร่วมปฏิบัติการ จับกุมพ่อค้าคนกลาง รับซื้อ-ขายข้อมูลส่วนบุคคล กว่า 15 ล้านรายชื่อ
- 9 26 กรกฎาคม 2566** แถลงข่าว สกมช. ผนึก ห้วเว่ย จัดแข่ง “Thailand Cyber Top Talent 2023” ทำชิงสุดยอดทีมไซเบอร์ของไทย เงินรางวัลกว่า 521,000 บาท



รายงานผลการดำเนินงาน ของคณะกรรมการตรวจสอบ Audit Committee Report

ผลการตรวจสอบโดยคณะกรรมการตรวจสอบ สกมช.
มีผลการปฏิบัติงานเป็นไปตามระเบียบแบบแผน
ไม่มีข้อบกพร่องที่เป็นนัยสำคัญ สรุปสาระสำคัญ ตาม QR code นี้



The audit committee's examination shows that the National Cyber Security Agency operates in compliance with regulations and policies. There were no significant discrepancies found. Key findings are summarized via QR code.





รายงานทางการเงิน Financial Report

ข้อมูลสำคัญการเงิน ปี 2566

รายงานของผู้สอบบัญชีรับอนุญาต

เสนอ คณะกรรมการ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ความเห็น

ข้าพเจ้าได้ตรวจสอบรายงานการเงินของ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งประกอบด้วยงบแสดงฐานะการเงิน ณ วันที่ 30 กันยายน 2566 งบแสดงผลการดำเนินงานทางการเงิน และงบแสดงการเปลี่ยนแปลงสินทรัพย์สุทธิ/ส่วนทุน สำหรับปีสิ้นสุดวันเดียวกัน และหมายเหตุประกอบงบการเงิน รวมถึงสรุปนโยบายการบัญชีที่สำคัญ

ข้าพเจ้าเห็นว่า รายงานการเงินข้างต้นนี้แสดงฐานะการเงินของ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ณ วันที่ 30 กันยายน 2566 และผลการดำเนินงานสำหรับปีสิ้นสุดวันเดียวกัน โดยถูกต้องตามที่ควรในสาระสำคัญตามมาตรฐานการบัญชีภาครัฐ และนโยบายการบัญชีภาครัฐที่กระทรวงการคลังกำหนด

เกณฑ์ในการแสดงความเห็น

ข้าพเจ้าได้ปฏิบัติงานตรวจสอบตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินและมาตรฐานการสอบบัญชีความรับผิดชอบของข้าพเจ้าได้กล่าวไว้ในวรรค ความรับผิดชอบของผู้สอบบัญชีต่อการตรวจสอบรายงานการเงินในรายงานของข้าพเจ้า ข้าพเจ้ามีความเป็นอิสระจากหน่วยงานตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินที่กำหนดโดยคณะกรรมการตรวจเงินแผ่นดินและประมวลจรรยาบรรณของผู้ประกอบวิชาชีพบัญชีรวมถึงมาตรฐานเรื่องความเป็นอิสระที่กำหนดโดยสภาวิชาชีพบัญชี (ประมวลจรรยาบรรณของผู้ประกอบวิชาชีพบัญชี) ในส่วนที่เกี่ยวข้องกับการตรวจสอบรายงานการเงิน และข้าพเจ้าได้ปฏิบัติตามความรับผิดชอบด้านจรรยาบรรณอื่น ๆ ซึ่งเป็นไปตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินและประมวลจรรยาบรรณของผู้ประกอบวิชาชีพบัญชี ข้าพเจ้าเชื่อว่าหลักฐานการสอบบัญชีที่ข้าพเจ้าได้รับเพียงพอและเหมาะสมเพื่อใช้เป็นเกณฑ์ในการแสดงความเห็นของข้าพเจ้า

เรื่องอื่น

รายงานการเงินของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ณ วันที่ 30 กันยายน 2565 ที่แสดงเป็นข้อมูลเปรียบเทียบตรวจสอบโดยผู้สอบบัญชีอื่น ซึ่งแสดงความเห็นอย่างไม่มีเงื่อนไขตามรายงานลงวันที่ 28 กุมภาพันธ์ 2566

ข้อมูลอื่น

ผู้บริหารเป็นผู้รับผิดชอบต่อข้อมูลอื่น ข้อมูลอื่นประกอบด้วย ข้อมูลซึ่งรวมอยู่ในรายงานประจำปี แต่ไม่รวมถึงรายงานการเงินและรายงานของผู้สอบบัญชีที่อยู่ในรายงานประจำปีนั้น ซึ่งผู้บริหารจะจัดเตรียมรายงานประจำปีให้ข้าพเจ้าภายหลังวันที่ในรายงานของผู้สอบบัญชีนี้

ความเห็นของข้าพเจ้าต่อรายงานการเงิน ไม่ครอบคลุมถึงข้อมูลอื่นและข้าพเจ้าไม่ได้ให้ความเชื่อมั่นต่อข้อมูลอื่น

ความรับผิดชอบของข้าพเจ้าที่เกี่ยวข้องกับการตรวจสอบรายงานการเงิน คือการอ่านพิจารณาว่า ข้อมูลอื่นมีความขัดแย้งที่มีสาระสำคัญกับรายงานการเงิน หรือกับความรู้ที่ได้รับจากการตรวจสอบของข้าพเจ้า หรือปรากฏว่าข้อมูลอื่นมีการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญหรือไม่

เมื่อข้าพเจ้าได้อ่านรายงานประจำปี หากข้าพเจ้าสรุปได้ว่าการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญข้าพเจ้าต้องสื่อสารเรื่องดังกล่าวกับผู้มีหน้าที่ในการกำกับดูแล

ความรับผิดชอบของผู้บริหารและผู้มีหน้าที่ในการกำกับดูแลต่อรายงานการเงิน

ผู้บริหารเป็นผู้รับผิดชอบในการจัดทำและการนำเสนอรายงานการเงินเหล่านี้โดยถูกต้องตามที่ควรตามมาตรฐานการบัญชีภาครัฐและนโยบายการบัญชีภาครัฐที่กระทรวงการคลังกำหนด และรับผิดชอบเกี่ยวกับการควบคุมภายในที่ผู้บริหารพิจารณาว่าจำเป็นเพื่อให้สามารถจัดทำรายงานการเงินที่ปราศจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญไม่ว่าจะเกิดจากการทุจริตหรือข้อผิดพลาด

ในการจัดทำรายงานการเงิน ผู้บริหารรับผิดชอบในการประเมินความสามารถของหน่วยงานในการดำเนินงานต่อเนื่องเปิดเผยเรื่องที่เกี่ยวข้องกับการดำเนินงานต่อเนื่องตามความเหมาะสม และการใช้เกณฑ์การบัญชีสำหรับการดำเนินงานต่อเนื่อง เว้นแต่มีข้อกำหนดในกฎหมายหรือเป็นนโยบายรัฐบาลที่จะเลิกหน่วยงานหรือผู้บริหารมีความตั้งใจที่จะเลิกหน่วยงานหรือหยุดดำเนินงานหรือไม่สามารถดำเนินงานต่อเนื่องต่อไปได้

ผู้มีหน้าที่ในการกำกับดูแลมีหน้าที่ในการสอดส่องดูแลกระบวนการในการจัดทำรายงานทางการเงินของหน่วยงาน

ความรับผิดชอบของผู้สอบบัญชีต่อ การตรวจสอบรายงานการเงิน

การตรวจสอบของข้าพเจ้ามีวัตถุประสงค์เพื่อให้ได้ความเชื่อมั่นอย่างสมเหตุสมผลว่า รายงานการเงินโดยรวมปราศจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญหรือไม่ ไม่ว่าจะเกิดจากการทุจริตหรือข้อผิดพลาด และเสนอรายงานของผู้สอบบัญชีซึ่งรวมความเห็นของข้าพเจ้าอยู่ด้วย ความเชื่อมั่นอย่างสมเหตุสมผลคือความเชื่อมั่นในระดับสูงแต่ไม่ได้เป็นการรับประกันว่าการปฏิบัติงานตรวจสอบตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินและมาตรฐานการสอบบัญชีจะสามารถตรวจพบข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญที่มีอยู่ได้เสมอไป ข้อมูลที่ขัดต่อข้อเท็จจริงอาจเกิดจากการทุจริตหรือข้อผิดพลาดและถือว่า มีสาระสำคัญเมื่อคาดการณ์ได้อย่างสมเหตุสมผลว่ารายการที่ขัดต่อข้อเท็จจริงแต่ละรายการหรือทุกรายการรวมกันจะมีผลต่อการตัดสินใจทางเศรษฐกิจของผู้ใช้งบการเงินจากการใช้รายงานการเงินเหล่านี้

ในการตรวจสอบของข้าพเจ้าตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินและมาตรฐานการสอบบัญชีข้าพเจ้าได้ใช้ดุลยพินิจและการสังเกตและสงสัยเยี่ยงผู้ประกอบวิชาชีพตลอดการตรวจสอบ การปฏิบัติงานของข้าพเจ้ารวมถึง

- ระบุและประเมินความเสี่ยงจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญในรายงานการเงิน ไม่ว่าจะเกิดจากการทุจริตหรือข้อผิดพลาด ออกแบบและปฏิบัติตามวิธีการตรวจสอบเพื่อตอบสนองต่อความเสี่ยงเหล่านั้น และได้หลักฐานการสอบบัญชีที่เพียงพอและเหมาะสมเพื่อเป็นเกณฑ์ในการแสดงความเห็นของข้าพเจ้า ความเสี่ยงที่ไม่พบข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญซึ่งเป็นผลมาจากการทุจริตจะสูงกว่าความเสี่ยงที่เกิดจากข้อผิดพลาด เนื่องจากการทุจริตอาจเกี่ยวกับการสมรู้ร่วมคิด การปลอมแปลงเอกสารหลักฐานการตั้งใจละเว้นการแสดงผลข้อมูล การแสดงข้อมูลที่ไม่ตรงตามข้อเท็จจริงหรือการแทรกแซงการควบคุมภายใน

- ทำความเข้าใจในระบบการควบคุมภายในที่เกี่ยวข้องกับการตรวจสอบ เพื่อออกแบบวิธีการตรวจสอบที่เหมาะสมกับสถานการณ์ แต่ไม่ใช่เพื่อวัตถุประสงค์ในการแสดงความเห็นต่อความมีประสิทธิภาพของการควบคุมภายในของหน่วยงาน

- ประเมินความเหมาะสมของนโยบายการบัญชีที่ผู้บริหารใช้และความสมเหตุสมผลของประมาณการทางบัญชีและการเปิดเผยข้อมูลที่เกี่ยวข้อง ซึ่งจัดทำขึ้นโดยผู้บริหาร

- สรุปเกี่ยวกับความเหมาะสมของการใช้เกณฑ์การบัญชีสำหรับการดำเนินงานต่อเนื่องของผู้บริหารและจากหลักฐานการสอบบัญชีที่ได้รับ สรุปว่ามีความไม่แน่นอนที่มีสาระสำคัญเกี่ยวกับเหตุการณ์หรือสถานการณ์ ที่อาจเป็นเหตุให้เกิดข้อสงสัยอย่างมีนัยสำคัญต่อความสามารถของหน่วยงานในการดำเนินงานต่อเนื่องหรือไม่ถ้าข้าพเจ้าได้ข้อสรุปว่ามีความไม่แน่นอนที่มีสาระสำคัญ ข้าพเจ้าต้องกล่าวไว้ในรายงานของผู้สอบบัญชีของข้าพเจ้า โดยให้ข้อสังเกตถึงการเปิดเผยข้อมูลในรายงานการเงินที่เกี่ยวข้อง หรือถ้าการเปิดเผยข้อมูลดังกล่าวไม่เพียงพอความเห็นของข้าพเจ้าจะเปลี่ยนแปลงไป ข้อสรุปของข้าพเจ้าขึ้นอยู่กับหลักฐานการสอบบัญชีที่ได้รับจนถึงวันที่ในรายงานของผู้สอบบัญชีของข้าพเจ้า อย่างไรก็ตาม เหตุการณ์หรือสถานการณ์ในอนาคตอาจเป็นเหตุให้หน่วยงานต้องหยุดการดำเนินงานต่อเนื่อง

- ประเมินการนำเสนอ โครงสร้างและเนื้อหาของรายงานการเงินโดยรวม รวมถึงการเปิดเผยข้อมูลว่า รายงานการเงินแสดงรายการและเหตุการณ์ในรูปแบบที่ทำให้มีการนำเสนอข้อมูลโดยถูกต้องตามที่ควรหรือไม่

ข้าพเจ้าได้สื่อสารกับผู้บริหารและผู้มีหน้าที่ในการกำกับดูแลในเรื่องต่าง ๆ ที่สำคัญ ซึ่งรวมถึงขอบเขตและช่วงเวลาของการตรวจสอบตามที่ได้วางแผนไว้ ประเด็นที่มีนัยสำคัญที่พบจากการตรวจสอบ รวมถึงข้อบกพร่องที่มีนัยสำคัญในระบบการควบคุมภายใน หากข้าพเจ้าได้พบในระหว่างการตรวจสอบของข้าพเจ้า

ข้าพเจ้าเป็นผู้รับผิดชอบงานสอบบัญชีและการนำเสนอรายงานฉบับนี้



(นายวิโรจน์ นริศรารานนท์)

ผู้สอบบัญชีรับอนุญาต ทะเบียนเลขที่ 3748

48 ซอยเจริญสุขนิทวงศ์ 34 ถนนเจริญสุขนิทวงศ์

แขวงอรุณอมรินทร์ เขตบางกอกน้อย

กรุงเทพมหานคร 10700

วันที่ 21 ธันวาคม 2566

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
งบแสดงฐานะการเงิน ณ วันที่ 30 กันยายน 2566

(หน่วย : บาท)

	หมายเหตุ	ปี 2566	ปี 2565
สินทรัพย์			
สินทรัพย์หมุนเวียน			
เงินสดและรายการเทียบเท่าเงินสด	5	182,511,805.46	96,675,385.01
ลูกหนี้อื่นระยะสั้น	6	313,863.68	43,791.78
วัสดุคงเหลือ	7	1,171,904.62	727,995.17
รวมสินทรัพย์หมุนเวียน		183,997,573.76	97,447,171.96
สินทรัพย์ไม่หมุนเวียน			
อาคารและอุปกรณ์ - สุทธิ	8	163,257,094.21	16,461,228.65
สินทรัพย์ไม่มีตัวตน - สุทธิ	9	8,268,418.10	5,076,595.93
รวมสินทรัพย์ไม่หมุนเวียน		171,525,512.31	21,537,824.58
รวมสินทรัพย์		355,523,086.07	118,984,996.54
หนี้สินและสินทรัพย์สุทธิ/ส่วนทุน			
หนี้สิน			
หนี้สินหมุนเวียน			
เจ้าหนี้อื่นระยะสั้น	10	35,507,126.08	1,783,074.75
เงินรับฝากระยะสั้น	11	6,059,923.90	2,288,697.90
รายได้รอการรับรู้	12	47,795,343.50	-
หนี้สินหมุนเวียนอื่น	13	495,548.48	323,308.12
รวมหนี้สินหมุนเวียน		89,857,941.96	4,395,080.77
รวมหนี้สิน		89,857,941.96	4,395,080.77
สินทรัพย์สุทธิ/ส่วนทุน			
ทุน		-	-
รายได้สูง (ต่ำ) กว่าค่าใช้จ่ายสะสม		265,665,144.11	114,589,915.77
รวมสินทรัพย์สุทธิ/ส่วนทุน		265,665,144.11	114,589,915.77
รวมหนี้สินและสินทรัพย์สุทธิ/ส่วนทุน		355,523,086.07	118,984,996.54

หมายเหตุประกอบงบการเงินเป็นส่วนหนึ่งของรายงานการเงินนี้



(นางมัตติกา จงพิริยะอนันต์)

ผู้อำนวยการสำนักงานการเงินและกลยุทธ์องค์กร

พลอากาศตรี



(อมร ชมเชย)

เลขาธิการคณะกรรมการการรักษาความมั่นคง
ปลอดภัยไซเบอร์แห่งชาติ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
งบแสดงผลการดำเนินงานทางการเงิน สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2566

(หน่วย : บาท)

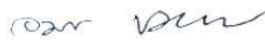
	หมายเหตุ	ปี 2566	ปี 2565
รายได้			
รายได้จากงบประมาณ	15	318,796,793.00	163,544,100.00
รายได้จากการอุดหนุนและบริจาค	16	114,747,418.53	108,245.00
รวมรายได้		433,544,211.53	163,652,345.00
ค่าใช้จ่าย			
ค่าใช้จ่ายบุคลากร	17	47,725,498.67	40,424,098.83
ค่าตอบแทน	18	301,522.58	1,302,958.16
ค่าใช้สอย	19	97,291,588.08	29,022,682.53
ค่าวัสดุ	20	4,156,976.54	2,873,801.15
ค่าสาธารณูปโภค	21	787,639.24	622,810.76
ค่าเสื่อมราคาและค่าตัดจำหน่าย	22	19,036,765.02	4,165,879.27
ค่าใช้จ่ายจากการอุดหนุนอื่นและบริจาค	23	114,148,324.00	-
รวมค่าใช้จ่าย		283,448,314.13	78,412,230.70
รายได้สูง (ต่ำ) กว่าค่าใช้จ่ายสุทธิ		150,095,897.40	85,240,114.30

หมายเหตุประกอบงบการเงินเป็นส่วนหนึ่งของรายงานการการเงินนี้



(นางมัตติกา จงพิริยะอนันต์)

ผู้อำนวยการสำนักงานการเงินและกลยุทธ์องค์กร

พลอากาศตรี 

(อมร ชมเชย)

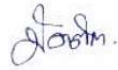
เลขาธิการคณะกรรมการการรักษาความมั่นคง
ปลอดภัยไซเบอร์แห่งชาติ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
งบแสดงการเปลี่ยนแปลงสินทรัพย์สุทธิ/ส่วนทุน สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2566

(หน่วย : บาท)

	ทุน	รายได้สูง / (ต่ำ) กว่าค่าใช้จ่ายสะสม	รวมสินทรัพย์ สุทธิ/ส่วนทุน
ยอดคงเหลือ ณ วันที่ 1 ตุลาคม 2564	-	29,349,801.47	29,349,801.47
การเปลี่ยนแปลงในสินทรัพย์สุทธิ/ส่วนทุนสำหรับปี 2565	-	85,240,114.30	85,240,114.30
รายได้สูง (ต่ำ) กว่าค่าใช้จ่ายสำหรับงวด			
ยอดคงเหลือ ณ วันที่ 30 กันยายน 2565	-	114,589,915.77	114,589,915.77
ยอดคงเหลือ ณ วันที่ 1 ตุลาคม 2565 - ตามที่รายงานไว้เดิม	-	114,589,915.77	114,589,915.77
ผลสะสมจากการแก้ไขข้อผิดพลาดปีก่อน		979,330.94	979,330.94
ยอดคงเหลือ ณ วันที่ 1 ตุลาคม 2565 - หลังการปรับปรุง	-	115,569,246.71	115,569,246.71
การเปลี่ยนแปลงในสินทรัพย์สุทธิ/ส่วนทุนสำหรับปี 2566			
รายได้สูง (ต่ำ) กว่าค่าใช้จ่ายสำหรับงวด		150,095,897.40	150,095,897.40
ยอดคงเหลือ ณ วันที่ 30 กันยายน 2566	-	265,665,144.11	265,665,144.11

หมายเหตุประกอบงบการเงินเป็นส่วนหนึ่งของรายงานการเงินนี้



(นางมัตติกา จงพิริยะอนันต์)

ผู้อำนวยการสำนักงานการเงินและกลยุทธ์องค์กร



(อมร ชมเชย)

เลขาธิการคณะกรรมการการรักษาความมั่นคง
ปลอดภัยไซเบอร์แห่งชาติ



การประเมินผลการดำเนินงาน

ประจำปีงบประมาณ พ.ศ. 2566

โดยบุคคลภายนอก (บริษัท วินทูเทเตอร์ จำกัด)

องค์ประกอบการประเมินผลการปฏิบัติงาน



ผลการดำเนินงานตามตัวชี้วัดของ สกมช. ตามกรอบการประเมินขององค์การมหาชน

ประสิทธิภาพ

ตัวชี้วัดที่สอดคล้องกับภารกิจตามวัตถุประสงค์การจัดตั้ง
ที่แสดงให้เห็นการเชื่อมโยงจากยุทธศาสตร์ นโยบาย และแผนระดับชาติ

ความสำเร็จของการเผยแพร่
และสร้างความเข้าใจในนโยบาย
และกฎระเบียบที่เกี่ยวข้อง
ด้านการรักษาความมั่นคง
ปลอดภัยไซเบอร์

(ร้อยละ 8)

100 คะแนน

เป้าหมายขั้นสูง
มีช่องทางการสื่อสาร

3 ช่องทาง

มีผู้เข้าร่วม
รวม **22,540 คน**

ความสำเร็จการจัดตั้ง
ศูนย์ประสานการรักษา
ความมั่นคงปลอดภัย
ระบบคอมพิวเตอร์แห่งชาติ
(ThaiCERT)

(ร้อยละ 4)

100 คะแนน

เป้าหมายขั้นสูง
ดำเนินการสำเร็จ จำนวน

444 เหตุการณ์

รายงานเหตุการณ์ภัยคุกคามทางไซเบอร์
ถึงหน่วยงานที่ประสบเหตุ

จำนวน **180 ฉบับ**

จำนวนหน่วยงานเป้าหมายที่ ThaiCERT
มีขีดความสามารถในการเฝ้าระวัง และ
ให้ความช่วยเหลือสนับสนุน การตอบสนอง
และรับมือฯ ภัยคุกคามทางไซเบอร์
ในห้วงเวลาเดียวกัน

จำนวน **24 หน่วยงาน**

ความสำเร็จในการจัดการฝึก
และทดสอบแผนเผชิญเหตุ
ในกรณีเกิดเหตุภัยคุกคาม
ทางไซเบอร์ในระดับวิกฤติ

(ร้อยละ 15)

100 คะแนน

เป้าหมายขั้นสูง
มีจำนวน

153 หน่วยงาน

เป้าหมายที่เข้าร่วมการฝึก
และมีผู้เข้าร่วมฝึกและทดสอบ
แผนเผชิญเหตุ

จำนวน **515 คน**

ความสำเร็จในการจัดทำ
แผนเผชิญเหตุด้านไซเบอร์
ของหน่วยงานภาครัฐ
และหน่วยงานโครงสร้างพื้นฐาน
ที่สำคัญทางสารสนเทศ

(ร้อยละ 15)

100 คะแนน

เป้าหมายขั้นสูง
มีจำนวน

50 หน่วยงาน

เป้าหมาย มีแผนเผชิญเหตุด้านไซเบอร์
ที่สอดคล้องกับประมวลแนวทางปฏิบัติ
และกรอบมาตรฐาน ประกอบด้วย

หน่วยงานควบคุมหรือกำกับดูแล
จำนวน **9 หน่วยงาน**

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
จำนวน **23 หน่วยงาน**

หน่วยงานของรัฐ
จำนวน **18 หน่วยงาน**



ปัญหา อุปสรรค และข้อเสนอแนะ

การดำเนินงานของ สกมช. ในปีงบประมาณ พ.ศ. 2566 ที่ผ่านมานั้น นับเป็นปีที่ 3 ของการดำเนินงานอย่างเป็นรูปธรรม และเป็นหน่วยงานหลักที่รับผิดชอบความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ แต่เนื่องด้วยภัยคุกคามทางไซเบอร์ที่มีความหลากหลายและทวีความรุนแรงเพิ่มมากขึ้นอย่างต่อเนื่อง ประกอบกับบุคลากรทางไซเบอร์ภายในประเทศมีจำนวนน้อย ซึ่งจำเป็นต้องใช้งบประมาณที่สูง และระยะเวลานานในการสร้างบุคลากรทางไซเบอร์ที่มีศักยภาพ สกมช. จึงได้มีการวิเคราะห์ปัญหาและอุปสรรค เพื่อนำมาเป็นแนวทางการแก้ไขการดำเนินงานในปีต่อไป ดังนี้

1. ด้านบุคลากร

1.1 บุคลากรของ สกมช. ในปีที่ผ่านมา มีพนักงานระดับปฏิบัติการและระดับบริหารรวมทั้งสิ้น 50 คน ในขณะที่ขอบเขตความรับผิดชอบที่ สกมช. ต้องดูแล มีเพิ่มมากขึ้น ทั้งจำนวนหน่วยงานและประชาชนที่ได้รับผลกระทบ และจำนวนเหตุการณ์ที่เกิดขึ้น สกมช. จึงไม่สามารถปฏิบัติงานแก้ไขปัญหาได้อย่างรวดเร็ว รวมถึงส่งผลกระทบต่อประสิทธิภาพของบุคลากรที่จำเป็นต้องได้รับการพัฒนาอย่างต่อเนื่อง

1.2 บุคลากรทางไซเบอร์ในภาพรวมของประเทศยังมีอยู่จำกัด และจำเป็นต้องเร่งพัฒนารวมถึงเสริมสร้างตั้งแต่การศึกษาเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับประถมศึกษา จนถึงระดับปริญญาอย่างครอบคลุมและทั่วถึง

2. ด้านงบประมาณ

ข้อจำกัดของงบประมาณในการพัฒนาและเสริมสร้างขีดความสามารถการรักษาความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของประเทศ แบ่งออกเป็น 3 ส่วน คือ (1) งบประมาณในการเสริมสร้างความพร้อมของ สกมช. (2) งบประมาณในเสริมสร้างขีดความสามารถให้กับหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และ หน่วยงานของรัฐ และ (3) งบประมาณในการสร้างความตระหนักรู้ให้กับหน่วยงานภาครัฐ ภาคเอกชน และ ประชาชน

3. ด้านเครื่องมือ

การจัดทำกฎหมายลำดับรองเพื่อเป็นเครื่องมือในการขับเคลื่อนให้หน่วยงานที่เกี่ยวข้องดำเนินการตามมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ได้กำหนดไว้ ยังไม่สามารถดำเนินการได้ด้วยความสะดวกและไม่มีความพร้อมของเทคโนโลยีเกิดข้อบกพร่องจากการปฏิบัติงานที่หละหลวม ทำให้เกิดจุดอ่อนและช่องโหว่จำนวนมาก โดยเฉพาะอย่างยิ่ง หน่วยงานของรัฐที่มีข้อมูลประชาชนเป็นจำนวนมาก แต่ยังไม่ได้ถูกประกาศให้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงยังไม่มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์หรือมีมาตรการที่ไม่สอดคล้องและเป็นไปตามมาตรฐานที่กำหนด

4. ด้านการขับเคลื่อนการนำนโยบายและแผนไปสู่การปฏิบัติ

หน่วยงานที่เกี่ยวข้องตามนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) ยังไม่สามารถปฏิบัติให้เป็นไปตามแผนงานที่กำหนดและไม่มีความพร้อมเพียงพอ จึงมีความจำเป็นต้องเร่งดำเนินการส่งเสริม ผลักดัน และติดตามให้สามารถดำเนินการวางแผน เตรียมการ ประสานงาน และดำเนินการจัดทำโครงการกิจกรรม ให้มีความสอดคล้องกับนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) และให้มีการจัดทำหรือปรับปรุงแก้ไขแผนของหน่วยงานให้มีความสอดคล้องกับนโยบายและแผนปฏิบัติการดังกล่าว โดยเร่งด่วน

บทสรุปสังกัาย รายงานประจำปี 2566 ของ สกมช.

ปี 2566 สกมช. มีการเปลี่ยนแปลงอย่างมีนัยสำคัญอยู่ 2 ประการ ประการแรก เป็นการเปลี่ยนแปลงภายใน โดยเป็นปีที่ สกมช. มีเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ท่านที่ 2 ได้แก่ พลอากาศตรี อมร ชมเชย ซึ่งได้ผ่านการเป็นรองเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมาแล้วในยุคแรก และประการที่สอง เป็นการเปลี่ยนแปลงภายนอก อันเนื่องมาจากภัยคุกคามทางไซเบอร์ได้ขยายความรุนแรงมากขึ้น ทั้งระดับองค์กรและระดับบุคคล ทำให้สังคมไทยทุกภาคส่วน ได้ตระหนักถึงภัยคุกคามทางไซเบอร์ ซึ่งเป็นภัยคุกคามรูปแบบใหม่ที่สามารถก่อความเสียหายให้กับตนเองและครอบครัวได้อย่างใหญ่หลวงมากกว่าภัยคุกคามใด ๆ ที่เคยเกิดขึ้นแล้ว การก่อกำเนิด สกมช. เพื่อมาจัดภัยดังกล่าว จึงเป็นความคาดหวังเปรียบดังแสงปลายอุโมงค์ที่สังคมและประชาชนเฝ้ารอคอย ซึ่งการเปลี่ยนแปลง ทั้ง 2 ประการนี้ ทำให้ สกมช. ต้องก้าวกระโดดออกจากมุมมืดของดิจิทัลชาว์ตัวเป็นพระเอกในการไล่ล่าโจรร้าย ซึ่งกำลังก่อความเดือดร้อนให้กับประเทศและประชาชนอย่างหนัก ภายใต้การบริหารงานของ พลอากาศตรี อมร ชมเชย เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติท่านใหม่ จึงต้องเร่งปรับกลยุทธ์ เพื่อจัดการกับภัยคุกคามไซเบอร์ที่เกิดขึ้นให้ได้โดยเร็ว การสร้างความเข้มแข็งโดยการกำหนด DNA ของ สกมช. เพื่อให้พนักงานทุกคนมีความมุ่งมั่นร่วมกัน จึงเป็นหัวใจหลักในการดำเนินการผ่านองค์ประกอบ 4 ส่วน ได้แก่



และเพื่อให้เป้าหมายการปฏิบัติงานมีประสิทธิภาพเป็นการพุ่งเป้าต่อความสำเร็จในการป้องกันและจัดภัยคุกคามทางไซเบอร์ให้กับประเทศและประชาชนอย่างรวดเร็ว สกมช. จึงปรับกลยุทธ์การทำงานเป็น 2 ด้านใหญ่ ๆ เพื่อให้สามารถจัดสรรทรัพยากรได้อย่างเหมาะสมและคุ้มค่าสูงสุด ได้แก่

1. การสร้างความเข้มแข็งให้กับตนเองและเครือข่าย

- เสริมสร้างความเข้มแข็งให้กับ สกมช. ในทุกด้าน
- เสริมสร้างความเข้มแข็งให้กับหน่วยงานควบคุมหรือกำกับดูแล (Regulator) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) และหน่วยงานของรัฐ
- เสริมสร้างความตระหนักรู้และภูมิคุ้มกันให้กับประชาชน

2. การแจ้งเตือนภัยอย่างรวดเร็วและลดความสูญเสียให้น้อยที่สุด

- การข่าวกรองที่มีประสิทธิภาพ
- การเข้าทำลายแหล่งกำเนิดภัยคุกคามทางไซเบอร์ และจัดภัยคุกคามทางไซเบอร์ด้วยความรวดเร็วและทันเวลา
- การฟื้นฟูสภาพความเสียหายจากภัยคุกคามทางไซเบอร์ให้กลับสู่สภาวะปกติโดยเร็ว

ผลการปฏิบัติงานในรอบปีงบประมาณ 2566 ที่ผ่านมา สกมช. สามารถดำเนินการป้องกันและขจัดภัยคุกคามทางไซเบอร์ให้กับประเทศและประชาชนได้อย่างกว้างขวางและรวดเร็ว ซึ่งบทเรียนในปีนี้จะทำให้ สกมช. มีความเข้มแข็งมากยิ่งขึ้นในปีต่อ ๆ ไป เป็นหลักประกันต่อความสงบเรียบร้อยของประเทศและประชาชน เพื่อส่งเสริมให้การพัฒนาประเทศมีความเจริญก้าวหน้ายิ่งขึ้นไป นำความพาสมาสู่ประชาชนคนไทยทุกคน

Conclusion

In 2023, NCSA had two significant changes. First, It was an internal change. This was the year that NCSA had the second secretary-general of the National Cyber Security Committee, named Air Vice Marshal Amorn Chomchoey, who had already been in the position of deputy secretary-general of the National Cyber Security Committee in the first era. Secondly, it was an external change due to cyber threats becoming more severe both at organizational and individual levels, making every sector of Thai society aware of cyber threats, which was a new type of threat that could cause greater damage to oneself and one's family than any other threat before. The creation of NCSA, to eliminate such dangers, was the expectation, like the light at the end of the tunnel that society was waiting for. With both changes, NCSA had to leap out of the dark corners of the building to show itself as a hero in chasing the thief which causes severe distress to the country and its people. Under the management of Air Vice Marshal Amorn Chomchoey, new Secretary-General of the National Cyber Security Committee, we must quickly adjust our strategy to deal with emerging cyber threats. Reinforcing by defining the DNA of NCSA, so that all employees share the same commitment is the main focus of operations through 4 components:

In order to achieve effective operational goals and aim for success in quickly preventing and eliminating cyber threats to the country and the people, NCSA has adjusted work strategy into 2 main areas in order to be able to allocate resources appropriately and the highest values are:

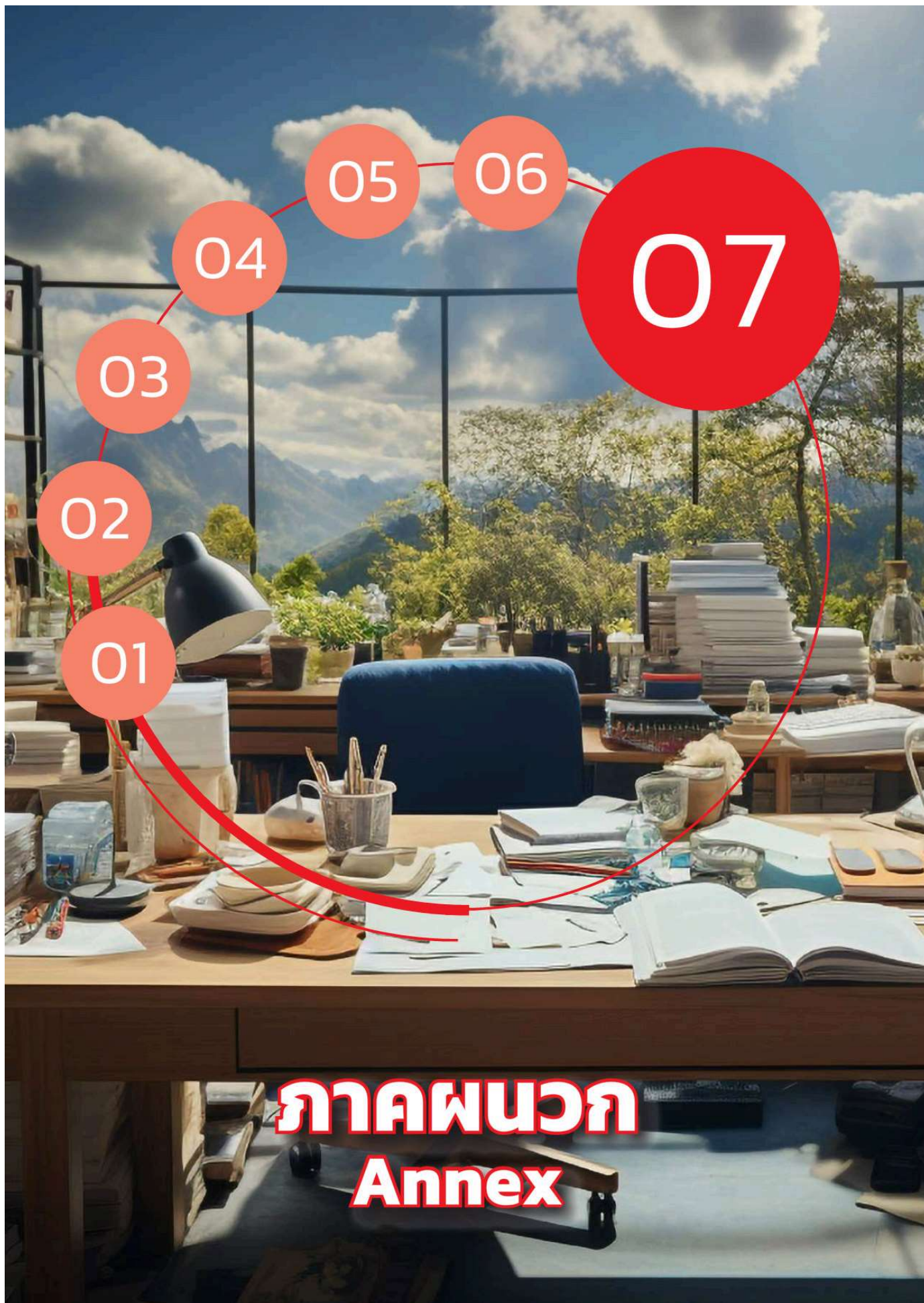
1. Strengthening oneself and one's network

- Strengthen NCSA in every aspect
- Strengthen Regulators, Organizations of Critical Information Infrastructure (CII) and government agencies
- Create awareness and immunity for the people

2. Immediately alerting of dangers and minimizing losses

- Efficient Intelligence
- Destroying the source of cyber threats and eliminating cyber threats quickly and in time
- Restoring damage from cyber threats to return to normal promptly

As a result of its performance in 2023, NCSA successfully prevented and mitigated cyber threats, ensuring the safety and security of the nation and its citizens on a broad scale. The lessons learned from this year's experiences will fortify NCSA for the future, fostering peace and stability while advancing the country's development. This commitment will drive Thailand towards greater progress and prosperity, bringing happiness to all its people.



คำศัพท์ทางไซเบอร์

คำศัพท์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

ภาษาอังกฤษ	ภาษาไทย	ความหมาย / คำจำกัดความ
APT	เอพีที	APT ย่อมาจาก Advanced Persistent Threat คือ การที่ผู้โจมตีฝังตัวอยู่ในระบบของเหยื่อเป็นเวลานานเพื่อเฝ้าดูพฤติกรรมและดักจับข้อมูล
Data Breach	ดาต้าบรีช	การเจาะระบบและขโมยข้อมูลสำคัญออกไปขายหรือเผยแพร่ เช่น การนำข้อมูลส่วนบุคคลของลูกค้าไปขาย หรือการล้วงข้อมูลงานวิจัยเพื่อแข่งขันทางการค้า
Fake Website	เฟค เว็บไซต์	เป็นองค์ประกอบที่ฟิชซิง สร้างขึ้นเพื่อล่อลวงข้อมูลโดยการสร้างเว็บไซต์ที่มีความเหมือนเว็บไซต์จริงมากที่สุดเพื่อให้ผู้ใช้งานหลงกลเข้ามาในระบบ รอให้ผู้ผู้ใช้ใส่ข้อมูลส่วนตัวต่าง ๆ ทำให้ข้อมูลส่วนตัวที่ควรรักษาเป็นความลับ ถูกโจรกรรมข้อมูลไปได้ ซึ่งทำให้ผู้ใช้ได้รับผลกระทบเป็นอย่างมากเพราะข้อมูลอาจถูกนำไปใช้ในทางที่เสียหาย โดยที่เราไม่สามารถหยุดได้เลยเพราะข้อมูลเป็นข้อมูลจริงของผู้ใช้เอง ส่งผลเสียให้กับเหยื่อที่หลงกลเป็นอย่างมาก
Fraud	ฟรูด	คดีฉ้อโกง หมายถึง คดีอาญาที่ผู้กระทำความผิดมีเจตนาแสวงหาประโยชน์โดยมิชอบเอาจากผู้ถูกหลอกลวง โดยหลอกลวงด้วยการแสดงข้อความอันเป็นเท็จ หรือปกปิดข้อความจริงที่ควรบอก ซึ่งการหลอกลวงและปกปิดนั้น ผู้ถูกหลอกลวงต้องเสียทรัพย์สินให้แก่ผู้กระทำความผิด หรือทำให้ผู้ถูกหลอกลวงหรือบุคคลที่สามทำ ถอน หรือทำลายเอกสารสิทธิ นอกจากนี้ ถ้าผู้เสียหายมีจำนวน 1 คนขึ้นไป เช่นนี้เป็นคดีฉ้อโกงประชาชน (Public fraud) ซึ่งเป็นความผิดอันยอมความไม่ได้ ภัยคุกคามประเภทฟรูด หรือการฉ้อโกงหลอกลวง สามารถแบ่งออกได้เป็น 2 ประเภท คือ Phishing (ฟิชซิง) คือการล่อหลอกเหยื่อเข้าหน้าเว็บไซต์ปลอม ซึ่งทำให้ดูคล้ายกับหน้าล็อกอินของเว็บไซต์จริง จุดประสงค์เพื่อขโมยพาสเวิร์ด และนำไปสู่การขโมยข้อมูลอื่น ๆ โดยเฉพาะในเรื่องธุรกรรมทางการเงิน Scam (สแคม) คือการแอบอ้างเพื่ออาศัยผลจากความเข้าใจผิด เช่น การสร้างหน้าเว็บไซต์ปลอมแอบอ้างว่าเป็นเว็บไซต์ของบริการที่มีชื่อเสียง หลอกให้ร่วมเล่นเกมเพื่อชิงรางวัล เพื่อขโมยข้อมูลส่วนบุคคล ซึ่งจะนำไปสู่การปลอมแปลงอื่น ๆ เพื่อผลประโยชน์ของผู้ไม่หวังดีต่อไป
Malware	มัลแวร์	โปรแกรมประสงค์ร้ายที่ถูกเขียนขึ้นมา เพื่อทำอันตรายกับข้อมูลในระบบ เช่น ทำให้เครื่องคอมพิวเตอร์ทำงานผิดปกติ ขโมยหรือทำลายข้อมูลหรืออาจจะเปิดช่องทางให้ผู้ไม่หวังดีเข้ามาควบคุมเครื่องของเราได้

ภาษาอังกฤษ	ภาษาไทย	ความหมาย / คำจำกัดความ
Misconfiguration	มิสคอนฟิกกูเรชั่น	การกำหนดค่าที่ไม่ถูกต้อง หรือไม่เหมาะสมของระบบข้อมูลหรือส่วนประกอบของระบบ ที่อาจนำไปสู่ช่องโหว่หรือจุดอ่อนของระบบ
Penetration Test	เพนิเทรชันเทส	Penetration Test หรือ PenTest เป็นวิธีการประเมินความเสี่ยงด้วยการทดสอบเจาะระบบเพื่อค้นหาจุดอ่อนในการเข้าถึงระบบต่าง ๆ โดยใช้ผู้เชี่ยวชาญ ช่วยให้สามารถประเมินความเสี่ยงของระบบเครือข่ายลูกค้าว่ามีความเสี่ยงตรงจุดใด ซึ่งจะเป็นการทดสอบเจาะระบบในเชิงลึก พร้อมแจ้งผลการทดสอบ และประเมินความเสี่ยงเพื่อเตรียมการป้องกันไว้ก่อน ซึ่งการตรวจหาช่องโหว่นี้เป็นหนึ่งในมาตรการป้องกันภัยคุกคามทางไซเบอร์ที่เหมาะสมสำหรับองค์กรที่ต้องการรักษาความปลอดภัยเป็นพิเศษและจำเป็นต้องตรวจสอบระบบอย่างสม่ำเสมอ
Ransom-ware	แรนซัมแวร์	มัลแวร์เรียกค่าไถ่ เป็นมัลแวร์ที่เข้ารหัสลับข้อมูลในเครื่องเหยื่อ ทำให้ไม่สามารถเข้าถึงข้อมูลได้ และเรียกค่าไถ่จากเหยื่อเพื่อแลกกับการถอดรหัสลับ
Social Engineering	โซเชียล อิงเจเนอริง	วิศวกรรมสังคม เป็นเทคนิคการหลอกลวงโดยใช้หลักการพื้นฐานทางจิตวิทยาเพื่อให้เหยื่อเปิดเผยข้อมูล ซึ่งบางครั้งอาจไม่จำเป็นต้องใช้เทคโนโลยีเข้ามาเกี่ยวข้องเลย ผู้ที่ตกเป็นเหยื่อของ Social Engineering อาจจะตกเป็นเหยื่อโดยความตั้งใจหรือไม่ตั้งใจของผู้ไม่หวังดีก็ได้ กล่าวคือ ถ้าผู้ไม่หวังดีมีเป้าหมายเฉพาะเจาะจง เช่น ต้องการข้อมูลความลับขององค์กรใดองค์กรหนึ่ง เหยื่อในที่นี้ก็จะมักจะเป็นผู้ที่มีสิทธิในการเข้าถึงข้อมูลความลับขององค์กรนั้น แต่หากเป้าหมายของผู้ไม่หวังดีเป็นแบบที่ไม่ได้เจาะจงเหยื่อ เช่น ต้องการรหัสบัตรเครดิต หรือบัญชีผู้ใช้และรหัสผ่านของบริการต่าง ๆ ของใครก็ได้ เหยื่อของผู้ไม่หวังดีนี้จะเป็นใครก็ตามซึ่งหลงเชื่อการหลอกลวงนั้น
Supply Chain Attack	ซัพพลายเชน แอทแทค	การโจมตีไปที่ผู้พัฒนาซอฟต์แวร์ โดยมีจุดประสงค์เพื่อสอดแทรกมัลแวร์ลงในแอปพลิเคชัน ซึ่งจะทำให้ลูกค้าผู้ใช้งานแอปพลิเคชันนั้นตกเป็นเหยื่อได้โดยไม่รู้ตัว เนื่องจากมัลแวร์จะแฝงตัวมาในรูปแบบของแอปพลิเคชันที่องค์กรซื้อใช้งานอยู่แล้ว หรืออาจจะกระจายตัวออกมาในรูปแบบของอัปเดตสำหรับแอปนั้น จึงมีโอกาที่จะหลุดรอดจากการตรวจจับได้สูงกว่าปกติ และสามารถทำงานในเครือข่ายของเป้าหมายได้เสมือนเป็นแอปพลิเคชันดั้งเดิมที่องค์กรไว้วางใจ
Website Defacement	การปลอมแปลงหน้าเว็บไซต์	การลบเจาะระบบเข้าไปเปลี่ยนหน้าเว็บไซต์ แสดงสัญลักษณ์ ใ้อวดความสามารถ หรือความเห็นทางการเมือง
Website Phishing	ฟิชซิง	การหลอกให้เข้าเว็บไซต์ปลอมเพื่อลวงเอาข้อมูลที่สำคัญ เช่น การปลอมเว็บไซต์ธนาคารและส่งอีเมลแจ้งลูกค้าธนาคารให้เข้ามากรอกข้อมูล username และ password ที่เว็บปลอม และข้อมูลที่กรอกจะส่งไปยังมิจฉาชีพ
Vulnerability	จุดอ่อนช่องโหว่	ช่องโหว่หรือจุดบกพร่องด้านระบบความปลอดภัยของคอมพิวเตอร์ โดยเปิดโอกาสให้ระบบข้อมูลอัตโนมัติถูกเจาะในรูปแบบการทำงานทางด้านฮาร์ดแวร์และซอฟต์แวร์ซึ่งสามารถเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ก่อให้เกิดความเสียหายหรือสามารถสร้างภัยคุกคามให้กับองค์กร

รายชื่อคณะกรรมการ

คณะกรรมการจัดทำรายงานผลการดำเนินงานประจำปี พ.ศ. 2566

- | | |
|---|----------------------------|
| 1. เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ | ประธานกรรมการ |
| 2. รองเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ | กรรมการ |
| 3. ผู้ช่วยเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ | กรรมการ |
| 4. ผู้เชี่ยวชาญด้านการจัดการองค์กร | กรรมการ |
| 5. ผู้ทรงคุณวุฒิพิเศษ | กรรมการ |
| 6. ผู้อำนวยการสำนัก/ศูนย์ฯ | กรรมการ |
| 7. ผู้อำนวยการฝ่ายตรวจสอบภายใน | กรรมการ |
| 8. ผู้อำนวยการฝ่ายการคุ้มครองข้อมูลส่วนบุคคล | กรรมการ |
| 9. ผู้อำนวยการฝ่ายพัฒนาองค์กร | กรรมการ |
| 10. ผู้อำนวยการฝ่ายบริหารความเสี่ยง | กรรมการ |
| 11. ผู้อำนวยการสำนักนโยบายยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ | กรรมการและเลขานุการ |
| 12. นางสาวสุกิสรา กูดีธราแม | กรรมการและผู้ช่วยเลขานุการ |
| 13. นางสาวสุวรรณี ขุนทองปาน | กรรมการและผู้ช่วยเลขานุการ |
| 14. นางสาวบัณฑิตย์ พุ่มกุมาร | กรรมการและผู้ช่วยเลขานุการ |
| 15. นายทักษิณ บุญรอด | กรรมการและผู้ช่วยเลขานุการ |

ผู้รวบรวมและสนับสนุนข้อมูล

- | | |
|-----------------------------------|--|
| 1. นายทศพล กลิ่นหอม | 13. นายพงศ์ชินทร์ สกฤตตันศักดิ์ |
| 2. นางอสิตา สุขสว่าง | 14. ว่าที่ ร.ต. หญิง กัญจนารักษ์ ประไพ |
| 3. พันโท ญาณินทร์ สุรพันธ์ไพโรจน์ | 15. นางสาวอรอุมา ธรรมศิริ |
| 4. นายสุนทร ศิริไพศาล | 16. นางสาวรัตนารักษ์ จันทน์นาม |
| 5. ร้อยตรี พีรพัฒน์ สุขเกิด | 17. นางสาวยุภาภรณ์ พุ่มโม่ง |
| 6. นางสาวสิริขวัญ ฉายติลก | 18. นางสาวภาวิณี เครือแก้ว |
| 7. นางสาววัชรภรณ์ จิตรสง่า | 19. นางสาวพรพรรณ มั่นช่วยวงศ์ |
| 8. นางสาวกนกวรรณ พรศุภปัทมา | 20. นายศุภณัฐ รัตนวราหะ |
| 9. นายอดิสร พิมลรัตน์ | 21. นายทรงวุฒิ ทวีแสง |
| 10. นางสาวศุภธรา สุวรรณาคม | 22. นางสาววิษุฒดาวัลย์ แสงบัวแก้ว |
| 11. นางสาวกมลพรรณ คงไข่ | 23. นายพงศธร ปรีวุฒิพงศ์ |
| 12. นางสาวเพชรไพรินทร์ ตันแก้ว | 24. นายกษิต โชคธนกุลชัย |



ช่องทางติดต่อ สกมช.

โทรศัพท์ : 02-142-6888

ที่อยู่ : 120 หมู่ 3 อาคารรัฐประศาสนภักดี
ชั้น 6-7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา
แขวงทุ่งสองห้อง เขตหลักสี่
กรุงเทพมหานคร 10210

Email : saraban@ncsa.or.th



ช่องทาง Social Media NCSA

Facebook : NCSA Thailand

Website : <https://www.ncsa.or.th>

Youtube : @ncsathailand

ช่องทางแจ้งเหตุภัยคุกคามทางไซเบอร์

**ศูนย์ประสานการรักษาความมั่นคงปลอดภัย
ระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT)**

โทรศัพท์ : 02-142-6885 (ติดต่อเวลาทำการ)

ศูนย์แจ้งเหตุภัยคุกคามทางไซเบอร์

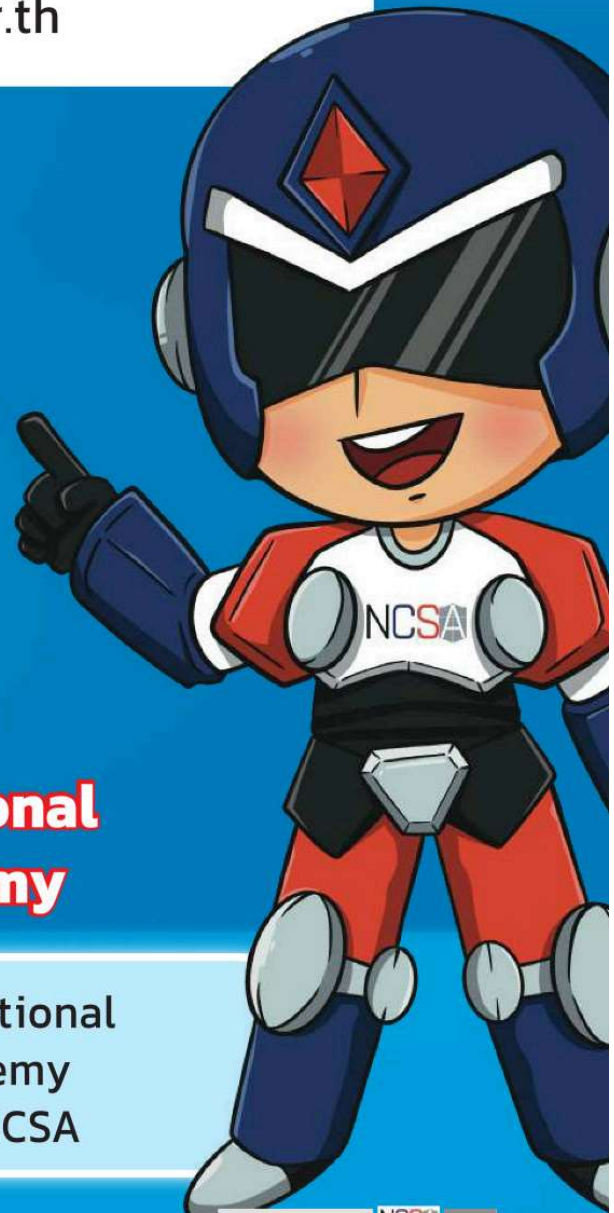
โทรศัพท์ : 02-114-3531 (24 ชั่วโมง)

Email : thaicert@ncsa.or.th

**Thailand National
Cyber Academy**

Facebook : Thailand National
Cyber Academy

Youtube : @THNCABbyNCSA



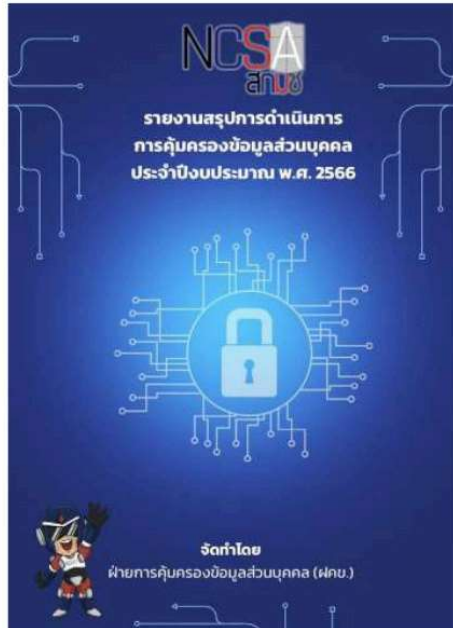
นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคง ปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)



การฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ Thailand National Cyber Exercise 2023



รายงานสรุปการดำเนินการการคุ้มครองข้อมูลส่วนบุคคล ประจำปีงบประมาณ พ.ศ. 2566



รายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่มีผลกระทบอย่างมีนัยสำคัญ ประจำปี 2566 (ห้วง 1 ตุลาคม 2565 - 30 กันยายน 2566)



เรียนฟรี! ใ้ใบ CERTIFICATE!

FREE

NCSA
สกนช
สำนักงานคณะกรรมการการ
อาชีวศึกษา
ศูนย์พัฒนาความปลอดภัยไซเบอร์แห่งชาติ

THNCA
Thailand National Cyber Academy
ศูนย์พัฒนาความปลอดภัยไซเบอร์แห่งชาติ

สำนักงานคณะกรรมการการอาชีวศึกษา
ศูนย์พัฒนาความปลอดภัยไซเบอร์แห่งชาติ

CYBER KNOWLEDGE CENTER

TEL. 02 502 7831

"คลังความรู้ด้านไซเบอร์"

สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ส่งเสริมสังคมการเรียนรู้และเผยแพร่คลังความรู้ด้านไซเบอร์ เพื่อพัฒนาทักษะและการเรียนรู้ได้อย่างไร้ขีดจำกัด เข้าใจถึงความสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์

SCAN ME

LINK : [HTTPS://LINKTR.EE/THNCA](https://linktr.ee/THNCA)

สแกนได้แล้ววันนี้
เรียนรู้ได้อย่างไร้ขีดจำกัด

พลอากาศตรี อมร ชมเชย

เลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

- ✓ CYBERSECURITY AWARENESS
- ✓ CYBERSECURITY SKILL
- ✓ อุุ่นใจไซเบอร์ AIS มีคอร์สทั้งหมดมากถึง 25 คอร์ส

140 NCSA สกนช รายงานประจำปี 2566

สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โทรศัพท์ 0-2502-7831 | อีเมล : academic@ncsa.or.th

ยันต์กันภัยไซเบอร์

“เตือนสติ เตือนใจ

ไม่ตกเป็นเหยื่อของมิจฉาชีพ”







PR ACTIVE TECTI^N

X TOTAL DEFENSE
CYBER COORDINATION OFFICE





E-BOOK



จัดทำโดย สำนักงานคณะกรรมการรักษา
ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
พิมพ์ครั้งที่ 1 จำนวน 800 เล่ม
มีนาคม 2567
พิมพ์ที่ บริษัท ศูนย์การพิมพ์แก่นจันทร์ จำกัด
ปีที่พิมพ์ 2567
ISBN 978-616-94218-1-8