

รายงานประจำปี 2565

Annual Report 2022



คำนำ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ สกมช. ได้จัดทำรายงานผลการดำเนินงานประจำปี 2565 ซึ่งเป็นไปตามมาตรา 39 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่ได้บัญญัติให้ สกมช. จัดทำรายงานผลการดำเนินงานประจำปีเสนอคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและนายกรัฐมนตรี ซึ่งเป็นรัฐมนตรีรักษาการตามพระราชบัญญัตินี้ดังกล่าว ภายในหนึ่งร้อยแปดสิบวันนับแต่วันสิ้นปีบัญชี และเผยแพร่รายงานนี้ต่อสาธารณชน

เพื่อให้เป็นไปตามที่กฎหมายกำหนด สกมช. ได้จัดทำรายงานผลการดำเนินงานประจำปี 2565 โดยมีสาระสำคัญ ประกอบด้วย ผลงานประจำปีงบประมาณ พ.ศ.2565 รายละเอียดของงบการเงินที่ผู้สอบบัญชีให้ความเห็นชอบแล้ว รายงานการประเมินผลการดำเนินงานของสำนักงานที่ประเมินโดยบุคคลภายนอก และปัญหา/อุปสรรคการดำเนินงานที่ผ่านมาและข้อเสนอแนะดังรายละเอียดที่ปรากฏอยู่ในรายงานฉบับนี้ ซึ่งนอกจากจะมีวัตถุประสงค์เพื่อเสนอต่อคณะกรรมการและรัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้ดังกล่าวแล้วยังได้เผยแพร่ให้ประชาชน นักเรียน นิสิต นักศึกษา บริษัท ห้างร้าน หน่วยงานทั้งภาครัฐและเอกชน รวมทั้งสาธารณชนทั่วไปได้รับทราบผลการดำเนินงานประจำปี 2565 ของ สกมช. ตามที่กฎหมายกำหนดไว้ สกมช. หวังเป็นอย่างยิ่งว่ารายงานฉบับนี้จะเป็นแหล่งรวบรวมข้อมูลที่สำคัญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในโลกยุคดิจิทัล ให้แก่ผู้สนใจ เช่น นักวิชาการ นักศึกษา สื่อมวลชน และประชาชนทั่วไป เพื่อสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์หรือเพื่อนำไปใช้ประโยชน์ตามที่เห็นสมควรต่อไป

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
มีนาคม 2566



Introduction

The National Cyber Security Agency (NCSA) has prepared the Annual Report 2022 under Article 39 of the Cyber Security Act B.E. 2562 (2019), by which the NCSA is required to prepare the annual report, submit it to the Committee and the Cabinet within 180 days from the fiscal year-end, and disclose it to the public.

The NCSA has prepared the 2022 Annual Report to comply with the law. The main content includes summary of NCSA performance in the fiscal year 2022, financial report by the auditor, report of NCSA performance evaluated by a third party, obstacles from previous implementations, and recommendations. Aside from being proposed to the Committee and relevant ministers, the report will also be disclosed to the companies, stores, private and public organizations, and the general public. We genuinely hope that this report will be a beneficial source of data regarding cyber security in the digital world to those interested, such as academics, students, media, and the general public, to raise awareness of cyber threats or make use of the information in this report.

National Cyber Security Agency.
March, 2023.



สารบัญ

Table of content

4

สารนายกรัฐมนตรีและประธานคณะกรรมการ

Messages from the Prime Minister and Chairman of NCSC

12

สารผู้ตรวจประเมิน

Message from the Auditor

14

คณะกรรมการ

การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

National Cyber Security Committee (NCSC)

16

คณะกรรมการ

กำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)

Cybersecurity Regulating Committee (CRC)

18

คณะกรรมการบริหาร

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)

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

20

บทสรุปผู้บริหาร

Executive Summary Report

27

โครงสร้างองค์กร

Organizational Structure

30

ผู้บริหารสำนักงานคณะกรรมการ

การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

Executives of National Cyber Security Agency (NCSA)

32

เกี่ยวกับ สกมช.

About NCSA

38

รายงานผลการดำเนินงานประจำปี

Summary of NCSA Performance in 2022

101

รายงานการเงิน

Financial Report

123

รายงานการประเมินผลการดำเนินงาน

ของสำนักงานที่ประเมินโดยบุคคลภายนอก

Summary Report of the NCSA Performance Evaluation
by Third Party

144

คำจำกัดความ

Definitions



สารนายกรัฐมนตรี



เทคโนโลยีดิจิทัลมีบทบาทสำคัญต่อการดำเนินชีวิตของพี่น้องประชาชนในปัจจุบัน และมีแนวโน้มความสำคัญเพิ่มมากขึ้นในอนาคต โดยที่ผ่านมามีพี่น้องประชาชนต้องปรับเปลี่ยนวิธีการดำเนินชีวิตสู่รูปแบบวิถีใหม่ (New Normal) อันเป็นผลจากสถานการณ์การแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 และผลกระทบจากการเปลี่ยนองค์กรสู่ดิจิทัล (Digital Transformation) แม้ว่าเทคโนโลยีและนวัตกรรมต่างๆ ที่ทันสมัยจะช่วยให้เกิดความสะดวกสบายและความคล่องตัวในการทำธุรกรรมและธุรกรรมต่างๆ แต่ขณะเดียวกันก็เป็นช่องทางในการก่ออาชญากรรมทางเทคโนโลยี ซึ่งเป็นความเสี่ยงที่อาจก่อให้เกิดความเสียหายแก่ชีวิตและทรัพย์สินของพี่น้องประชาชน รัฐบาลให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยได้ขับเคลื่อนนโยบายและแผนปฏิบัติการว่าด้วยความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570) เพื่อใช้เป็นกรอบแนวทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย รวมทั้งมุ่งเน้นบูรณาการความร่วมมือของทุกภาคส่วนทั้งภายในประเทศและระหว่างประเทศ ซึ่งจะช่วยให้บริหารจัดการเป็นไปอย่างมีประสิทธิภาพและเป็นเอกภาพ

ผมขอชื่นชมสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่มีส่วนสำคัญในการเสนอแนะและสนับสนุนจัดทำ

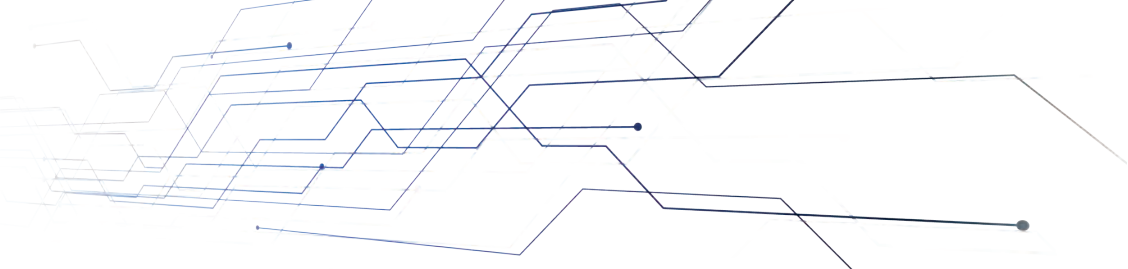
นโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ และเตรียมความพร้อมในการป้องกันภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจากปัจจัยภายในหรือภายนอกประเทศ ซึ่งผมหวังเป็นอย่างยิ่งว่ารายงานผลการดำเนินงานฉบับนี้จะเป็นประโยชน์แก่หน่วยงานที่เกี่ยวข้องและสร้างความเข้าใจให้แก่พี่น้องประชาชนเกี่ยวกับการรักษาความมั่นคงของชาติ ซึ่งมีส่วนสำคัญที่ทำให้สังคมมีความสงบเรียบร้อย และพี่น้องประชาชนมีความปลอดภัยอย่างยิ่งยืน

ในโอกาสนี้ ผมขออาราธนาคุณพระศรีรัตนตรัยและสิ่งศักดิ์สิทธิ์ทั้งหลายที่ทุกท่านเคารพนับถือ อีกทั้งพระบารมีของพระบาทสมเด็จพระเจ้าอยู่หัว และสมเด็จพระนางเจ้าพระบรมราชินี ได้โปรดดลบันดาลประทานพรให้ผู้บริหาร ข้าราชการ เจ้าหน้าที่ และผู้ที่มีส่วนเกี่ยวข้อง กับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติทุกคน ประสบแต่ความสุข ความเจริญ มีกำลังกาย กำลังใจ ที่เข้มแข็งมีสุขภาพพลานามัยแข็งแรงสมบูรณ์ และสัมฤทธิ์ผลในสิ่งอันพึงปรารถนาทุกประการ โดยทั่วกัน

waiok

(ประยุทธ์ จันทร์โอชา)

นายกรัฐมนตรี



Message from the Prime Minister

Technology plays a key role in people's livelihood today and is likely to be more crucial in the future. For the past few years, Thai people have adjusted to the new normal due to the COVID-19 pandemic and digital transformation. While technology and innovation facilitate daily activities and business transactions, they also leave a gap for technological crimes which threaten the lives and properties of the public. The Government places an emphasis on cybersecurity by pushing the Policy and Action Plan on Cyber Security (2022 – 2027) as the guideline for cybersecurity in Thailand. We also seek collaboration among relevant parties locally and internationally to ensure effective and uniform management.

I would like to express my admiration for the committed effort of the National Cyber Security Agency regarding their recommendations and supports for the national policies, measures, and guidelines for cybersecurity and preparation for internal and external cyber threats. I genuinely hope

that this annual report will benefit relevant agencies and establish an understanding of national security, which significantly contributes to social peace and order for the people.

On this occasion, I would like to pray to our Lord Buddha, holy beings, the King, and the Queen to give their best wishes and blessings to directors and staffs at the Office of the National Cyber Security Committee, along with their family members. May you find happiness, good health, and a good spirit.

General Prayuth Chan-ocha,
Prime Minister.



สารรองนายกรัฐมนตรี

ปฏิบัติหน้าที่ประธานกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

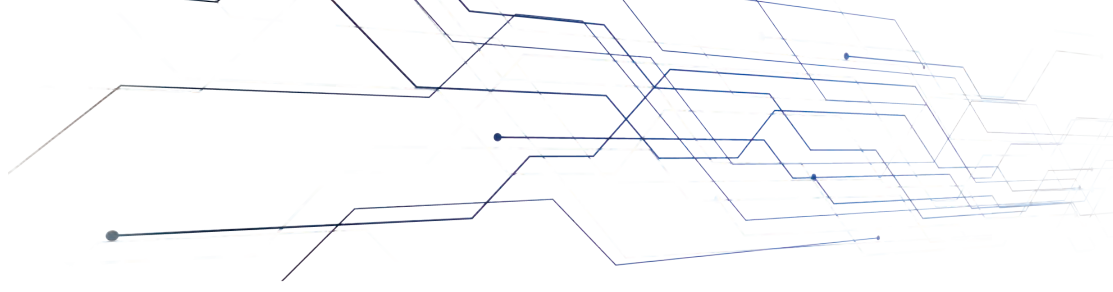
ภัยคุกคามทางไซเบอร์ถือเป็นภัยคุกคามที่ใกล้ตัวของพี่น้องประชาชน และส่งผลกระทบต่อความมั่นคงของชาติ ปัจจุบันนวัตกรรมและเทคโนโลยีสมัยใหม่ได้เข้ามามีบทบาทต่อการดำรงชีวิตประจำวันของพี่น้องประชาชนมากยิ่งขึ้น รัฐบาลมีความห่วงใยพี่น้องประชาชนทุกคน ที่อาจได้รับผลกระทบและได้รับความเสียหายจากภัยคุกคามทางไซเบอร์ จึงได้จัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่รับผิดชอบและเตรียมความพร้อมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมทั้งให้ความสำคัญกับการยกระดับการรักษาความมั่นคงปลอดภัยของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีประสิทธิภาพ และบูรณาการทำงานร่วมกับหน่วยงานที่เกี่ยวข้องเพื่อขับเคลื่อนงานและการปฏิบัติตามนโยบายและแผนปฏิบัติการว่าด้วยความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570) รวมทั้งส่งเสริมและขับเคลื่อนนโยบายและแผนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้ทุกภาคส่วนนำไปใช้เป็นแนวทางในการส่งเสริมสร้างระบบการเฝ้าระวัง และตอบสนอง

ต่อภัยคุกคามทางไซเบอร์ให้กับหน่วยงานเพื่อให้ระบบการให้บริการแก่พี่น้องประชาชนเกิดเสถียรภาพและปลอดภัยสูงสุด โดยมีเป้าหมายเพื่อลดความเสี่ยงจากการคุกคามทางไซเบอร์ ทั้งภายในและภายนอกประเทศที่ส่งผลกระทบต่อความมั่นคงของรัฐ เศรษฐกิจ และความสงบเรียบร้อยภายในประเทศ

ผมหวังอย่างยิ่งว่ารายงานผลการดำเนินงานประจำปี 2565 ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับนี้ จะเป็นประโยชน์ต่อทุกภาคส่วนในการนำไปใช้ประกอบการกำหนดนโยบาย แผนและการนำไปปฏิบัติเพื่อป้องกัน รับมือเพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมทั้งเป็นการเผยแพร่ความรู้ให้แก่พี่น้องประชาชน เพื่อจะได้ร่วมป้องกันภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อไป

วเลอ

(ประวิตร วงษ์สุวรรณ)
รองนายกรัฐมนตรี



Message from the Deputy Prime Minister

Acting Chairman of the National Cyber Security Committee (NCSC)

Cyber threats are very close to our people and compromise national security. Today, innovation and technology have become more crucial for the daily livelihood of people. With great concern for the impact and damage from cyber threats, the Government established the National Cyber Security Agency (NCSA) as the main agency in charge of preparing the country for cyber threats and promoting cyber security of critical information infrastructures to be effective. NCSA will also collaborate with other agencies to expedite and implement the Policy and Action Plan on Cyber Security (2022 – 2027) and encourage other agencies to adopt it to monitor and address cyber threats to ensure maximum reliability and security for the public. The goal is to

minimize cyber threats from inside and outside the country that compromise the security of the state, the economy, and public order.

I sincerely hope that the 2022 annual report of the NCSA will be useful for any organization to formulate policies and measures to prevent, address, and minimize cyber threats, and raise awareness of cyber threats among the general public to help prevent cyber threats effectively in the future.

General Prawit Wongsuwan,

Deputy Prime Minister,
Acting Chairman of NCSC.



สารรัฐมนตรีว่าการกระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)
และประธานกรรมการบริหารสำนักงานคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)

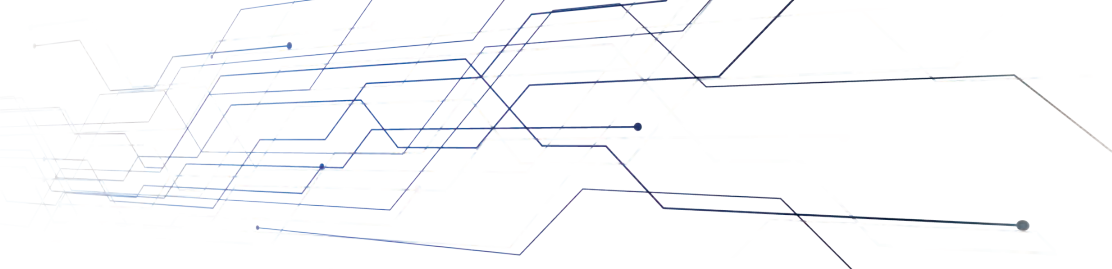


ในปัจจุบันประเทศไทยเรามีการพัฒนาระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายเพื่อการรับส่งข้อมูลที่สำคัญในทุกกระบวนการทำงาน ไม่ว่าจะเป็นการดำเนินงานตามนโยบายที่สำคัญของรัฐบาลการดำเนินงานทั้งภาครัฐและภาคเอกชนล้วนแล้วแต่มีความเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายที่สำคัญในทุกกระบวนการ ดังนั้นการรักษาความมั่นคงปลอดภัยทางไซเบอร์จึงถือว่าเป็นหัวใจสำคัญที่จะทำให้ระบบต่าง ๆ ที่ใช้กันอยู่จนเป็นกิจวัตรประจำวันนั้นมีความเสถียรและยังคงสถานะใช้งานได้และมีความปลอดภัย รวมทั้งมีความพร้อมที่จะรับมือกับภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ รวมถึงการสร้างความตระหนักให้กับประชาชนคนไทยทุกคนให้รู้เท่าทันภัยคุกคามทางไซเบอร์ เพื่อจะได้เกิดความรู้สึกลปลอดภัยและมีความมั่นใจที่จะใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย รวมทั้งไม่ตกเป็นเหยื่อของเหล่ามิจฉาชีพ การกิจที่สำคัญที่กล่าวมานี้ รัฐบาลได้ให้ความสำคัญกับเรื่องความปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายของพี่น้องประชาชน จึงได้จัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อที่จะได้เป็นหน่วยงานหลักที่รับผิดชอบการรักษา

ความมั่นคงปลอดภัยทางไซเบอร์ให้แก่ประเทศไทย โดยอาศัยความร่วมมือจากทุกภาคส่วนในการที่จะเฝ้าระวังและตอบสนองภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ ทั้งจากภายในและภายนอกประเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศระบบเครือข่ายของประเทศรองรับการใช้งานและการเติบโตของเศรษฐกิจของประเทศให้ก้าวไปสู่โลกดิจิทัลอย่างสมบูรณ์และปลอดภัย ผมจึงขอเป็นกำลังใจให้กับพนักงานและเจ้าหน้าที่ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติทุกท่านในอันที่จะทำงานอย่างทุ่มเทต่อไป

(นายชัยวุฒิ ธนาคมานุสรณ์)

รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม



Message from the Minister of Digital Economy and Society

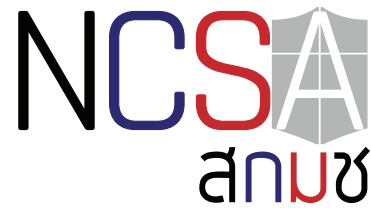
Chairman of the Cybersecurity Regulating Committee (CRC)
And Chairman of the Committee Managing the Office
of the National Cybersecurity Committee (CMO)

At present, Thailand has been developing information technology systems and networks to transmit information at all levels. Whether it is the implementation of important policies of the government, operations in both the public and private sectors are all involved in the use of information technology systems and critical networks in all processes. Therefore, cybersecurity is the key to make systems that are used in daily routines stable and remain functional and secure as well as to be dealing with cyber threats in various forms, including raising Thai people awareness in cyber threats and to feel safe and confident to use information technology systems and networks as well as not being victim. The important tasks mentioned above, the government has given important that Thai people security use information technology systems and networks Therefore, the National Cyber Security Agency (NCSA) was established as agency which was under the

Security Act. To become the main agency responsible for maintaining cyber security for Thailand by relying on the cooperation of all sector to look after and responding every form of cyber threats. The information technology system and network system can be used to support growth of the country economy moving toward the digital world completely and securely. I would like to encourage all employees and officers of the Nation Cyber Security Agency (NCSA) to continue to keep hard working.

Mr. Chaiwut Thanakamanusorn

Minister of Digital Economy Society,
Chairman of CRC and Chairman of CMO.



สารเลขาธิการ

คณะกรรมการ

การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ทบาทของ สภามช. ในปีงบประมาณ 2565 ซึ่งเป็นปีที่ 2 ของการจัดตั้ง สภามช. และเป็นปีที่ 2 ที่ผมดำรงตำแหน่งเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีความท้าทายในหลายมิติ ปรากฏภัยคุกคามทางไซเบอร์เพิ่มมากขึ้นในทุกภาคส่วน ไม่ว่าจะเป็นหน่วยงานภาครัฐ หรือภาคเอกชน โดยเฉพาะภัยคุกคามทางไซเบอร์ในลักษณะการหลอกลวงกับประชาชนโดยตรงนับวันจะทวีความรุนแรงมากขึ้นอย่างเห็นได้ชัด ประชาชนถูกมิจฉาชีพหลอกลวงในหลายช่องทางและหลายวิธี ทำให้สูญเสียทรัพย์สินเงินทองจำนวนมากในแต่ละวัน ซึ่ง สภามช. ก็มีได้ตั้งนอใจ ได้ดำเนินการในหลายรูปแบบ เพื่อประสานงานกับหน่วยงาน ที่เกี่ยวข้องในการป้องกันภัยด้านนี้ รวมทั้งการให้ความรู้และความตระหนักรู้กับประชาชนให้รู้เท่าทันภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในปัจจุบัน เพื่อป้องกันมิให้ตนเองต้องตกเป็นเหยื่อของมิจฉาชีพในเรื่องนี้ และด้วยความทุ่มเทในการทำงานอย่างหนักของพนักงานและลูกจ้างของ สภามช. ในรอบปีที่ผ่านมา ทำให้ สภามช. ได้มีส่วนร่วมในการป้องกันและลดระดับความร้ายแรงของภัยคุกคามทางไซเบอร์ลงได้อย่างมาก แม้จะมีข้อจำกัดอยู่บ้างในเรื่องกำลังคนและอุปกรณ์ เนื่องจาก 2 ปี แรกของการจัดตั้ง สภามช. ยังมีปัญหาด้านการขาดแคลนงบประมาณเป็นปัญหาใหญ่ที่ต้องแก้ไขต่อไป

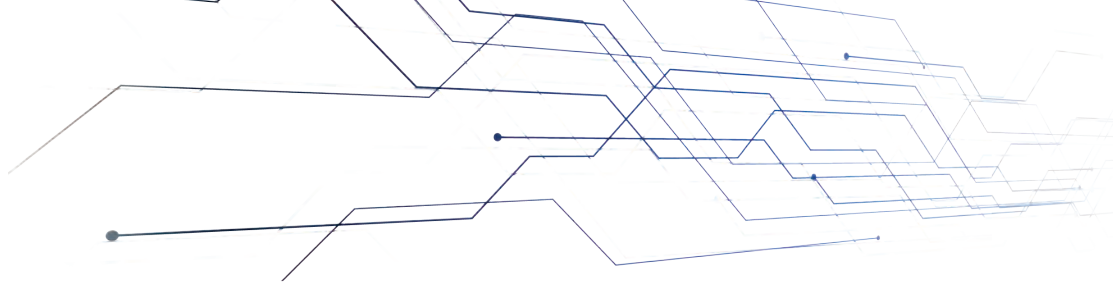
แม้ว่าการดำรงตำแหน่งเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติของ ผมจะยุติลงในสิ้นเดือนกันยายน 2565 ตามวาระการดำรงตำแหน่งที่ พ.ร.บ. การรักษาความ

มั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดไว้ แต่งานของ สภามช. ยังคงต้องดำเนินต่อไปเพื่อสร้างความปลอดภัยทางไซเบอร์ ให้กับประเทศชาติและประชาชน ซึ่งภารกิจดังกล่าวนี้ ถือเป็นพันธะสัญญาของพนักงานและลูกจ้าง ของ สภามช. ทุกคน ที่จะต้องเร่งทำงานอย่างหนัก เพื่อความปลอดภัยของประเทศชาติและความสงบสุขของประชาชนคนไทยทุกคน การผลักดันให้คณะรัฐมนตรีให้ความเห็นชอบนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) จะก่อให้เกิดการบูรณาการความร่วมมือของทุกภาคส่วนในการแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์ของประเทศอย่างเป็นรูปธรรม ซึ่งผมมีความเชื่อมั่นและมั่นใจว่า ผู้บริหาร พนักงาน และลูกจ้าง ของ สภามช. ทุกคน จะปฏิบัติหน้าที่อันยิ่งใหญ่นี้ให้บรรลุผลสำเร็จและได้รับการยอมรับ ในขีดความสามารถและประสิทธิภาพ การปฏิบัติงานทั้งในระดับประเทศและในระดับนานาชาติ โดยมีเป้าหมายสุดท้ายร่วมกันคือ ป้องกันและขจัดภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อประชาชนคนไทยให้ได้โดยเร็ว

พลเอก

(ดร.ปรัชญา เฉลิมวัฒน์)

เลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ



Message from the Secretary-General of National Cyber Security Committee

In the fiscal year 2022, it was the second year after the establishment of the National Cyber Security Agency (NCSA) and the second year as my service as the Secretary - General of the National Cyber Security Committee, there have been challenges in several dimensions. We have faced with more cyber threats in all sectors, including public and private organizations. In particular, direct scamming to the public has been increasingly severe. People have been deceived by scammers in many different ways and through different channels, causing the loss of a large amount of money and assets each day. Concerned by the situation, the NCSA has taken several actions, including coordinating with relevant agencies to protect the citizens from the threats, educating the public, and raising awareness of cyber threats so that they do not become a victim. Thanks to the dedication of the NCSA officers and employees last year, the NCSA has prevented and mitigated the level of cyber threats significantly despite the limitations of human resources and tools. It should be noted that, after two years of establishment, the NCSA is still in

short of the budget, which requires further improvements.

Although my role as the Secretary - General of NCSC will be over at the end of September 2022 according to the term of position specified by the Cyber Security Act B.E. 2562, the work of the NCSA must continue to create cyber security for the nation and the people. This mission is the commitment of all NCSA staffs and employees to work hard for the safety of the nation and the peace of all Thai people. Pushing the Cabinet to approve Policies and Action Plans on Cyber Security (2022 - 2027) will lead to the cooperation from all sectors in solving cyber security problems of the country in a concrete manner. I am confident that all NCSA executives, employees, and officers will perform this great job to achieve and gain recognition for their competence and performance both locally and internationally, with the ultimate goal of preventing and eliminating cyber threats from the Thai people successfully.

General Dr. Prachya Chalermwat,
Secretary-General of the National Cyber Security Agency.



WIN
TOGETHER

สารพัตรวบรวม

ในปี 2565 ที่ผ่านมานั้น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งจัดตั้งขึ้นตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 นั้นมีผลงานโดดเด่นจำนวนมาก ทั้งการจัดทำนโยบาย/แผน/กฎหมาย/กฎระเบียบ/ประกาศ/มาตรการ/มาตรฐานที่สนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศที่ กกม. และ กมช. พิจารณาให้ความเห็นชอบ จำนวน 6 เรื่อง การฝึกอบรมขีดความสามารถทางไซเบอร์ ระดับประเทศ พร้อมหนังสือคู่มือการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ THAILAND'S NATIONAL CYBER EXERCISE 2022 เพื่อเตรียมให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง มีความรู้ความเข้าใจเพิ่มมากขึ้นเกี่ยวกับการรับมือภัยคุกคามทางไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีการยก (ร่าง) แนวทางการประเมินความเสี่ยงต่อภัยคุกคามไซเบอร์ของประเทศจำนวน 3 ฉบับ และ (ร่าง) แนวทางการประเมินความเสี่ยงต่อภัยคุกคามไซเบอร์ของประเทศจำนวน 3 ฉบับ รวมถึงมีการจัดทำนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570) ที่ได้รับความเห็นชอบจากมติ ครม. เมื่อวันที่ 20 กันยายน 2565

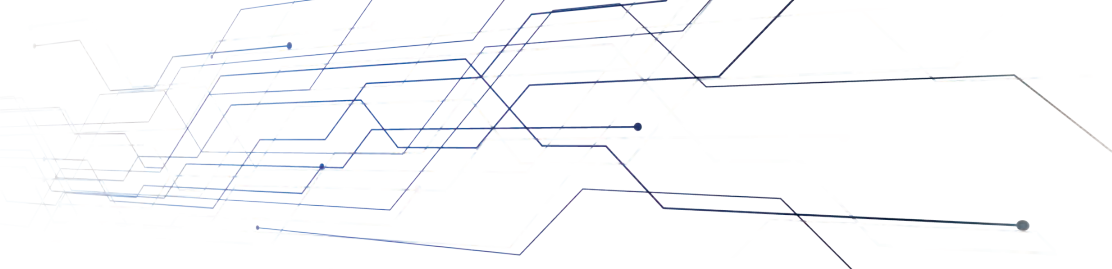
จากแนวทางการประเมินองค์กรมหาชน ประจำปีงบประมาณ พ.ศ.2565 ที่พิจารณา

จาก 4 องค์ประกอบคือ ด้านประสิทธิภาพ ด้านประสิทธิผล ด้านประสิทธิภาพและความคุ้มค่าในการดำเนินงาน ด้านศักยภาพขององค์การมหาชน และ ด้านการควบคุมดูแลกิจการของคณะกรรมการ องค์การมหาชนได้คะแนนรวมอยู่ที่ 91.83 จัดอยู่ในระดับดีมาก แม้จะยังมีข้อเสนอให้ปรับปรุงระบบบริหารจัดการองค์กรสู่ระบบราชการ 4.0 (PMQA 4.0) และองค์กรสมรรถนะสูง (High Performance Organization) รวมถึงให้ความสำคัญกับการนำเทคโนโลยีดิจิทัลมาใช้ในการปฏิบัติงานตามแผนปฏิบัติการดิจิทัลระยะ 5 ปีของ สกมช. และเพิ่มประสิทธิภาพในการประสานงานระหว่างหน่วยงานรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ตามผลการสำรวจความพึงพอใจจากผู้มีส่วนได้ส่วนเสียของ สกมช.

เช่นเดียวกับปีที่ผ่านมา คะแนนผลการประเมินองค์กรที่ระดับ “ดีมาก” แม้จะมีข้อจำกัดด้านการบริหารจัดการและงบประมาณ คงเป็นสัญญาณที่ดีว่า สกมช. จะสามารถเป็นผู้นำในการขับเคลื่อนการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ของประเทศอย่างมีประสิทธิภาพ พร้อมตอบสนองต่อภัยคุกคามไซเบอร์ในทุกมิติตามวิสัยทัศน์ที่องค์กรได้กำหนดไว้อย่างยั่งยืน

(นายอดิษฐ์ กุญชร ณ อุตยา)

กรรมการผู้จัดการ บริษัท วันทูเทเตอร์ จำกัด



Message from the Auditor

In 2022, the National Cyber Security Agency, established by virtue of the Cyber Security Act, B.E. 2562, had several outstanding achievements. For example, the National Cyber Security Committee (NCSC) and the Cybersecurity Regulating Committee (CRC) have approved six policies, plans, laws, regulations, notifications, measures, and standards that support cyber security of the country. Some cyber capability training sessions have been organized. The manual for Thailand National Cyber Exercise 2022 was established to prepare government agencies, regulatory agencies, critical information infrastructure agencies, and other relevant agencies to understand better how to address cyber threats according to the Cyber Security Act, B.E. 2562. Three national guidelines for assessing cyber threats have been drafted. The Policies and Action Plans on Cyber Security (2022 - 2027) have been approved by the Cabinet on 20th September 2022.

The guideline for evaluating the performance of public organizations for the fiscal year 2022 involves four elements: effectiveness, efficiency, the capability of a public organization, and corporate governance of the board of a public organization. The NCSA received a score of 91.83, which

was at a very good level. However, there are recommendations for improvement on the management toward Public Sector Management Quality Award 4.0 (PMQA 4.0), the High-Performance Organization, emphasising on application of digital technology according to the five-year digital action plan of the NCSA, the efficient coordination between the public and private organization in response to and addressing cyber threats according to the satisfactory survey from stakeholders.

Like the previous year, the evaluation score remained at a “very good level” despite limitations on management and the budget. This is a good sign that the NCSA will be the leader in improving national cyber security effectively and be highly responsive to cyber threats in all dimensions as specified in the vision of the agency in a sustainable manner.

Mr. Adisai Kunjara Na Ayudhya,
Managing Director of Win Together Co., Ltd.

คณะกรรมการ การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

National Cyber Security Committee (NCSC)



พลเอก ประวิตร วงษ์สุวรรณ
รองนายกรัฐมนตรี
ปฏิบัติหน้าที่ประธานกรรมการ
General Prawit Wongsuwan
Deputy Prime Minister Acting Chairman

กรรมการโดยตำแหน่ง Committees by Position

พลเอก ชัยชาญ ช้างมงคล
รัฐมนตรีช่วยว่าการกระทรวงกลาโหม
General Chaichan Chanmongkon
Deputy Prime Minister of Defense



**ศาสตราจารย์พิเศษ
วิศิษฐ์ วิศิษฐ์สรอรรถ**
ปลัดกระทรวงยุติธรรม
Adjunct Professor Wisit Wisitsora-at
Permanent Secretary, Ministry of Justice



นายชัยวุฒิ ธนาคมานุสรณ์
รัฐมนตรีว่าการกระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม
Mr. Chaiwut Thanakamanusorn
Minister of Digital Economy and Society



พลตำรวจเอก สุวัฒน์ แจ้งยอดสุข
ผู้บัญชาการตำรวจแห่งชาติ
Police General Suwat Jangyodsuk
Commissioner General, Royal Thai Police



นายกฤษฎา จีนะวิจารณะ
ปลัดกระทรวงการคลัง
Mr. Kritsada Chinavicharana
Permanent Secretary, Ministry of Finance



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



พลเอก ดร.ปรัชญา เฉลิมวัฒน์
เลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
กรรมการและเลขานุการ
General Dr. Prachya Chalermwat
Secretary-General, National Cyber Security Committee
Committee and Secretary

กรรมการผู้ทรงคุณวุฒิ Honorary Committees

ดร.ปริญญ์ หอมเอนก

ด้านการรักษาความมั่นคง
ปลอดภัยไซเบอร์

Dr. Prinya Hom-aneek

Expert Committee on Cyber Security



นายไพบูลย์ อมรภิญโญเกียรติ

ด้านกฎหมาย

Mr. Paiboon amonpinyokeat

Expert Committee on Legal Affairs



พลเอก มโน บุชเกษม

ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

General Mano Nuchkasem

Information Technology and
Expert Committee on Communications



นายวิเชฐ ตันติวานิช

ด้านการเงิน

Mr. Vichate Tantiwanich

Expert Committee on Finance



พันตำรวจเอก ญาณพล ยั่งยืน

ด้านวิศวกรรมศาสตร์

Police Colonel Yanpol Yungyuen

Expert Committee on Engineering



นายแพทย์บดินทร์ ทรัพย์สมบูรณ์

ด้านสาธารณสุข

Dr. Bordin Sapsomboon

Expert Committee on Public Health



รองศาสตราจารย์

ดร.ปณิธาน วัฒนายากร

ด้านความสัมพันธ์ระหว่างประเทศ

Associate Professor

Dr. Panitan Wattanayagorn

Expert Committee on International Relations



คณะกรรมการ กำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กคม.)

Cybersecurity Regulating Committee (CRC)

กรรมการโดยตำแหน่ง Committees by Position





นายชัยวุฒิ ธนาคมานุสรณ์
รัฐมนตรีว่าการกระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม
Mr. Chaiwut Thanakamanusorn
Minister of Digital Economy and
Society Chairman

กรรมการผู้ทรงคุณวุฒิ Honorary Committees

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



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

ดร. พันธุ์ศักดิ์ ศรีรัชตพงษ์
ด้านเทคโนโลยีสารสนเทศ
Dr. Pansak Sirirattaphong
Expert Committee on information and
Communication Technology



ดร. รอม หิรัญพุกษ์
ด้านวิทยาศาสตร์หรือด้านวิศวกรรมศาสตร์
Dr. Rom Hiranpruk
Expert Committee on Science or Engineering



พลเอก ดร.ปรัชญา เฉลิมวัฒน์
เลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
กรรมการและเลขานุการ
General Dr. Prachya Chalermwat
Secretary-General, National Cyber Security Committee
Committee and Secretary

คณะกรรมการบริหาร สำนักงานคณะกรรมการ การรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)

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

นายชัยวุฒิ ธนาคมานุสรณ์
รัฐมนตรีว่าการกระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม
Mr. Chaiwut Thanakamanusorn
Minister of Digital Economy and
Society Chairman



กรรมการโดยตำแหน่ง Committees by Position

นางสาวอัจฉรินทร์ พัฒนพันธ์ชัย
ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
Ms. Ajarin Pattanapanchai
Permanent Secretary,
Ministry of Digital Economy and Society



นายกิตติพงษ์ มหารัตนาวงศ์
ผู้ช่วยเลขาธิการ ก.พ.
Mr. Kitipong Maharatanawongs
Assistant Secretary-General
Office of the Civil Service Commission

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



นางสาวสุนทรี สุภาสงวน
รองเลขาธิการ ก.พ.ส.
Ms. Soontree Supasaguan
Deputy Secretary-General
Office of the Public Sector
Development Commission



พลเอก ดร.ปรัชญา เฉลิมวัฒน์
เลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
กรรมการและเลขานุการ
General Dr. Prachya Chalermwat
Secretary-General, National Cyber Security Committee
Committee and Secretary

กรรมการผู้ทรงคุณวุฒิ Honorary Committees

ดร. ชัยชนะ มิตรพันธ์

ด้านการรักษาความมั่นคง
ปลอดภัยไซเบอร์

Mr. Chaichana Mitrpant

Expert Committee on Cyber Security



**รองศาสตราจารย์
ดร.เสาวณีย์ ไทยรุ่งโรจน์**

ด้านเศรษฐศาสตร์

**Assoc. Prof.
Dr.Sauwanee Thairungroj**

Expert Committee on Economics



พลเอก ภูษพงศ์ พงษ์ศิริ

ด้านสังคมศาสตร์

Gen. Pushpong Pongsiri

Expert Committee on Social Sciences



นางแก้วใจ นาคสกุล

ด้านการบริหารจัดการองค์กร

Mrs. Kaewjai Nacaskul

Expert Committee on
Organizational Administration



**รองศาสตราจารย์
สุรศักดิ์ สงวนพงษ์**

ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

Assoc. Surasak Sanguanpong

Expert Committee on information
and Communication Technology



ภายใต้การบริหารจัดการของ พลเอก ดร.ปรัชญา เฉลิมวัฒน์ เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในปีที่ 2 นับเป็นก้าวสำคัญของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ในการพัฒนาและยกระดับขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศให้เพิ่มสูงขึ้น เพื่อเสริมสร้างให้ทุกภาคส่วนของประเทศมีภูมิคุ้มกันต่อภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพตามวัตถุประสงค์ และเป้าหมายที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดไว้ในปีงบประมาณ พ.ศ. 2565 สกมช. ยังคงให้ความสำคัญกับการดำเนินงานตามแผนงานต่อเนื่องจากการดำเนินงานในปีงบประมาณ พ.ศ. 2564 ที่ผ่านมาถึง 6 ด้าน และได้มีการเพิ่มเป้าหมายการพัฒนา สกมช. สู่การเป็นองค์กรที่มีสมรรถนะสูง เพื่อให้ สกมช. เป็นหน่วยงานหลักของชาติในการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ เป็นที่ยอมรับของนานาประเทศ โดยมีผลการดำเนินงานที่สำคัญทั้ง 7 ด้าน ดังนี้

การขับเคลื่อนนโยบายและแผนด้านความมั่นคงปลอดภัยไซเบอร์

เพื่อให้วัตถุประสงค์และเป้าหมายที่กำหนดไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 บรรลุผลอย่างเป็นรูปธรรม สกมช. จึงได้จัดทำร่างนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2656 - 2570) ขึ้น เพื่อใช้เป็นแนวทางสำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในการดำเนินการด้านการ

Under the Management of General Dr. Prachya Chalermwat, who has been the Secretary-General of the National Cyber Security Committee for the second year, it has been a milestone for the National Cyber Security Agency (NCSA) in developing and upgrading the capability to maintain national cyber security to increase the immunity of all sectors against cyber threats according to the objectives and goals stipulated in the Cyber Security Act B.E. 2562 (2019) and stated in the fiscal year 2022. In addition, NCSA also emphasizes the follow-up on the continuous implementation of plans in the fiscal year 2021 in six areas. The NCSA aims to transform into a high-performance agency as the main national agency to maintain cyber security to be internationally recognized. The seven key achievements are summarized below.

Driving the policies and action plans on cyber security

To achieve the objectives and goals stipulated in the Cyber Security Act B.E. 2562 (2019), the National Cyber Security Agency (NCSA) has formulated the Policies and Action Plans on Maintaining Cyber Security (2023 - 2027) as a guideline for government agencies and critical information infrastructure agencies to maintain cyber security in their respective responsibilities and the action plans for maintaining cyber security to be prepared for

รักษาความมั่นคงปลอดภัยไซเบอร์ในขอบเขตความรับผิดชอบ และจัดทำแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้มีความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ให้ได้ในทุกมิติ ซึ่งคณะรัฐมนตรีได้มีมติให้ความเห็นชอบในนโยบายและแผนดังกล่าวแล้วเมื่อวันที่ 20 กันยายน 2565 และคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อนุมัติให้ประกาศเป็นการทั่วไปแล้ว โดยมีแผนยุทธศาสตร์ที่สำคัญทั้งหมด 4 แผน ได้แก่ ยุทธศาสตร์ที่ 1 สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ (บุคลากร องค์ความรู้และเทคโนโลยี) ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ ยุทธศาสตร์ที่ 3 สร้างบริการภาครัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้ และยุทธศาสตร์ที่ 4 สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน

การจัดทำกฎหมายลำดับรอง ประกาศระเบียบที่เกี่ยวข้อง

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีกฎหมายลำดับรองที่ต้องจัดทำตามที่บทบัญญัติตามมาตราต่างๆ กำหนดไว้จำนวนทั้งสิ้น 41 ฉบับ ซึ่งผลการจัดทำกฎหมายลำดับรองดังกล่าวในปีงบประมาณ 2565 ได้จัดทำเสร็จสมบูรณ์จำนวน 5 ฉบับ นับตั้งแต่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ประกาศใช้ สกมช. ได้จัดทำกฎหมายลำดับรองเสร็จสิ้นไปแล้วจำนวน 32 ฉบับ คิดเป็นร้อยละ 78 ของจำนวนกฎหมายลำดับรองที่ต้องจัดทำ

cyber threats in all dimensions. The Cabinet approved the Policies and Action Plans on 20 September 2022, and the National Cyber Security Committee has officially approved it. There are four strategic plans: Strategy 1: To increase the country's capability of maintaining cyber security (human resources, knowledge, and technology), Strategy 2: To integrate collaboration to prepare for cyber threats and restore the normal condition, Strategy 3: To establish public services and critical information infrastructure to have cyber security and resilience to restore their normal condition, and Strategy 4: To develop the potential of national agencies to be of great quality and standards.

Preparations of minor laws, notifications, and relevant regulations

According to the Cyber Security Act B.E. 2562, 41 minor laws must be prepared pursuant to the provisions thereof. As of the fiscal year 2022, five minor laws have been prepared. Since the Cyber Security Act B.E. 2562 has been in effect, NSCA has prepared 32 minor laws, representing 78 percent of the minor laws required. Only nine laws are underway. In addition, NSCA has enacted several minor laws for internal enforcement. As a result, the agency's operations are more convenient and flexible. Other government agencies and

และอยู่ระหว่างการดำเนินงานอีกเพียง 9 ฉบับ เท่านั้น อีกทั้ง สกมช. ได้จัดทำกฎหมายลำดับรองเพื่อใช้ในการบริหารภายในของ สกมช. อีกจำนวนหลายฉบับ ทำให้ปัจจุบัน สกมช. สามารถปฏิบัติงานได้อย่างคล่องตัวมากยิ่งขึ้น และอำนวยความสะดวกให้หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหลักการปฏิบัติที่ชัดเจนในการเฝ้าระวังรับมือ และจัดภัยคุกคามทางไซเบอร์ที่เกิดหรืออาจจะเกิดขึ้นกับหน่วยงานของตน

ส่งเสริมความร่วมมือกับหน่วยงานองค์กรทั้งภายในประเทศและระหว่างประเทศ

สกมช. ได้ขยายความร่วมมือกับหน่วยงานและองค์กรทั้งภายในประเทศและระหว่างประเทศอย่างกว้างขวางและในทุกมิติ มีการจัดทำบันทึกความร่วมมือกับหน่วยงานทั้งในประเทศและต่างประเทศจำนวน 5 ฉบับ การส่งเสริมความร่วมมือภายใต้กรอบความร่วมมือทั้งพหุภาคีและทวิภาคีกับมิตรประเทศต่างๆจำนวน 13 ประเทศ ทั้งในรูปการร่วมประชุมและการแลกเปลี่ยนการเยี่ยมชมของผู้บริหารระดับสูง อีกทั้งยังมีการสร้างเครือข่ายความร่วมมือกับหน่วยงานและองค์กรในประเทศเพิ่มมากขึ้น เช่น การประชุม Thailand CERTs Community (TH-CC) การสนับสนุนภารกิจแลกเปลี่ยนการดำเนินงานตามยุทธศาสตร์ชาติด้านความมั่นคงของกรมการทหารและความมั่นคงของวุฒิสภา และสุดท้ายได้มีการแต่งตั้งคณะทำงานจัดทำแผนรับมือภัยคุกคามทางไซเบอร์เพื่อเป็นกลไกประสานความร่วมมือในการรับมือกับภัยคุกคามทางไซเบอร์ในระดับชาติ

เฝ้าระวัง รับมือ ภัยคุกคามทางไซเบอร์

การปฏิบัติงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (NCERT)

critical information infrastructure agencies have had clear practice guidelines for vigilance, response, and elimination against cyber threats that have occurred or may occur to their organizations.

Promoting collaboration with domestic and international organizations

NSCA has expanded its collaboration with domestic and international organizations in various dimensions. There have been five MOUs with domestic and international organizations and achieved multilateral and bilateral cooperation frameworks with 13 ally countries in the forms of conferences and exchange visits of chief executive officers, and more collaboration networks with local organizations. For example, the Thailand CERTs Community (TH-CC) conference was held. There has been support for the achievement report conference for implementing the national security strategies of the military commissioner and the senate. Finally, a working group has been appointed to develop a cyber threat response plan as a mechanism for coordinating cooperation in dealing with cyber threats at the national level.

Vigilance against cyber threats

The operations of the National Computer Emergency Response Team (NCERT) under the supervision of NSCA in the fiscal year 2022 encountered cyber threats in various forms and at an evidently higher frequency than the previous year. NCERT has been

ภายใต้การกำกับของ สกมช. ในปีงบประมาณ พ.ศ. 2565 ต้องเผชิญกับภัยคุกคามทางไซเบอร์ในหลายรูปแบบและมีจำนวนสูงขึ้นจากปีก่อนอย่างเห็นได้ชัด ทั้งนี้ NCERT ได้ปฏิบัติการเฝ้าระวังและแจ้งเตือนภัยคุกคามทางไซเบอร์ให้กับหน่วยงานของรัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และประชาชนทั่วไปในหลายรูปแบบมากกว่า 500 เหตุการณ์ รวมทั้งการปฏิบัติการสนับสนุนทางไซเบอร์และการให้ความช่วยเหลือหน่วยงานที่ถูกโจมตีทางไซเบอร์ โดยจากการปฏิบัติในรอบปีงบประมาณ พ.ศ. 2565 พบว่า การโจมตีด้วย การแฮกเว็บไซต์ มีจำนวนมากกว่าการโจมตีในรูปแบบอื่นๆ โดยเฉพาะการโจมตีในการลักษณะวัตถุประสงค์เพื่อแฝงหน้าเว็บไซต์การพนันออนไลน์ในเว็บไซต์ของหน่วยงานของรัฐ ซึ่งสถิติที่ตรวจพบหน่วยงานด้านการศึกษา และหน่วยงานด้านสาธารณสุขเป็นหน่วยงานที่ถูกโจมตีทางไซเบอร์สูงสุด

การพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์และสร้างการตระหนักรู้ให้กับประชาชน

สกมช. ได้ดำเนินการจัดการอบรมให้ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ในหัวข้อที่เป็นปัจจุบันและทันสมัยต่อเหตุการณ์ ซึ่งจัดขึ้นเป็นประจำทุกเดือนเพื่อสร้างความตระหนักรู้ให้กับเยาวชนและประชาชนทั่วไป โดยในปีงบประมาณ พ.ศ. 2565 มีผู้เข้าร่วมอบรมในระบบออนไลน์มากกว่า 18,000 คน รวมทั้งยังเพิ่มช่องทางในการสร้างความตระหนักรู้ในด้านอื่นๆ เช่น การจัดนิทรรศการ การให้บริการบริการวิชาการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานอุดมศึกษาต่างๆ เป็นต้น สำหรับการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ตามโครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ระยะที่ 1 ซึ่งได้ดำเนินการ

watching out and sending warnings regarding cyber threats to government agencies, critical information infrastructure agencies, and the general public for more than 500 events. The team has lent cyber support for the agencies attached by cyber threats as well. In the fiscal year 2022, there were more website hacks than other forms of cyber threats with an aim to disguise online gambling websites on those of government agencies. According to statistics, educational and public health agencies were most hit by cyber threats.

Developing cyber security personnel and raising awareness among the public

NSCA has provided monthly training in cyber security on up-to-date topic to raise awareness among the public and youths. In the fiscal year 2022, there were more than 18,000 online participants. There are other channels for raising awareness, such as exhibitions and academic services on cyber security for higher education institutions. Regarding human resources development on cyber security pursuant to Personnel Development Acceleration Program in Cyber Security Phase 1, the project has been implemented with great success. In total, 4,149 participants passed the training, which was 1,000 people more than expected. In addition, NSCA organized skills and knowledge training

จนใกล้จะจบโครงการแล้วนั้นได้บรรลุผลสัมฤทธิ์อย่างดีมีผู้ผ่านการอบรมหลักสูตรต่างๆ จำนวนทั้งสิ้น 4,149 คน ซึ่งสูงกว่าเป้าหมายที่ตั้งไว้ประมาณ 1,000 คน นอกจากนี้ สกมช.ยังได้จัดการอบรมการเพิ่มทักษะและพัฒนาความรู้ความสามารถให้กับบุคลากรของหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Cyber Clinic) อย่างต่อเนื่องตลอดปี มากกว่า 5,500 ชั่วโมง โดยมีผู้สนใจเข้าร่วมการอบรมมากกว่า 1,800 คน และในปีงบประมาณ พ.ศ. 2565 สกมช. ได้จัดการแข่งขันทักษะทางไซเบอร์ Thailand Cyber Top Talent 2022 ซึ่งเป็นการจัดต่อเนื่องเป็นปีที่ 2 โดยมีทีมเข้าร่วมการแข่งขันทั้งสิ้น 393 ทีม และมีผู้เข้าร่วมการแข่งขันมากกว่า 1,100 คน

การยกระดับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานของรัฐ

เพื่อเป็นการยกระดับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานของรัฐให้มีขีดความสามารถสูงขึ้น สกมช. จึงได้ดำเนินการหลายกิจกรรมและหลายรูปแบบตามมาตรการที่จำเป็นดังนี้ การประเมินความพร้อมในการรับมือความเสี่ยงต่อภัยคุกคามทางไซเบอร์ ระดับกลุ่มหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและระดับหน่วยงานของรัฐ กิจกรรม Countdown เพื่อให้หน่วยงานดังกล่าวได้ทราบถึงประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับ หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การจัดทำร่างมาตรฐานวิชาชีพ ผู้ปฏิบัติงานด้านไซเบอร์ การฝึกเพื่อทดสอบขีดความสามารถ

(Cyber Clinic) for personnel of regulatory bodies, government agencies, and critical information infrastructure agencies throughout the year totaling 5,500 hours. The Cyber Clinic attracted more than 1,800 participants. In the fiscal year 2022, NCSA organized Thailand Cyber Top Talent 2022, which has been the second consecutive year. This competition was attended by 393 teams and more than 1,100 contestants.

Upgrading critical information infrastructure agencies and government agencies

To upgrade the capability of critical information infrastructure agencies and government agencies, NCSA has implemented various activities pursuant to necessary measures, including assessment of preparedness for cyber threats at critical information infrastructure agencies and government agencies, the countdown activity for such agencies to know the practice and standard frameworks for cyber security for critical information infrastructure agencies and government agencies, Thailand's National Cyber Exercise 2022, and Prime minister Awards: Thailand Cyber security Excellent Awards 2022. In the fiscal year 2022, a total of 127 agencies participated in the activities,

ทางไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Thailand's National Cyber Exercise 2022) และการจัดงาน Prime minister Awards : Thailand Cyber security Excellent Awards 2022 โดย ในปีงบประมาณ พ.ศ. 2565 มีหน่วยงานที่เข้าร่วมจำนวนทั้งสิ้น 127 หน่วยงาน และมีหน่วยงานที่ได้รับประกาศเกียรติคุณสำหรับหน่วยงานที่มีการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์เป็นเลิศ (Certificate of Cyber safety) จำนวน 36 หน่วยงาน

การพัฒนา สกมช. สู่การเป็นองค์กรที่มีสมรรถนะสูง

สกมช. เป็นหน่วยงานระดับชาติที่มีการดำเนินงานในการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับประเทศ ทั้งในฐานะเป็นผู้ปฏิบัติและผู้ประสานงานให้เกิดสภาพแวดล้อมที่เอื้ออำนวยต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ จึงมีความจำเป็นต้องได้รับการพัฒนาให้เป็นองค์กรสมรรถนะสูงสามารถปฏิบัติงานภายใต้สถานการณ์ที่ร้ายแรงและวิกฤติด้านภัยคุกคามทางไซเบอร์ได้ทุกมิติและทุกรูปแบบ ในปีงบประมาณ พ.ศ. 2565 จึงได้มีการเสริมสร้างความเข้มแข็งให้กับหน่วยงานภายใน สกมช. ในทุกระบบ เช่น ระบบการบริหารบุคคล ได้มีการจัดทำแผนกลยุทธ์การบริหารและพัฒนาบุคลากรระยะ 3 ปี (พ.ศ. 2565-2567) การพัฒนาบุคลากรภายใต้กิจกรรมในหลายรูปแบบ การสร้างวัฒนธรรมการถ่ายทอดองค์ความรู้และพัฒนาบุคลากรภายในอย่างต่อเนื่อง สำหรับระบบการควบคุมและสั่งการ ได้มีการนำระบบ Back Office ที่ทันสมัยมาใช้งานเพื่อให้เกิดความรวดเร็วและมีประสิทธิภาพสูงขึ้น และเพื่อให้เป็นองค์กรที่มีความโปร่งใส มีธรรมาภิบาล จึงได้มีการจัดทำแผนการตรวจสอบภายในระยะ 5 ปี (พ.ศ. 2565-2569) เพื่อใช้เป็นกรอบในการตรวจสอบ

while 36 agencies were awarded a Certificate of Cyber Safety.

Developing NCSA into a highly capable agency

NCSA is a national agency in charge of maintaining cyber security for the country, as both the practitioner and the coordinator for an environment supportive to cyber security. Therefore, it must be developed into a highly capable agency that can work in severe situations and cyber threat crises in all dimensions and all forms. In 2022, internal divisions of NCSA were strengthened. For example, the human resources management system has prepared a three-year strategy for human resources management and development (2022 – 2024), including personnel development activities, a culture of continuous knowledge transfer, and internal personnel development. For the control and command systems, a modern back office has been introduced for better speed and efficiency. For transparency and governance, there is a five-year audit plan (2022 – 2026) as the outline for transparency audits in all systems. These efforts will transform NCSA into an agency with high capability, good governance, and international acceptance.

ความโปร่งใสทุกระบบงาน ซึ่งจะทำให้ สกมช. เป็นหน่วยงานที่มีสมรรถนะสูงและมีธรรมาภิบาล เป็นที่ยอมรับของนานาชาติ

ผลการประเมินการดำเนินงาน ของสำนักงานคณะกรรมการการรักษา ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประจำปีงบประมาณ 2565

ผลการประเมินการดำเนินงานของ สกมช. ตามมาตรา 39 แห่ง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีการประเมินผลการดำเนินงานองค์กรในปีที่สองผ่านแนวคิดการประเมินตามองค์ประกอบ 4 ด้าน ได้แก่ องค์ประกอบที่ 1 ด้านประสิทธิภาพ ได้ระดับคะแนน 39.38 คะแนน จากคะแนนเต็ม 40 คะแนน องค์ประกอบที่ 2 ด้านประสิทธิภาพ ได้ระดับคะแนน 28.75 คะแนน จากคะแนนเต็ม 30 คะแนน องค์ประกอบที่ 3 ด้านศักยภาพขององค์การมหาชน ได้ระดับคะแนน 15 คะแนน จากคะแนนเต็ม 20 คะแนน องค์ประกอบที่ 4 ด้านการควบคุมดูแลกิจการของคณะกรรมการองค์การมหาชน ได้ระดับคะแนน 8.7 คะแนน จากคะแนนเต็ม 10 คะแนน รวมแล้วได้คะแนนผลการประเมินการดำเนินงาน ประจำปีงบประมาณ พ.ศ. 2565 เท่ากับ **91.83** จากคะแนนเต็ม 100 คะแนน อยู่ในระดับ **ดีมาก**

Performance evaluation results of the National Cyber Security Agency in the fiscal year 2022

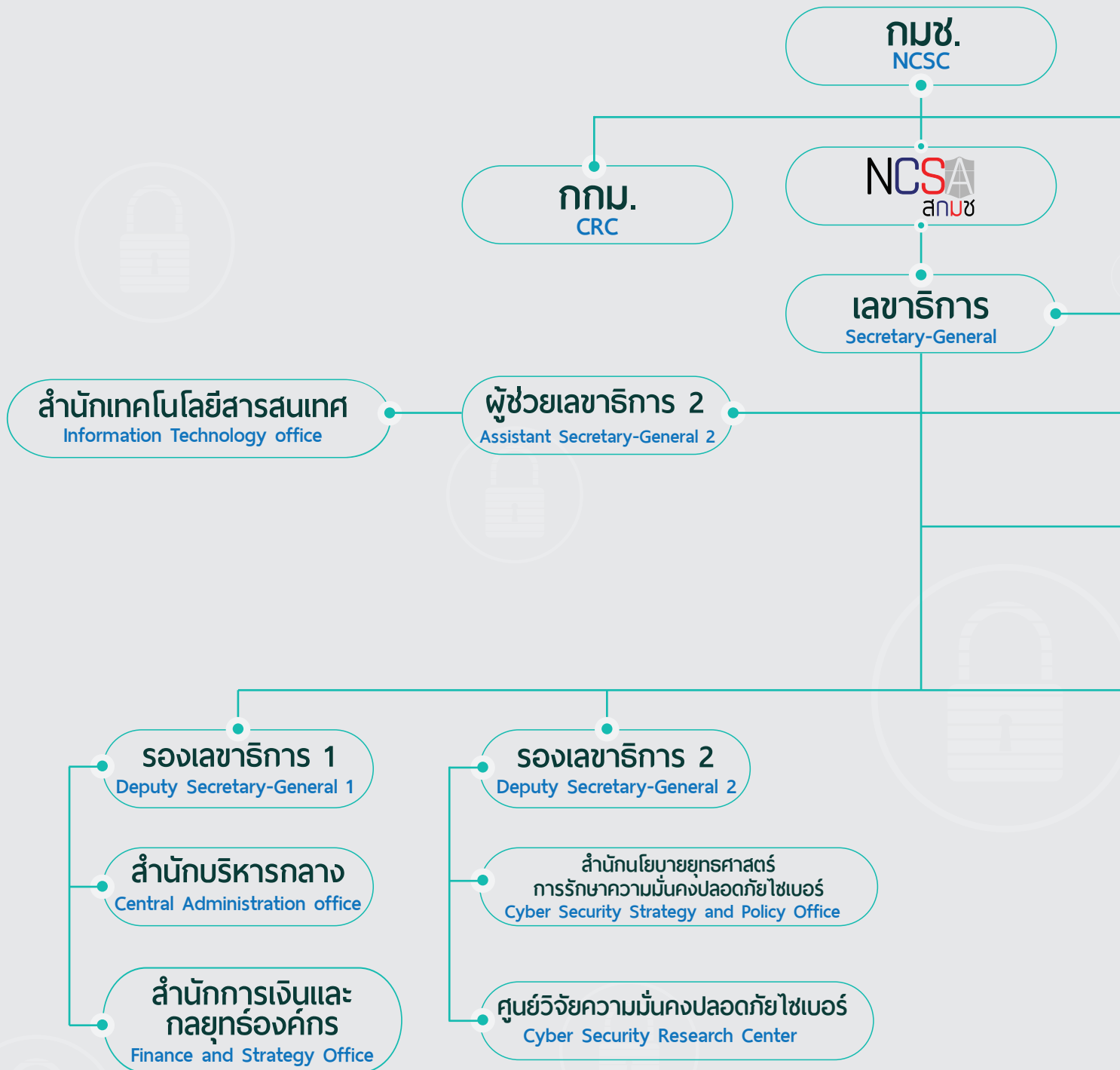
The performance of NCSA is evaluated pursuant to Article 39 of the Cyber Security Act B.E. 2562. In the past two years, the evaluation was based on four elements: effectiveness 39.38/40 points, efficiency 28.75/30 points, the capability of a public organization 15/20 points, and corporate governance of the board of a public organization 8.7/10 points. In total, the result of the performance evaluation for the fiscal year 2022 was **91.83/100 points, which is a very good level.**

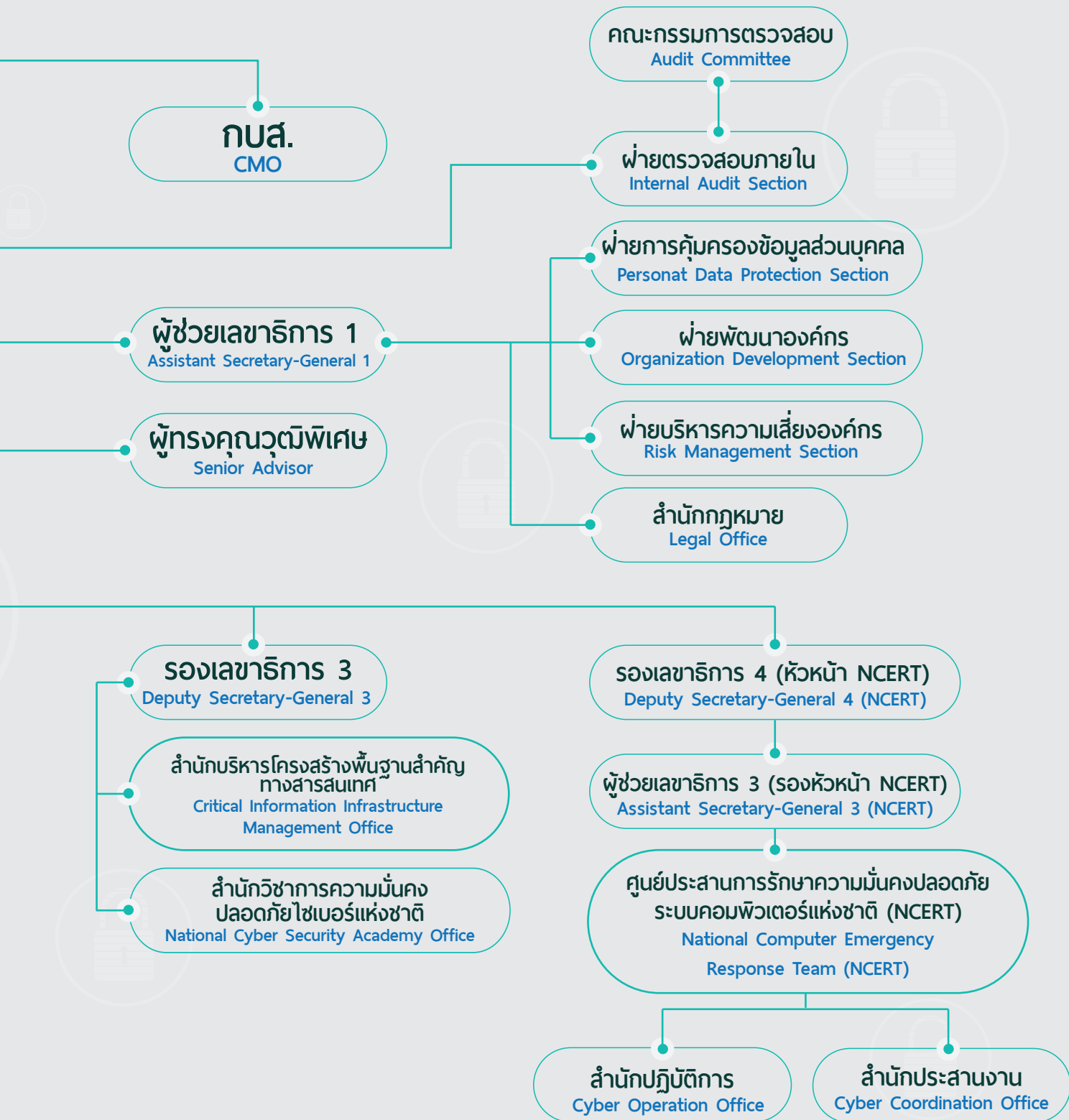




โครงสร้างองค์กร

Organizational Structure





ผู้บริหารสำนักงาน

Executive National Cyber Security Agency (NCSA)

- 1 **Gen. Dr. Prachya Chalermwat**
Secretary-General (January 1, 2021 - September 30, 2022)
- 2 **Gen. Krishna Laiviratana**
Deputy Secretary-General 1
- 3 **Lt. Gen. Parinya Chaidilok**
Expert
- 4 **Gen. Suchart Wongmark**
Senior Advisor 1
- 5 **Capt. Dr. Nattapon Chatprechakul**
Acting Director of Information Technology Office
- 6 **Asst. Prof. Dr. Waraporn Promwikorn**
Director of Central Administration Office
- 7 **Mrs. Mattika Jongpiriyaanant**
Director of Finance and Strategy Office
- 8 **Capt. Sirinate Rugvong**
Director of National Cyber Security Academy Office
- 9 **Ms. Saichon Saelee**
Acting Director of Cyber Coordination office
- 10 **Pol. Col. Naughtakrit Phromchan**
Director of Cyber Operation Office





AVM Amorn Chomchoey 11
Secretary-General (October 1, 2022 - Present)

AVM Amorn Chomchoey 12
Deputy Secretary-General 4

Maj. Gen. Katavout Kajohnkittiyut 13
Senior Advisor 2

Maj. Gen. Teerawut Wittayakorn 14
Assistant Secretary-General 3

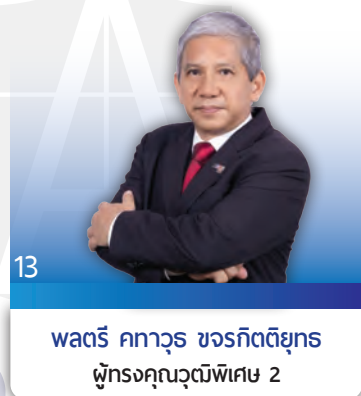
Mrs. Kingnapa Bangchaud 15
Director of Cyber Security Strategy and Policy Office

Col. Suwatchai Bunsom 16
Acting Director of Cyber Security Research Center

AVM Jadet Khuhakongkit 17
Director of Critical information Infrastructure Management Office

Ms. Darunee Phikulthong 18
Director of Legal Office

Lt. Cdr. Saktipong Sibmuenpiam 19
Director of Internal Audit Section





สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ National Cyber Security Agency

ประวัติความเป็นมา สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งมีผลบังคับใช้เมื่อวันที่ 28 พฤษภาคม 2562 ให้จัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นหน่วยงานของรัฐที่มีหน้าที่กำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบและสร้างความเดือดร้อนต่อประชาชน ตลอดจนความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ

หน้าที่ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ คือ รับผิดชอบงาน ตามพระราชบัญญัติ ประสานงานร่วมกันทั้งภาครัฐและเอกชน รวมถึงกำหนดนโยบาย ระเบียบ มาตรฐาน ขันดำนแนวทางความปลอดภัยสำหรับหน่วยงานรัฐ ป้องกันรับมือภัยคุกคามทางไซเบอร์ ตลอดจนความมั่นคง ของรัฐและความสงบเรียบร้อยของประเทศ ตั้งเป้ายะสามปีคือ สร้างบุคลากรด้าน Cyber Security

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีตัวย่อว่า สกมช. และมีชื่อภาษาอังกฤษ “National Cyber Security Agency (NCSA)” เป็นหน่วยงานของรัฐในรูปแบบ องค์การมหาชน ซึ่งมุ่งเน้นการบริหารและดำเนินงานอย่างมีประสิทธิภาพ เพื่อเป็นหน่วยงานกลาง สร้างกลไก ขับเคลื่อนการทำงานด้านการดูแลและรับมือภัยคุกคามทางไซเบอร์ รวมทั้งให้ความช่วยเหลือ สนับสนุน ให้ความรู้ ความเข้าใจ ให้หน่วยงานภาครัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และประชาชน เพื่อลดความเสี่ยงและบรรเทาความเสียหายจากภัยคุกคามที่อาจเกิดขึ้น





มคังปลอดภัยไซเบอร์แห่งชาติ
Security Agency

เกี่ยวกับ สกมช.

About NCSA

History of the National Cyber Security Agency

According to the Cyber Security Act B.E. 2562, effective on 28 May 2019, the National Cyber Security Agency was established as a government agency in charge of making the policies, measures, and guidelines for maintaining cyber security for public and private organizations as the critical information infrastructure agencies in preventing, responding to, and mitigating the risk of cyber threats. The purpose is to prevent or minimize the impacts on the public and to ensure national security, peace, and order.

The duties of the National Cyber Security Agency are the assigned tasks as per the Act, the coordination between public and private organizations, making policies, regulations, minimum standards of cyber security for government agencies in response to cyber threats, and national security, peace, and order. The three-year goal is to build more cyber security personnel.

The National Cyber Security Agency is abbreviated as NCSA. It is a public organization aiming to operate effectively as the central agency to build a mechanism for driving and supervising the response to cyber threats, supporting and educating other public agencies, critical information infrastructure agencies, and the general public to mitigate the potential risks and impacts of cyber threats.



รายงานประจำปี 2565

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

วิสัยทัศน์ Vision



“ เป็นผู้นำในการขับเคลื่อนในการบริหาร
จัดการความมั่นคงปลอดภัยไซเบอร์
ของประเทศที่มีประสิทธิภาพ
พร้อมตอบสนองต่อภัยคุกคามไซเบอร์ทุกมิติ ”

“Take the leading role in overseeing national cyber security effectively and being well
prepared for cyber threats in all dimensions”

แนวทางการเชื่อมโยงแผนระดับต่าง ๆ

The guideline for integrating different levels of plans

1 แผนระดับ Plan Level	ยุทธศาสตร์ชาติ 20 ปี ด้านความมั่นคง ด้านเสริมสร้างขีดความสามารถ ในการแข่งขัน ด้านการปรับสมดุลและพัฒนาระบบการบริหารจัดการภาครัฐ The 20-year national strategy on security, competitiveness, balance, and development of public administration systems
2 แผนระดับ Plan Level	แผนพัฒนาเศรษฐกิจและสังคม ฉบับที่ 13 The 13 th National Economic and Social Development Plan
3 แผนระดับ Plan Level	นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570) The Policies and Action Plans on Cyber Security (2022 – 2027)

พันธกิจ Mission



1

เสนอแนะและขับเคลื่อนนโยบาย แผน ยุทธศาสตร์ และปรับปรุงกฎหมายว่าด้วย การรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้ง ศึกษาวิจัย กำหนดแนวทางมาตรฐาน มาตรการที่เกี่ยวข้อง ให้สอดคล้องกับสถานการณ์ทั้งในปัจจุบันและอนาคต

Recommend and implement policies, plans, and strategies, amend laws on maintaining cyber security, research and determine relevant standards and measures suitable for situations at present and in the future

2

กำกับ ดูแล เพาะระวัง ติดตาม วิเคราะห์ ประมวลผล แจ้งเตือน และปฏิบัติการ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

Regulate, oversee, monitor, track, analyze, process, alert, and act to prevent, address, and minimize the risk of cyber threats

3

เป็นศูนย์กลางในการประสานความร่วมมือ รวมทั้ง ส่งเสริม สนับสนุน และช่วยเหลือหน่วยงานภาครัฐและเอกชนทั้งในประเทศและต่างประเทศ เพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

Function as the center for coordinating cooperation, supporting, promoting, and assisting public and private organizations domestically and internationally to maintain cyber security

4

เผยแพร่ความรู้ความเข้าใจ และสนับสนุนการพัฒนาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

Disseminate knowledge, establish understanding, and support the development of cyber security personnel

แนวทางการพัฒนาสำนักงานตามแผนปฏิบัติการ

Guideline for developing the NCSA according to the Action Plan

ปีที่ 1
The 1st Year

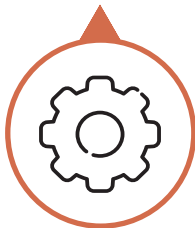
การจัดตั้งสำนักงาน
Establishment of the NCSA



ปีที่ 3
The 3rd Year

รุกสู่หน่วยงานที่เกี่ยวข้อง
เพื่อให้เกิดมาตรฐาน
Advancing to relevant agencies to
create a standard

ปีที่ 2
The 2nd Year



สร้างขีดความสามารถของสำนักงานและสร้างระบบ
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
Building the capacity of the NCSA and the cyber security system

เป้าหมายในปีต่อไป

Next Year's Goal

“ การเสริมสร้างขีดความสามารถของสำนักงาน
และหน่วยงานเป้าหมายพร้อมเสริมสร้างความรู้ความเข้าใจ
และสร้างความตระหนักรู้ให้กับประชาชน
ในการรักษาความมั่นคงปลอดภัยไซเบอร์ ”

“Strengthening the capability of the NCSA and target agencies,
providing knowledge, establishing understanding,
and raising public awareness of cyber security”

กลยุทธ์องค์กร

Organizational Strategies

กลยุทธ์ที่ Strategy

1

พัฒนาขีดความสามารถของสำนักงานในการป้องกัน
รับมือ ฝ้าระวัง และแก้ไขภัยคุกคามไซเบอร์

Develop the capabilities of the NCSA to prevent, respond to,
monitor, and resolve cyber threats

กลยุทธ์ที่ Strategy

2

ศึกษาแนวโน้ม ทิศทาง และการจัดทำนโยบาย/แผน/
กฎหมาย/กฎระเบียบ/ประกาศ/มาตรการ/มาตรฐาน
ที่สนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

Study the trends, directions, and preparations of policies, plans,
laws, regulations, notifications, measures, and standards that
support national cyber security

กลยุทธ์ที่ Strategy

3

ส่งเสริม สนับสนุนงานวิจัยและพัฒนาเทคโนโลยี
องค์ความรู้ที่เกี่ยวกับ การรักษาความมั่นคงปลอดภัย
ไซเบอร์ของประเทศ

Promote and support research and development in technology and
knowledge related to national cyber security

กลยุทธ์ที่ Strategy

4

สนับสนุนการดำเนินงานตามยุทธศาสตร์นโยบายและ
แผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับ
หน่วยงาน

Support the implementation of the strategies, policies, and
plans on cyber security at the agency level

กลยุทธ์ที่ Strategy

5

กำกับ ดูแล ให้องค์หน่วยงานที่เกี่ยวข้องสามารถป้องกัน
รับมือและลดความเสี่ยง จากภัยคุกคามทางไซเบอร์

Regulate and supervise relevant agencies to prevent, cope with,
and minimize risks from cyber threats

กลยุทธ์ที่ Strategy

6

สร้างเครือข่ายความร่วมมือเพื่อบูรณาการการทำงานร่วมกัน
รวมถึงส่งเสริมสนับสนุนการแลกเปลี่ยนข้อมูล

Create a network to integrate, collaborate, and support data sharing

กลยุทธ์ที่ Strategy

7

พัฒนาศักยภาพและเพิ่มทักษะบุคลากรด้านการรักษา
ความมั่นคงปลอดภัยไซเบอร์

Develop potential and improve skills of cyber security personnel

กลยุทธ์ที่ Strategy

8

สร้างบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

Build up cyber security personnel

กลยุทธ์ที่ Strategy

9

สร้างความตระหนักและการรับรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

Raise awareness and recognition of cyber security

รายงานผลการดำเนินงาน พ.ศ. 2565

Performance Report 2022



การขับเคลื่อน Implementation

การขับเคลื่อนนโยบายและแผนด้านความมั่นคงปลอดภัยไซเบอร์
Implementation of policies and plans on cyber security



การเฝ้าระวัง รับมือ Vigilance and response

การเฝ้าระวัง รับมือภัยคุกคามทางไซเบอร์
Vigilance and response to cyber threats



การจัดทำกฎหมาย Enactment

การจัดทำกฎหมายลำดับรอง ประกาศ ระเบียบ ที่เกี่ยวข้อง
Enactment of minor laws, notifications, and regulations applicable



การพัฒนา Development

การพัฒนาบุคลากร ด้านความมั่นคงปลอดภัยไซเบอร์
และสร้างความตระหนักรู้
Development of cyber security personnel
and awareness



การส่งเสริมความร่วมมือ Promoting collaboration

การส่งเสริมความร่วมมือกับหน่วยงาน องค์กรทั้งภายในประเทศ
และระหว่างประเทศ
Promoting collaboration with domestic and international
organizations



การยกระดับ Upgrading

การยกระดับหน่วยงานโครงสร้างพื้นฐานสำคัญ
ทางสารสนเทศและหน่วยงานของรัฐ
Upgrading critical information infrastructure agencies
and government agencies



องค์กรที่มีสมรรถนะสูง High-performance organization

การพัฒนา สกมช. สู่การเป็นองค์กรที่มีสมรรถนะสูง
Developing NCSA into a high-performance organization



การขับเคลื่อน

Implementation

การขับเคลื่อนนโยบายและแผนด้านความมั่นคง
ปลอดภัยไซเบอร์

Implementation of policies and plans on cyber security

1

รายงานประจำปี 2565

การขับเคลื่อนนโยบาย และแผนด้านความมั่นคงปลอดภัยไซเบอร์

Implementation of policies and plans on cyber security



การขับเคลื่อนนโยบายและแผนปฏิบัติการ ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

(พ.ศ. 2565 - 2570) Implementation of Cybersecurity Policy and Action Plan 2022 - 2027

การประชุมคณะรัฐมนตรีเมื่อวันที่ 20 กันยายน 2565 มีมติเห็นชอบ (ร่าง) นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) โดยประกาศในราชกิจจานุเบกษา เมื่อวันที่ 9 ธันวาคม 2565 และมีผลบังคับใช้เมื่อวันที่ 10 ธันวาคม 2565

At the meeting on 20 September 2022, the Cabinet approved the (Draft) Cybersecurity Policy and Action Plan 2022 - 2027. Accordingly, the Cybersecurity Policy and Action Plan 2022 - 2027 was published in the Royal Thai Government Gazette on 9 December 2022, and became effective on 10 December 2022.

นโยบายและแผนปฏิบัติการ Cybersecurity Policy and Action Plan 2022 - 2027

ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565-2570

“บริการที่สำคัญของประเทศไทยมีความมั่นคงปลอดภัยไซเบอร์ เพื่อความยั่งยืนทางเศรษฐกิจและสังคม”
 “Cybersecurity for Thailand’s critical services to ensure economic and social sustainability”

ยุทธศาสตร์ที่ Strategy

1

สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ (บุคลากร องค์ความรู้ และเทคโนโลยี)

Buildup all the ecosystem and cyber capacity for all components: people, knowledge, technology, system

เพื่อเสริมสร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยบูรณาการบุคลากร องค์ความรู้ และเทคโนโลยีนำไปสู่การพัฒนาผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมของประเทศ

To build country’s cybersecurity capacity by integrating workforce, knowledge, and technology, to develop cybersecurity innovation



เพิ่มบุคลากรที่มีความสามารถด้านความมั่นคงปลอดภัยไซเบอร์
Increasing cybersecurity workforce



สร้างความตระหนักรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์
Raising cybersecurity awareness and skill



ส่งเสริมการวิจัยและพัฒนาและนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์
Promoting cybersecurity research and development, including innovation

ยุทธศาสตร์ที่ Strategy

2

บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้

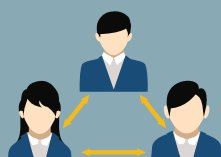
Build Up synergy via strong partnership and integrated effort

เพื่อบูรณาการความร่วมมือในการเตรียมความพร้อมสำหรับการรับมือภัยคุกคามทางไซเบอร์ และการฟื้นคืนบริการที่สำคัญสู่สภาพปกติได้อย่างรวดเร็วกับทุกภาคส่วน ทั้งภายในประเทศและระหว่างประเทศ

To integrate domestic and international collaboration in preparation for cyber threat response and recovery of critical services to normal operations



ส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและภาคเอกชน
Promoting and supporting public-private partnership



ประสานความร่วมมือระหว่างประเทศเพื่อรับมือภัยคุกคาม
Coordinating international collaboration to address cyber threat

ยุทธศาสตร์ที่ Strategy

3

สร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้

Improved Resiliency for CII and Government service

เพื่อส่งเสริมบริการภาครัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์ และสามารถฟื้นคืนบริการที่สำคัญสู่สภาพปกติได้

To promote cyber resilience for government services and critical information infrastructure



กำหนดมาตรการการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII)
Providing minimum security standard for critical information infrastructure organization



กำหนดโครงสร้างการกำกับดูแลและกรอบกฎหมายสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
Establishing a regulatory structure and legal framework for critical information infrastructure organization



ปกป้องระบบข้อมูลและเครือข่ายของหน่วยงานภาครัฐ
Protecting government agency's data systems and networks

ยุทธศาสตร์ที่ Strategy

4

สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน

Strive to be World class cybersecurity organizations: improve related agency and organizations in terms of standards and quality of services offers

มุ่งสร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐานเพื่อให้บริการจัดการด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

To enhance national agency capability to achieve standards and quality for handling cybersecurity effectively



เพิ่มขีดความสามารถในการรับมือและตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์
Increasing capability to response to cybersecurity-related incidents



ส่งเสริมและสนับสนุนการแบ่งปันข้อมูลภัยคุกคาม
Promoting and supporting threat information sharing



ส่งเสริมและสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์
Promoting and supporting cybersecurity

2

การจัดทำกฎหมาย

Enactment

การจัดทำกฎหมายลำดับรอง ภายใต้พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

Enactment of minor laws
under the Cyber Security Act B.E. 2562

กฎหมายลำดับรองที่สำคัญ
สำหรับบังคับใช้กับหน่วยงานของรัฐ
หน่วยงานควบคุมหรือกำกับดูแล

และหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ

Significant minor laws to be enforced with government agencies,
regulatory or supervisory agencies, and critical information infrastructure agencies

กฎหมายลำดับรอง
จำนวนทั้งสิ้น

Totally 41 minor laws

41

ฉบับ

คิดเป็น Making

100%



ดำเนินการ
แล้วเสร็จ

Completed 32 laws

32 ฉบับ

คิดเป็น Representing

78%



อยู่ระหว่าง
ดำเนินการ

9 laws in progress

9 ฉบับ

คิดเป็น Representing

22%



การจัดทำกฎหมายลำดับรองภายใต้โครงการจัดทำนโยบาย และแผนตามพระราชบัญญัติการรักษาความมั่นคง ปลอดภัยไซเบอร์ ประจำปีงบประมาณ 2565

Enactment of minor laws under the policy-making and planning according
to the Cyber Security Act in the fiscal year 2022



จำนวน

6

ฉบับ

enactments

ประกาศ กมช. เรื่อง การกำหนดหลักเกณฑ์
ลักษณะหน่วยงานที่มีการกิจหรือให้บริการ
เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทาง
สารสนเทศฯ

Notification of the NCSC on the prescribing
of principles and qualifications
of agencies assigned with
the missions or services of
critical information infrastructure



ประกาศ กมช. เรื่อง การกำหนดระดับ
ความรู้ความชำนาญด้านการรักษาความ
มั่นคงปลอดภัยไซเบอร์เพื่อแต่งตั้งเป็น
พนักงานเจ้าหน้าที่ฯ

Notification of the NCSC on the prescribing
of knowledge and expertise
levels in maintaining cyber
security to be appointed as
a competent authority



ประกาศ กมช. เรื่อง ลักษณะ หน้าที่และ
ความรับผิดชอบของศูนย์ประสานการรักษา
ความมั่นคงปลอดภัยระบบคอมพิวเตอร์ฯ

Notification of the NCSC on
the characteristics, duties,
and responsibilities of the
National Computer Emergency
Response Team



ประกาศ กมช. เรื่อง ลักษณะภัยคุกคามทาง
ไซเบอร์ มาตรการป้องกันรับมือ ประเมิน
ปราบปรามและระงับภัยคุกคามทางไซเบอร์
แต่ละระดับฯ

Notification of the NCSC on
the characteristics of cyber
threats, countermeasures,
assessment, suppression,
and inhibition of each level
of cyber threats



ประกาศ กกม. เรื่อง ประมวลแนวทาง
ปฏิบัติและกรอบมาตรฐานด้านการรักษา
ความมั่นคงปลอดภัยไซเบอร์ฯ

Notification of the NCSC on
the procedures, guideline
practice, and standards for
maintaining cyber security



ระเบียบ กกม. ว่าด้วยการมอบอำนาจ
ให้ปฏิบัติแทนฯ

Regulation of the NCSC on
delegation of authority



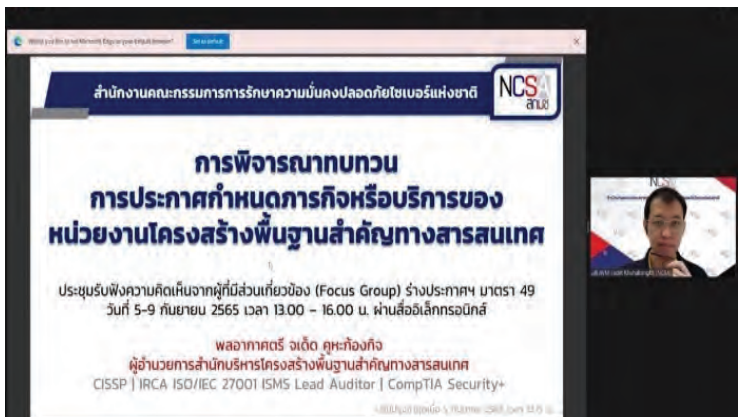
การทบทวนประกาศ กมช. เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็น หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมาย การควบคุม และกำกับดูแล พ.ศ.2564

A review of the Notification of the NCSC on the prescribing of principles and qualifications of agencies assigned with the missions or services of critical information infrastructure and delegation, regulation, and supervision B.E. 2564 (2021)

การทบทวนประกาศ กมช. เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็น หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมาย การควบคุมและกำกับดูแล พ.ศ. 2564 ได้จัดให้มีการทบทวนภารกิจหรือบริการที่ถือว่าเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ให้มีความครอบคลุมและเหมาะสมในการนำไปปฏิบัติเพิ่มมากขึ้น รวมถึงเป็นการดำเนินการให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งกำหนดให้คณะกรรมการจะต้องพิจารณาทบทวนการประกาศกำหนดภารกิจหรือบริการดังกล่าวเป็นคราว ๆ ไปตามความเหมาะสม ซึ่งมีการจัดประชุมรับฟังความคิดเห็นจากผู้ที่มีส่วนเกี่ยวข้อง (Focus Group) ต่อร่างประกาศฯ ตามมาตรา 49 แห่ง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เมื่อวันที่ 5-9 กันยายน 2565 มีจำนวนผู้แทนจากหน่วยงานเข้าร่วมทั้งสิ้น 195 คน

Upon the review of the Notification of the NCSC on the prescribing of principles and qualifications of agencies assigned with the missions or services of critical information infrastructure and delegation, regulation, and supervision B.E. 2564 (2021), the meeting members reviewed the missions or services that are critical

information infrastructure of the country to be more comprehensive and practical. According to the Cyber Security Act B.E. 2562, the Committee shall periodically review such missions and services as deemed appropriate. A focus-group meeting may be organized to hear stakeholders' opinions on the notification according to Article 49 of the Cyber Security Act B.E. 2562. The review meeting was organized from 5 - 9 September 2022, with 195 participants.



3

การส่งเสริมความร่วมมือ Promoting Collaboration

การส่งเสริมความร่วมมือกับหน่วยงานองค์กร
ทั้งภายในประเทศและระหว่างประเทศ
Promoting collaboration with domestic
and international organizations

การบันทึกลงนามความร่วมมือ

Memorandum of Collaboration

การลงนามบันทึกความร่วมมือได้ดำเนินการหารือและประสานงานกับหน่วยงานหรือองค์กรที่ประสงค์ที่จะร่วมมือในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยการจัดทำบันทึกความเข้าใจความร่วมมือ ข้อตกลง ด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเสนอคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

ลงนามแล้วทั้งสิ้น

Signed

There have been efforts to talk and sign memorandums of collaboration with agencies and organizations that intend to work together to maintain cyber security. Memorandums of collaboration have been executed to establish the understanding, partnerships, and agreement on cyber security, which were presented to the National Cyber Security Committee (NCSC)

5

ฉบับ 5 MOUs with 5 organizations
หน่วยงาน



ทปอ
ที่ประชุมอธิการบดีแห่งประเทศไทย
Council of University Presidents of Thailand



(สาธารณรัฐประชาชนจีน ประเทศอิสราเอล กองทัพไทย
ที่ประชุมอธิการบดีแห่งประเทศไทย (ทปอ.)
และบริษัท หัวเว่ย เทคโนโลยี (ประเทศไทย))

People's Republic of China, Israel, the Royal Thai Army,
Council of University Presidents of Thailand,
and Huawei Technology (Thailand) Co., Ltd.



การดำเนินงานภายใต้กรอบความร่วมมือ ทวิภาคีและพหุภาคี

Bilateral and Multilateral Collaboration

การส่งเสริมความร่วมมือระหว่างประเทศ
Promoting international collaboration

รวม with totally

13 ประเทศ
countries

เข้าร่วมประชุมหารือ ประชุมเชิงปฏิบัติการ
อบรม สัมมนา เพื่อส่งเสริมและสนับสนุน
ความร่วมมือระหว่างประเทศด้านความ
มั่นคงปลอดภัยไซเบอร์

Participating in meetings,
workshops, training, and
seminars to promote and
support international
collaboration in cybersecurity.

จำนวนทั้งสิ้น totally

197 ครั้ง
times



การประชุม Thailand CERTs Community (TH-CC)

Thailand CERTs Community Meeting (TH-CC)

การประชุม Thailand CERTs Community (TH-CC) การดำเนินงานตามนโยบายการส่งเสริมและสนับสนุนในการพัฒนาศักยภาพด้านความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งภาครัฐ และเอกชน ให้เป็นมาตรฐานสากล จึงจัดประชุมคณะทำงานของ Thailand CERTs Community (TH-CC) เพื่อเป็นการสร้าง Network และสร้างความร่วมมือ สนับสนุนการสร้างเครือข่ายในการทำงานร่วมกัน ระหว่าง Sectoral CERT เมื่อวันที่ 24 สิงหาคม 2565 เพื่อยกระดับความมั่นคงปลอดภัยทางไซเบอร์ โดยมี พลเอก ปรัชญา เฉลิมวัฒน์ เลขาธิการคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นประธานกล่าวเปิดประชุม ทั้งนี้ ดร.กิตติ โฆษะวิสุทธิ์ ที่ปรึกษากิตติมศักดิ์และกรรมการ TB-CERT และพลอากาศตรี อมร ชมเชย รองเลขาธิการฯ พร้อมผู้แทน NCERT, TB-CERT, TTC-CERT, TCM-CERT, TI-CERT และ หน่วยงานที่อยู่ระหว่างเตรียมการจัดตั้ง เช่น ผู้แทนสำนักงานข่าวกรองแห่งชาติ (Sectoral CERT ด้านความมั่นคง) ผู้แทนสำนักงานปลัดกระทรวงสาธารณสุข (Sectoral CERT ด้านสาธารณสุข) และ สำนักงานพัฒนารัฐบาลดิจิทัล (GOV-CERT) เข้าร่วมประชุม

Thailand CERTs Community Meeting (TH-CC) was organized according to the policy to promote the capability of cyber security of critical information infrastructure agencies in the public and private sectors to achieve the international standard. The working team of Thailand CERTs Community Meeting (TH-CC) gathered to build a network of collaboration between sectoral CERT. The meeting was held on 24 August 2022 to improve cyber security, chaired by Dr. Prachya Chalermwat, Secretary of the National Cyber Security Committee. The meeting was attended by Dr. Kitti Kosavisutte, Honorary Advisor and Committee, AVM Amorn Chomchoey, Assistant Secretary, representatives from NCERT, TB-CERT, TTC-CERT, TCM-CERT, TI-CERT, and other organizations that were in the process of establishment, such as representatives from Sectoral CERT on National Intelligence, Sectoral CERT on Public Health, and GOV-CERT.



การสนับสนุนการแถลงผลสัมฤทธิ์คณะกรรมการการทหารและความมั่นคงของรัฐ วุฒิสภา และสำนักงานสภาความมั่นคงแห่งชาติ

Supporting the Achievements Declaration of the State Military and Security Commission, the Senate, and the Office of the National Security Council.

การสนับสนุนการกิจการดำเนินการตามยุทธศาสตร์ชาติด้านความมั่นคงและแผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคง โดยร่วมแถลงผลการดำเนินงานของสำนักงานที่แสดงถึงผลสัมฤทธิ์ในการดำเนินงานตามยุทธศาสตร์ชาติด้านความมั่นคงและแผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นความมั่นคง ซึ่งจัดโดยคณะกรรมการการทหารและความมั่นคงของรัฐ วุฒิสภา และสำนักงานสภาความมั่นคงแห่งชาติ

Contributing to the implementation of the National Security Strategy and its Master Plan. This includes having the National Security Strategy's Accomplishment Declaration, which was held by the State Military and Security Commission, the Senate, and the Office of the National Security Council.



การเข้าร่วมการสัมมนา The 5th Edition of the EU - ASEAN Security and Defence Policy Seminar ณ กรุงบรัสเซลล์ ประเทศเบลเยียม

Participating the 5th Edition of the EU - ASEAN Security and Defence Policy Seminar in Brussels, Belgium



สหภาพยุโรป ทั้งการเข้าร่วมสัมมนาดังด้วยตนเอง และผ่านระบบออนไลน์ รวมกว่า 100 คน สำหรับประเทศไทย มีผู้แทนจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กระทรวงกลาโหม และกระทรวงการต่างประเทศ เข้าร่วมการสัมมนาดัง โดยมีประเด็นสำคัญ ได้แก่ ความมั่นคงในบริบทโลก

การสัมมนา The 5th Edition of the EU - ASEAN Security and Defence Policy Seminar ระหว่างวันที่ 24 - 30 มิถุนายน 2565 ณ กรุงบรัสเซลล์ ประเทศเบลเยียม ซึ่งจัดขึ้นโดยกระทรวงการต่างประเทศแห่งสหภาพยุโรป (European External Action Service: EEAS) ร่วมกับ EU Enhancing Security Cooperation In and With Asia (ESIWA) โดยมีวัตถุประสงค์เพื่อการแลกเปลี่ยนแนวคิด ประสบการณ์ และหารือโอกาสและแนวทางสำหรับสหภาพยุโรป และอาเซียนในการดำเนินการร่วมมืออย่างเป็นรูปธรรม มีผู้เข้าร่วมการสัมมนาจากหน่วยงานความมั่นคงของประเทศสมาชิกอาเซียนและ

และภูมิภาคความมั่นคงทางทะเล การรักษาความมั่นคงปลอดภัยไซเบอร์ และปฏิบัติการรักษาสันติภาพและการบริหารวิกฤตการณ์ นอกจากนี้ยังได้พบปะและหารือร่วมกับ DG Miguel de Bruycker ผู้อำนวยการศูนย์ไซเบอร์แห่งประเทศเบลเยียม (Centre for Cybersecurity Belgium: CCB) เพื่อแลกเปลี่ยนแนวคิดและมุมมองเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ประสบการณ์ ปัญหา และอุปสรรคในการจัดตั้งหน่วยงานไซเบอร์ การเสริมสร้างศักยภาพบุคลากรทางไซเบอร์ รวมถึงการดำเนินโครงการ safeonweb ของประเทศเบลเยียม โดยประเทศไทยและประเทศเบลเยียมได้มี

ความคิดเห็นตรงกันที่จะพัฒนาความร่วมมือระหว่างกันให้เป็นรูปธรรมยิ่งขึ้น ด้วยการจัดทำบันทึกความเข้าใจ (Memorandum of Understanding: MoU) ซึ่งจะได้มีการหารือในรายละเอียดร่วมกันต่อไป

The 5th Edition of the EU - ASEAN Security and Defence Policy Seminar was organized during 24 - 30 June 2022 in Brussels, Belgium, hosted by the European External Action Service (EEAS) and the EU Enhancing Security Cooperation In and With Asia (ESIWA). The objective of the seminar was to exchange ideas, share experiences, and discuss the opportunities or ways for concrete collaboration between European Union and ASEAN. More than 100 participants attended the seminar, including representatives of national security agency from ASEAN and European countries, both in person and online. The representatives of Thailand were officials from the NCSA, the Ministry of Defence, and the Ministry of Foreign Affairs. The key themes included global and regional security, maritime security, cybersecurity, peace operations, and crisis management. The NCSA also had a meeting with DG Miguel de Bruycker, Director of the Centre for Cybersecurity Belgium (CCB), to exchange ideas and perspectives on cybersecurity, his experiences, and obstacles

in establishing a new cybersecurity agency, building capacity of cybersecurity workforce, and implementation of Belgium's safeonweb project. Thailand and Belgium agreed to develop a more concrete collaboration through a Memorandum of Understanding (MOU), which will be further discussed later.



การสร้างเครือข่ายสื่อมวลชน พสานความร่วมมือด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์

Creating a network of mass media to achieve collaboration
in maintaining cyber security

การสร้างเครือข่ายสื่อมวลชน พสานความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ร่วมกับชมรมเครือข่ายนักสื่อสารข้อมูลเชิงลึกแห่งประเทศไทย Thailand Data Journalism Network (TDJ) ในการแลกเปลี่ยนข้อคิดเห็นและหารือแนวทางในการร่วมมือกันสร้างความเข้าใจระหว่าง สกมช. และ TDJ ให้ความรู้ ความตระหนักและรับมือกับภัยไซเบอร์ของประชาชน อันจะเป็นการสร้างความตระหนักด้านไซเบอร์และสร้างความเชื่อมั่นในหน่วยงานด้านไซเบอร์ของประเทศให้กับสาธารณชน ณ สมาคมนักข่าวนักหนังสือพิมพ์แห่งประเทศไทย

This event aimed to create a network of mass media to achieve collaboration in maintaining cyber security with Thailand Data Journalism Network (TDJ). The participants shared their opinions and discussed ways to establish an understanding between the NCSA and TDJ, to raise awareness among the public of cyber security, and convince the people to be confident in cyber-related agencies in Thailand. This event was held at the Thai Journalists Association.

จัดเวทีสนทนากลุ่มเพื่อระดมสมองของตัวแทนสื่อมวลชนระดับผู้บริหาร

Organized a seminar to brainstorm ideas with executive representatives of mass media

10

สำนักข่าว
news agencies



การแต่งตั้งคณะทำงานจัดทำแผนรับมือ เหตุภัยคุกคามทางไซเบอร์

Appointment of the working group in making a response plan
for cyber threats

การแต่งตั้งคณะทำงานจัดทำแผนรับมือเหตุภัยคุกคามทางไซเบอร์ เพื่อเป็นกลไกในการรับมือภัยคุกคามทางไซเบอร์ในระดับชาติ ตั้งแต่ระดับไม่ร้ายแรงจนไปถึงระดับวิกฤต ส่งผลให้เกิดการอำนวยความสะดวกการบริหารจัดการเหตุการณ์ความมั่นคงระดับชาติ และประสานความร่วมมือกับเครือข่ายการบริหารเหตุการณ์ภายในประเทศและระหว่างประเทศได้อย่างมีประสิทธิภาพ



A working team was appointed to prepare a response plan for cyber threats as the counter-mechanism against cyber threats at the national level. The plan involves countermeasures from non-critical to critical cyber threat events. The response plan will facilitate the operations to address national security crises and collaboration with domestic and international networks against cyber threats effectively.

4

การเฝ้าระวัง รับมือ

Vigilance and response

การเฝ้าระวัง รับมือภัยคุกคามทางไซเบอร์

Vigilance and response to cyber threats



การเฝ้าระวังเหตุการณ์คุกคามทางไซเบอร์ เพื่อสนับสนุนการปฏิบัติการช่วยเหลือ ของศูนย์ประสานการรักษาความมั่นคง ปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

Vigilance for cyber threats to support operations of the Thai Computer Emergency Response Team

ศูนย์ประสานการรักษาความมั่นคง
ปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ซึ่งเป็น
หน่วยงานในสังกัด สกมช. ต้องเผชิญกับ
ปัญหาความพร้อมด้านบุคลากรและงบประมาณ
แต่ด้วยบทบาทภารกิจ และหน้าที่ ศูนย์ประสาน
การรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์
แห่งชาติ จำเป็นต้องดำเนินงานภายใต้ทรัพยากร
ที่มีอยู่อย่างจำกัด โดยอาศัยความร่วมมือจาก
หลายภาคส่วน

จากข้อมูลสถิติและสถานการณ์ทาง
ไซเบอร์ในห้วงที่ผ่านมา พบว่าเหตุการณ์จำนวน
มากที่หน่วยงานภาครัฐและเอกชนถูกโจมตีแล้วเกิด
ผลกระทบไปถึงความมั่นคงปลอดภัยของข้อมูล
และความเชื่อมั่นของประชาชนในประเทศ การกิจ
ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของ
ศูนย์ประสาน การรักษาความมั่นคงปลอดภัยระบบ
คอมพิวเตอร์แห่งชาติ จึงไม่ถูกจำกัดเฉพาะการ
ปฏิบัติร่วมกับหน่วยงานโครงสร้างพื้นฐานสำคัญ
ทางสารสนเทศ หรือร่วมกับหน่วยงานของรัฐ
เท่านั้น

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคง
ปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ยังมุ่งมั่น
จะแสวงหาความร่วมมือระหว่าง หน่วยงานภาครัฐ
เอกชนรวมถึงภาคประชาชน
เพื่อสามารถเป็นหน่วยงานหลัก
ในการดูแลรักษาความมั่นคง
ปลอดภัยทางไซเบอร์ เฝ้าระวัง
และเตรียมความพร้อมรับมือใน
กรณีที่มีการโจมตีทางไซเบอร์
ให้กับประเทศได้อย่างทันทั่วทั้ง

The Thai Computer Emergency
Response Team (Thai CERT), an agency
under the supervision of the NCSA,
encounters personnel and budget shortage.
Still, Thai CERT manages to perform its
duties successfully thanks to cooperation
and support from several sectors.

According to previous statistics and
cyber situations, there have been several
incidents where public and private
organizations were attacked so critically
that information privacy and public con-
fidence were compromised. Therefore, the
mission of Thai CERT in maintaining cyber
security is not limited only to collaboration
with critical information infrastructure and
government agencies.

Thai CERT is committed to seeking
collaboration with government agencies,
private organizations, and the people sector
as the country's leading agency in
maintaining cyber security, vigilance, and
preparedness for prompt and timely
response to cyberattacks.



สถานการณ์ภัยคุกคามทางไซเบอร์ ในประเทศไทย ปี 2565

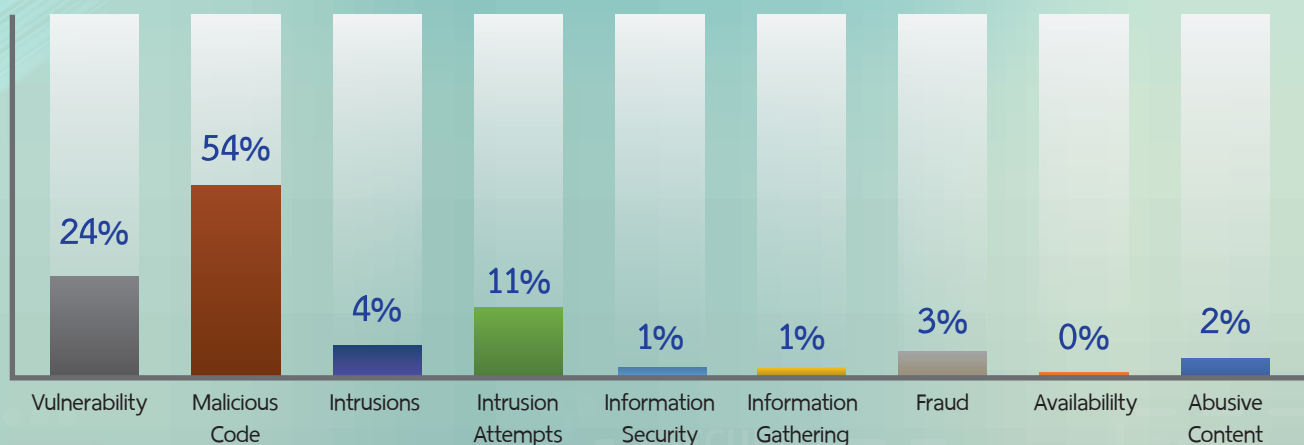
The situation of cyber threats in Thailand in 2022

หน่วย : เหตุการณ์
Unit : Incidents

ประเภทภัยคุกคาม/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
Abusive Content	5	2	5	7	0	1	1	4	6	4	6	6	47
Availability	2	0	0	0	0	0	0	0	0	0	3	7	12
Fraud	13	9	7	6	9	10	6	9	1	0	0	3	73
Information Gathering	4	4	1	0	9	4	1	0	0	0	0	0	23
Information Security	3	1	2	1	6	1	0	1	0	1	2	1	19
Intrusion Attempts	4	13	95	17	7	6	22	6	29	33	18	18	268
Intrusions	14	4	3	23	4	13	4	1	2	0	17	24	109
Malicious Code	96	128	127	111	66	201	126	136	151	50	79	94	1,365
Vulnerability	31	25	35	55	52	106	80	45	48	24	43	57	601
Total	172	186	275	220	153	342	240	202	237	112	168	210	2,517

ตารางที่ 1 : แสดงสถิติภัยคุกคาม เดือน ตุลาคม 2564 – กันยายน 2565 ของ ThaiCERT

Table 1: Statistics of cyber threats from October 2021 – September 2022, Thai CERT



ภาพที่ 1 : แสดงประเภทภัยคุกคามทางไซเบอร์

Figure 1: Types of cyber threats

จากข้อมูลสถิติภัยคุกคามทางไซเบอร์ ในปี 2565 โดย ThaiCERT ปรากฏพบภัยคุกคามทางไซเบอร์ประเภท Malicious Code มากที่สุด 54% รองลงมาคือ ประเภท Vulnerability และ Intrusion Attempts มีสัดส่วนอยู่ที่ 24% และ 11% ตามลำดับ

According to the statistics of cyber threats in 2022 by ThaiCERT, the most common type of cyber threat was malicious code (54%), followed by vulnerability (24%) and intrusion attempts (11%), respectively.

การแจ้งเตือนเหตุการณ์ภัยคุกคาม ให้กับหน่วยงานต่างๆ อย่างเป็นทางการ

Official warnings of cyber threats to other organizations

การแก้ไขปัญหาเกี่ยวกับเหตุการณ์ภัยคุกคามทางไซเบอร์ ในปี 2565 ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ หรือ National CERT ได้สนับสนุนการแก้ไขปัญหาเกี่ยวกับเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

In 2022, the Thai Computer Emergency Response Team (ThaiCERT) supported the solutions to cyber threat incidents. The details are presented below.



การบริหารจัดการคุณภาพ Quality management

1. จัดการอบรมหลักสูตรพนักงานเจ้าหน้าที่ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

Organizing staff training according to the Cyber Security Act B.E. 2562

39
หน่วยงาน
agencies

81
คน
participants

2. สร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ให้กับหน่วยงานต่าง ๆ
Raising awareness of cyber threats to various agencies

29
ครั้ง
times

มีผู้เข้าร่วมทั้งสิ้น
participants
2,978 คน

3. ดำเนินการประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อเป็นการช่วยป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อประชาชน ดังนี้
Coordinating with various agencies to prevent and minimize the risk of cyber threats that affect the people

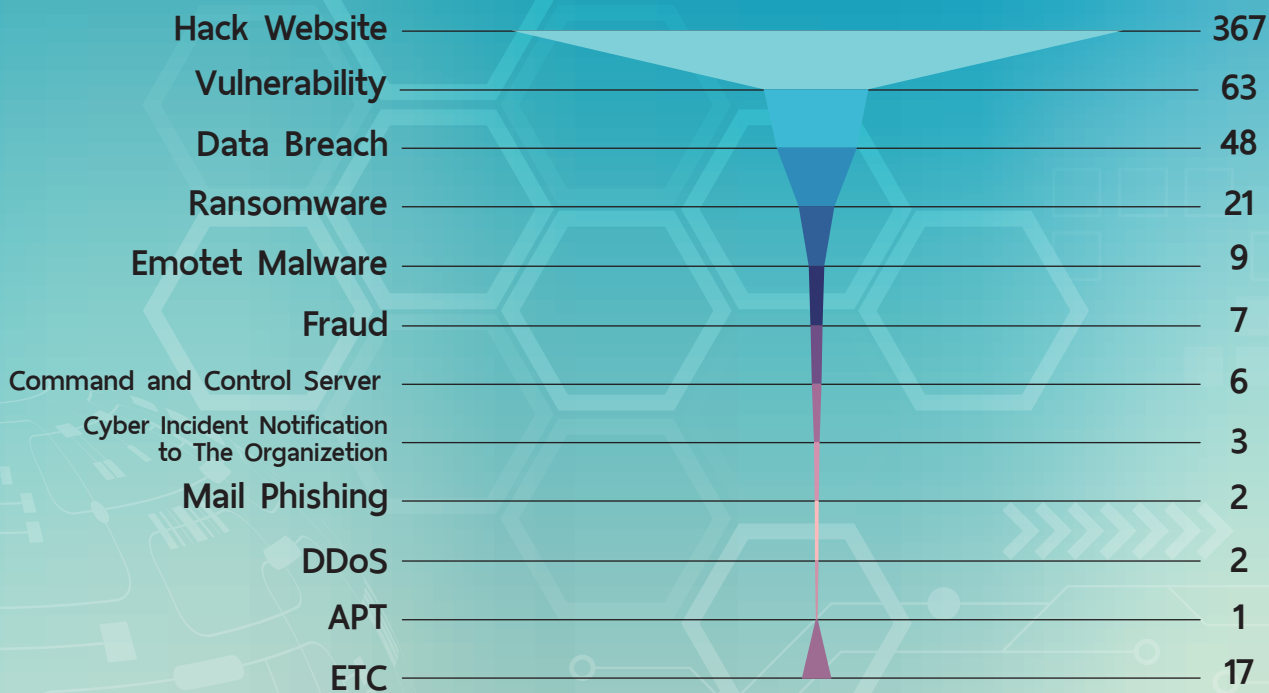
3.1 ให้ดำเนินการกับบริษัทที่มีส่วนเกี่ยวข้องกับเงินกู้ยืมระบบ
Requesting prosecutions against firms involved with informal loans

3.2 ขอให้ระงับการให้บริการผู้ใช้งานแอปพลิเคชันสำหรับสนทนา ที่เกี่ยวกับเงินกู้ยืมระบบ
Requesting suspension of service for chat users involved with informal loans

3.3 ขอให้ระงับหมายเลขโทรศัพท์ที่เกี่ยวข้องกับเงินกู้ยืมระบบ
Requesting suspension of phone numbers involved with informal loans

ภาพรวมภัยคุกคามทางไซเบอร์ที่ NATIONAL CERT ตรวจพบและดำเนินการในปี 2565

Overview of cyber threat incidents detected and settled by ThaiCERT in 2022



กราฟแสดงเหตุการณ์ภัยคุกคามทางไซเบอร์
The graph shows the overview of cyber threat incidents



367

เหตุการณ์ incidents

ประเภท Hacked Website มากที่สุด
The most common type is website hacking



63

เหตุการณ์ incidents

รองลงมาเป็นประเภท จุดอ่อนช่องโหว่
Followed by vulnerability



48

เหตุการณ์ incidents

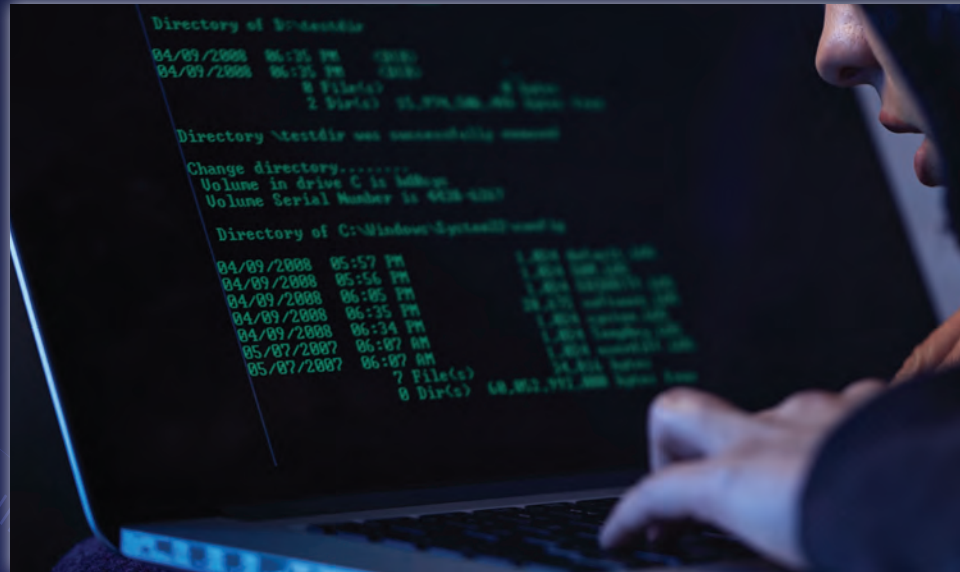
และข้อมูลรั่วไหล
And data breach

ปฏิบัติการสนับสนุนทางไซเบอร์ Cyber Support Operations

PENTESTRATION

การปฏิบัติการเพื่อประเมินความเสี่ยงด้วยการทดสอบเจาะระบบเพื่อค้นหาจุดอ่อนในการเข้าถึงระบบต่างๆ โดยใช้ผู้เชี่ยวชาญ

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



Pentest

7

Units

Va Scan

22

Units

INCIDENT RESPONSE

การปฏิบัติการ เพื่อตรวจสอบหลักฐานให้คำปรึกษาในการช่วยเหลือตอบสนองและรับมือฯ หน่วยงานที่ร้องขอและลงพื้นที่เข้าช่วยเหลือ ตรวจสอบพิสูจน์หลักฐานจัดทำแผนฟื้นฟูหลังการกำจัดเหตุให้กับหน่วยงานที่ร้องขอและทำการติดตามหลังจากให้การช่วยเหลือ

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.

IR

12

Units

follow up

15

Units

สกมช. ให้การช่วยเหลือหน่วยงาน ในการรับมือภัยคุกคามทางไซเบอร์

NCSA assisted various agencies in response to cyber threats

WARNING

การประสานงานเพื่อระงับภัยคุกคามทางไซเบอร์ ในปัจจุบันพบเว็บไซต์หน่วยงานของรัฐถูกปลอมเป็นจำนวนมากโดยผู้ไม่ประสงค์ดี เว็บไซต์ปลอมจะมีเนื้อหาเหมือนกับเว็บไซต์จริง ทำให้เหยื่อหรือผู้เข้าถึงเว็บไซต์หลงเชื่อว่าเป็นเว็บไซต์จริงของหน่วยงาน โดยแก็งคอลเซ็นเตอร์อาจหลอกให้ไปเว็บไซต์เพื่อดาวน์โหลดมัลแวร์ที่เป็นอันตราย สุดท้าย อาจทำให้เงินหมดบัญชี ซึ่งเว็บไซต์ที่ถูกปลอมหรือเลียนแบบ อาทิเช่น เว็บไซต์ DSI และเว็บไซต์ กรมสรรพากร

At present, the websites of many government agencies are being forged into phishing websites by scammers. Phishing websites contain similar content to real ones to trick the victims and visitors into believing they are the official websites. Scam call centers will trick people into visiting their websites to download malware. As a result, victims will lose all money in their accounts. The websites duplicated as phishing websites are, for example, the DSI website and the Department of Revenue website.



ตัวอย่างสถานการณ์อาชญากรรมทางไซเบอร์ ที่กระทบต่อประชาชนและมีความสัมพันธ์กับความมั่นคง ปลอดภัยทางไซเบอร์

Cybercrimes that affected people and cyber security

พบการเลียนแบบเว็บไซต์
ของหน่วยงานราชการเป็นจำนวนมาก
โดยภายในหน้าเว็บไซต์มีลักษณะคล้ายคลึง
กับเว็บไซต์จริง หากมีผู้หลงเชื่อทำการ
ดาวน์โหลดแอปพลิเคชันและติดตั้งโปรแกรม
ที่เป็นอันตรายลงในอุปกรณ์โทรศัพท์มือถือ
ก็จะถูกขโมยข้อมูล

จากสถานการณ์ดังกล่าว สกมช.
ได้ประสานงานเพื่อขอระงับการเผยแพร่
เว็บไซต์ปลอม เพื่อป้องกันความเสียหายต่อ
ประชาชน

รวมจำนวน amount

43

เว็บไซต์ Website



There have been many phishing websites that look like official websites of government agencies. If people are tricked into downloading malicious applications or malware on their mobile phones, their data will be pirated.

Due to the aforementioned situation, the NCSA has coordinated with relevant parties to shut down such phishing websites to prevent damage to the public.

กรณี SMS โดยใช้ Sender Name เหมือนกับหน่วยงาน ตัวอย่างเช่น คนร้ายสวมรอยปลอมเป็น call center ของ E-commerce platform

A summary of phishing on E-commerce platforms in 3 steps

1 เริ่มต้นด้วยการส่ง SMS ใช้ Sender Name เหมือนกับ Platform เพื่ออ้างตัวเป็น Call Center ให้เหยื่อคลิก
ที่มีมัลแวร์หรือให้เพิ่มเพื่อน เพื่อเอา Username, Password, Pin code ของเหยื่อ

A scammer starts by sending an SMS using the sender's name that resembles the call center of a famous E-commerce platform. The SMS will lure the victim into clicking on a link that contains malware or ask the victim to add friends to acquire the victim's username, password, and pin code.

2 ใช้ข้อมูลส่วนตัวที่ได้ Log in เป็นเจ้าของบัญชี ไปซื้อสินค้าออนไลน์ ที่สามารถเปลี่ยนสภาพ เป็นเงินได้
เช่น บัตรเติมเกมออนไลน์

They will use the personal data the owner has used to log in to purchase online products that can be cashed, such as online game credit.

3 แล้วจึงถ่ายโอนไปที่คนร้าย ทั้งหมด ใช้เวลาเพียงไม่กี่นาทีหลังจากคนร้ายเข้าถึงบัญชีเหยื่อได้

All the credit will be transferred to the scammer's account. It takes only a few minutes after the scammer accesses the victim's account.

แนวโน้มสถานการณ์ภัยคุกคามทางไซเบอร์ ในห้วงปี 2565

The trend of cyber threat situation in 2022

พบการโจมตีด้วยการแฮกเว็บไซต์ มากกว่าการโจมตีรูปแบบอื่นๆ คิดเป็น 2 ใน 3 ของการโจมตีทางไซเบอร์ที่ตรวจพบในประเทศไทย เช่น การโจมตีในลักษณะทำไปเพื่อการแฝงหน้าเว็บพบนอนไลน์ในเว็บไซต์ ของหน่วยงาน เพื่อเพิ่มโอกาสและประสิทธิภาพการค้นหาผ่าน SearchEngine, การโจมตีโดยเปลี่ยนแปลงหน้าเว็บไซต์ (Website Defacement) ของหน่วยงานเพื่อใช้เป็นพื้นที่ทดสอบความสามารถของแฮกเกอร์หรือแสดงการเคลื่อนไหวทางการเมือง นอกจากนี้ ยังพบการโจมตีด้วยการแฮกเว็บไซต์แบบอื่นๆ ที่น่าสนใจ เช่น การสร้างหน้าเว็บไซต์เพื่อหลอก Phishing อยู่บนเว็บไซต์ หน่วยงานของรัฐ และการฝังมัลแวร์อันตรายบนหน้าเว็บไซต์หน่วยงานที่อาจหลอกให้ผู้เข้าถึงดาวน์โหลดไปติดตั้งได้

Website hacking is two or three times more common than other cyberattacks in Thailand. For example, some attacks intended to disguise online gambling websites on official websites for search engine optimization. Other cyberattacks defaced official websites. These were meant as a showoff of hacker skills or political movements. There were also other intriguing hacking activities, such as phishing on official websites and concealing malware on official websites that trick visitors into downloading dangerous applications.



การโจมตีที่อาจสร้างความเสียหายให้กับหน่วยงานต่างๆ และอาจใช้เวลาในการแก้ไขมากที่สุด ได้แก่ Ransomware โดยได้รับรายงานว่า มักเกิดเหตุขึ้นกับภาครัฐที่มีความสำคัญ หรือเอกชนที่เป็นธุรกิจขนาดใหญ่ในหลายประเภทอุตสาหกรรม

The cyberattack that might cause the most damage and take recovery time is ransomware. It was reported that ransomware occurred to major government agencies or large private organizations in many industries.

รายงานประจำปี 2565

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)



หน่วยงานด้านการศึกษา และหน่วยงานด้านสาธารณสุข เป็นหน่วยงานประเภทที่มีจำนวนหน่วยงานถูกโจมตีทางไซเบอร์สูงสุด โดยเฉพาะเว็บไซต์ที่ใช้เป็นสื่อประชาสัมพันธ์ที่เปิดให้บริการอยู่เป็นจำนวนมาก

Websites of educational and public health agencies were most hit by cyberattacks, especially those used by many people.





5

การพัฒนา

Development

การพัฒนาบุคลากรด้านความมั่นคงปลอดภัย
ไซเบอร์และสร้างการตระหนักรู้ให้กับประชาชน

Development of cyber security personnel
and public awareness

การจัดอบรมเพื่อสร้างความตระหนักรู้ ให้กับประชาชนทั่วไป

Cybersecurity Knowledge Sharing

Cyber Security Knowledge Sharing

สกมช.ดำเนินการจัดอบรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Knowledge Sharing) ในหัวข้อที่เป็นปัจจุบันและทันสมัยต่อเหตุการณ์ ซึ่งจัดขึ้นเป็นประจำทุกเดือน เพื่อสร้างความตระหนักรู้ให้กับเยาวชนและประชาชนทั่วไปให้รู้เท่าทันภัยไซเบอร์ที่พัฒนาไปอย่างรวดเร็วและหลากหลายรูปแบบ

The NCSA organized training on cyber security, focusing on up-to-date topics. The training is organized monthly to raise cyber security awareness among youths and the general public. This training call CyberSecurity Knowledge Sharing.

โดยมีผู้เข้าร่วมอบรมในระบบออนไลน์
With more than 22,000 online participants

มากกว่า **22,000** คน

CYBER SECURITY KNOWLEDGE SHARING 15

PDPA
Personal Data Protection Act

วันจันทร์ที่ 28 มีนาคม 2565 13.00 - 15.00 น.

ลงทะเบียนและรับชมผ่านทาง
Zoom
Facebook: NCSA Thailand
LIVE

QR Code

ศูนย์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โทร: 0-2142-8886 | อีเมล: academic@ncsa.or.th

Personal Data
Protection Act
: PDPA

CYBER SECURITY KNOWLEDGE SHARING 19

STOP BULLYING จะดีกว่าไหม... ถ้าเราให้เกียรติกัน

วันเสาร์ที่ 2 กรกฎาคม พ.ศ. 2565 เวลา 13.00 - 15.00 น.

ผู้เข้าร่วมอบรมจะได้รับวุฒิบัตร
เมื่อเข้าร่วมอบรมและผ่านเกณฑ์
การทดสอบออนไลน์ 80% ขึ้นไป

สิทธิพิเศษ!! สำหรับผู้เข้าร่วมอบรม

สนับสนุน
โดย

QR Code

ศูนย์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โทร: 0-2142-8886 | อีเมล: academic@ncsa.or.th

Stop Bullying
จะดีกว่าไหม...ถ้าเราให้
เกียรติกัน

Security Concerns in Using Blockchains and Smart Contracts

CYBER SECURITY KNOWLEDGE SHARING #17

Security Concerns in Using Blockchains and Smart Contracts

📅 วันอังคารที่ 10 พฤษภาคม พ.ศ. 2565 🕒 เวลา 13.30 - 15.30 น.

👤 **พลเอก ดร.ปรีชา เเล้ววัฒน**
เลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

👤 **นายวิชาญ นพ. ชนเดช**
รองเลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

👤 **ดร.พิชญ์ นพ. นาน**
นักวิจัยอาวุโส ศูนย์วิจัย
เทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

👤 **คุณสิริวิทย์ ทวีทอง**
CTO & Co-Founder บริษัท Inspex

👤 **คุณวิรัตน์ ทวีทอง**
COO & Co-Founder บริษัท Inspex

📱 **ลงทะเบียนและรับชมผ่านทาง**
Zoom: [https://nca.zoom.us/j/9101111111](#)
Facebook Live: [https://www.facebook.com/NCSA.Thailand](#)
QR Code:

📞 ศูนย์ประสานงาน: 0-2142-6885 | อีเมล: academ@nca.go.th

ระบบ DNS (Domain Name System) ทางรอด!!!...ช่วยลด ปัญหาการหลอกลวง

CYBER SECURITY KNOWLEDGE SHARING #21

Domain Name System
ทางรอด...ช่วยลดปัญหาการหลอกลวง

📅 วันพุธที่ 7 กันยายน พ.ศ. 2565 🕒 เวลา 13.30 - 15.30 น.

👤 **คุณจตุพร พงษ์**
ประธานคณะกรรมการป้องกันและปราบปราม
การทุจริตแห่งชาติ (ปปช.)

👤 **คุณชยา อภิรัตน์**
นักวิจัยอาวุโส ศูนย์วิจัย
เทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

👤 **พลอากาศตรี นพ. ชนเดช**
รองเลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

👤 **พลเอก ดร.ปรีชา เเล้ววัฒน**
เลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

📱 **ลงทะเบียนและรับชมผ่านทาง**
Zoom: [https://nca.zoom.us/j/9101111111](#)
Facebook Live: [https://www.facebook.com/NCSA.Thailand](#)
QR Code:

📞 ศูนย์ประสานงาน: 0-2142-6885 | อีเมล: academ@nca.go.th

ภัยไซเบอร์จากระบบ Remote Working

วัยเกษียณยุคใหม่ ห่วงไกลภัยไซเบอร์

การยกระดับมาตรฐาน CII
ตาม พ.ร.บ. ไซเบอร์



Cybersecurity Knowledge Sharing

รู้เท่าทันภัยคุกคามทางไซเบอร์ฉบับพนักงาน
มืออาชีพ : Cybersecurity for professional
employees

Data Layer Protection

Infrastructure ในรูปแบบ Multi-Cloud
กับความสัมพันธ์ด้าน Cybersecurity

ควอนตัมคอมพิวเตอร์ - ประโยชน์
ภัยคุกคาม และการรับมือ

การจัดอบรมเพื่อสร้างความตระหนักรู้ ให้กับประชาชนทั่วไป

Cyber Security Knowledge Sharing

การจัดอบรมเยาวชนรุ่นใหม่รู้เท่าทันภัยไซเบอร์ Cyber Security Literacy Training for Youths

การจัดอบรมเยาวชนรุ่นใหม่รู้เท่าทันภัยไซเบอร์ เพื่อเป็นการสร้างความรู้ความเข้าใจกับนักเรียนระดับประถมศึกษา มัธยมศึกษา และนิสิต/นักศึกษาทั่วประเทศ ให้ตระหนักถึงภัยที่อาจเกิดขึ้นจากการใช้อินเทอร์เน็ตและเทคโนโลยี พร้อมเรียนรู้วิธีป้องกันภัยคุกคามทางอินเทอร์เน็ตในเบื้องต้น และสามารถนำความรู้ที่ได้รับไปถ่ายทอดแก่ผู้ปกครองและบุคคลรอบข้างได้ อีกทั้งเป็นการสร้างภูมิคุ้มกันภัยทางไซเบอร์โดยภาพรวมให้กับสังคมไทย ตลอดจนเป็นการสร้างแรงบันดาลใจให้กับเยาวชน นักเรียน นักศึกษา เกิดความสนใจอาชีพด้านความมั่นคงปลอดภัยไซเบอร์ นำไปสู่การพัฒนาศักยภาพและเพิ่มบุคลากรด้านไซเบอร์ของประเทศในอนาคตอีกด้วย



มีเยาวชนเข้าร่วม
มากกว่า **9,000** คน
With more than 9,000 youths attending



The cyber security training for youth aims to establish knowledge and understanding of cyber security among students in primary schools, high schools, and universities across the country to be aware of the dangers when using the Internet and modern technology. The training also offers basic ways to protect themselves from online threats. The knowledge from this training can be transferred to their parents and the people around them. This training can improve cyber immunity in Thai society and inspire young people and students to be interested in cyber security careers, eventually leading to improving cyber security capability and personnel of the country in the future.

กิจกรรมอบรมเยาวชนรุ่นใหม่รู้เท่าทันภัยไซเบอร์ (ระดับประถมศึกษา)

รู้...ซี CYBER

วันพุธที่ 14 กันยายน 2565 เวลา 08:00 - 09:00 น.

ผู้เข้าร่วมอบรมจะได้รับวุฒิบัตร เมื่อเข้าร่วมอบรมและผ่านเกณฑ์การทดสอบออนไลน์ 60% ขึ้นไป

อีกรฟิคะ!! สู้รับของรางวัล

วิทยากร: คุณนันทกร พงษ์ทอง รองอธิบดีฯ NCSA
"ความรู้เบื้องต้นเกี่ยวกับความปลอดภัยไซเบอร์"

วิทยากร: คุณนันทกร พงษ์ทอง รองอธิบดีฯ NCSA
"การรู้เท่าทันสื่อ"

QR Code: <https://www.ncsa.go.th>

Facebook Live: NCSA Thailand

Supported by: NCSA, THNCA, and others.

ศูนย์ความเป็นเลิศ สาขาวิชาการวางแผนความปลอดภัยไซเบอร์แห่งชาติ โทรศัพท์ 0-2142-6885

กิจกรรมอบรมเยาวชนรุ่นใหม่รู้เท่าทันภัยไซเบอร์ (ระดับประถมศึกษา)

รู้...ซี CYBER

วันพุธที่ 14 กันยายน 2565 เวลา 13:00 - 16:00 น.

ผู้เข้าร่วมอบรมจะได้รับวุฒิบัตร เมื่อเข้าร่วมอบรมและผ่านเกณฑ์การทดสอบออนไลน์ 60% ขึ้นไป

อีกรฟิคะ!! สู้รับของรางวัล

วิทยากร: คุณนันทกร พงษ์ทอง รองอธิบดีฯ NCSA
"ความรู้เบื้องต้นเกี่ยวกับความปลอดภัยไซเบอร์"

วิทยากร: คุณนันทกร พงษ์ทอง รองอธิบดีฯ NCSA
"การรู้เท่าทันสื่อ"

วิทยากร: คุณนันทกร พงษ์ทอง รองอธิบดีฯ NCSA
"การรู้เท่าทันสื่อ"

วิทยากร: คุณนันทกร พงษ์ทอง รองอธิบดีฯ NCSA
"การรู้เท่าทันสื่อ"

QR Code: <https://www.ncsa.go.th>

Facebook Live: NCSA Thailand

Supported by: NCSA, THNCA, and others.

ศูนย์ความเป็นเลิศ สาขาวิชาการวางแผนความปลอดภัยไซเบอร์แห่งชาติ โทรศัพท์ 0-2142-6885

กิจกรรมอบรมเยาวชนรุ่นใหม่รู้เท่าทันภัยไซเบอร์ (ระดับประถมศึกษา)

รู้...ซี CYBER

วันพุธที่ 14 กันยายน 2565 เวลา 09:00 - 12:00 น.

ผู้เข้าร่วมอบรมจะได้รับวุฒิบัตร เมื่อเข้าร่วมอบรมและผ่านเกณฑ์การทดสอบออนไลน์ 60% ขึ้นไป

อีกรฟิคะ!! สู้รับของรางวัล

วิทยากร: คุณนันทกร พงษ์ทอง รองอธิบดีฯ NCSA
"ความรู้เบื้องต้นเกี่ยวกับความปลอดภัยไซเบอร์"

วิทยากร: คุณนันทกร พงษ์ทอง รองอธิบดีฯ NCSA
"การรู้เท่าทันสื่อ"

วิทยากร: คุณนันทกร พงษ์ทอง รองอธิบดีฯ NCSA
"การรู้เท่าทันสื่อ"

วิทยากร: คุณนันทกร พงษ์ทอง รองอธิบดีฯ NCSA
"การรู้เท่าทันสื่อ"

QR Code: <https://www.ncsa.go.th>

Facebook Live: NCSA Thailand

Supported by: NCSA, THNCA, and others.

ศูนย์ความเป็นเลิศ สาขาวิชาการวางแผนความปลอดภัยไซเบอร์แห่งชาติ โทรศัพท์ 0-2142-6885

Academic services on cyber security



The NCSA realizes the importance of cyber security and aims to improve the capability of cyber security personnel. Academic services on cyber security help disseminate and share knowledge on cyber security. Cyber security personnel can apply the knowledge to their organizations, whether in the public or private sectors, such as Maejo University, Burapha University, the Ministry of Foreign Affairs, Nissan Motor (Thailand) Co., Ltd., and Microsoft Thailand Co., Ltd.



การสร้างความรู้ความตระหนักถึงการรักษาความมั่นคงปลอดภัยไซเบอร์

Raising awareness of maintaining cyber security



สทช.ได้มีการจัดนิทรรศการให้ความรู้กับหน่วยงาน องค์กร โรงเรียนต่างๆ มีวัตถุประสงค์ เพื่อเผยแพร่ความรู้และสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่กลุ่มเป้าหมายต่างๆ ทั้งภาครัฐและเอกชน นักเรียน นิสิต นักศึกษา และประชาชนทั่วไป อาทิ งาน “เทคโนโลยีก้าวล้ำ นวัตกรรมก้าวหน้า วิทยาศาสตร์นำพา พัฒนาสุขภาวะกายใจ” ณ โรงเรียนสาธิตแห่งมหาวิทยาลัยเกษตรศาสตร์ งานนวัตกรรมภูมิปัญญาผู้สูงอายุ สร้างงาน สร้างอาชีพ ณ ศูนย์ราชการเฉลิมพระเกียรติฯ แจ้งวัฒนะ และงาน Defense & Security 2022 ณ ศูนย์ประชุมอิมแพคเมืองทองธานี

The NCSA organized exhibitions to disseminate knowledge to agencies, organizations, and schools and raise awareness of cyber security to various target groups in the public and private sectors, students, and the general public. For example, the “Advanced Technology, Advanced Innovation, and Science-led Physical and Mental Health” exhibition was held at Kasetsart University Laboratory School. The Elderly Wisdom Innovation for Careers was held at Chaeng Watthana Government Complex. The Defense & Security 2022 Exhibition was held at the IMPACT Exhibition and Convention Center.

การเร่งรัดการพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ ระยะที่ 1 Intensive Cybersecurity Capacity Building Program)

Intensive Cybersecurity Capacity Building Program Phase 1

การพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ในทุกกระดับที่มีประสิทธิภาพให้มีการพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ในระยะเร่งด่วน สนับสนุนการดำเนินงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

Building the capacity of cyber security personnel at all levels urgently to support the operations under the Cyber Security Act B.E. 2562 (2019)



กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
Ministry of Digital Economy and Society

ภาพรวมการพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์

Overview of cyber security personnel development

การอบรมเชิงปฏิบัติการหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์

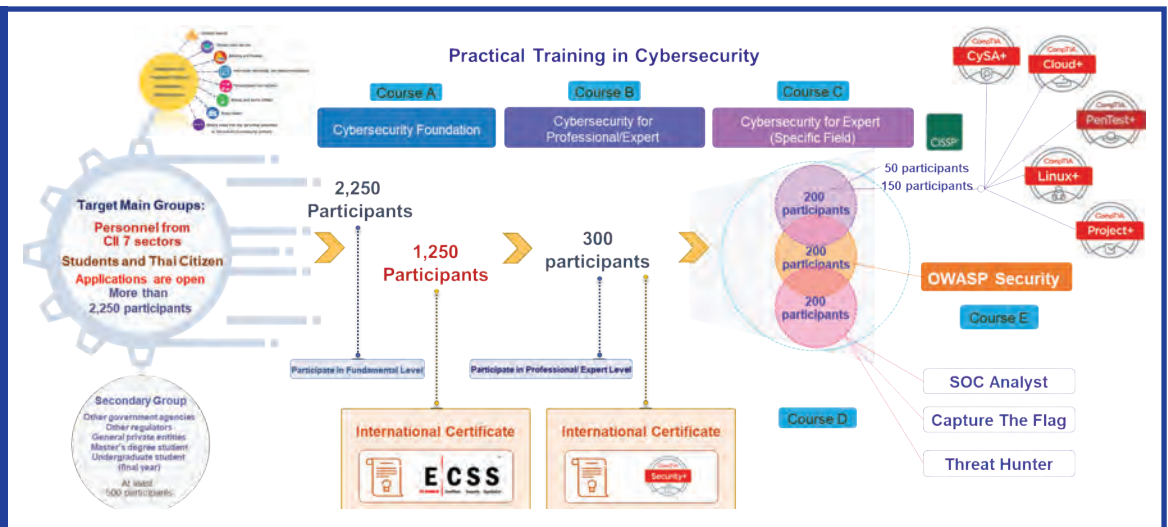
Workshop training on cyber security

เป้าหมายดำเนินโครงการ

Target of the project

เริ่มโครงการ เมื่อ พฤษภาคม 2564

Starting in May 2021



ผลสำเร็จของโครงการ

Achievements of the project

เป้าหมายที่ตั้งไว้

3,200 คน

ผู้เข้าร่วมอบรมรวม
4,169 คน

Target 3,200 participants

Actual participants 4,169 people

ผลสัมฤทธิ์ของการพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์

Achievements of cyber security personnel development

Course D&E: หลักสูตรระดับผู้เชี่ยวชาญ ภาคปฏิบัติ D&E Course Advanced Program Workshop	ECSS Course A: หลักสูตรระดับพื้นฐาน Course A: Basic program	หลักสูตรระดับผู้บริหาร Executive Program	Course B: หลักสูตรระดับผู้เชี่ยวชาญ Course B: Advanced Program	Course C: หลักสูตรระดับผู้เชี่ยวชาญเฉพาะด้าน Course C: Specialized Program
เป้าหมาย 400 คน ผู้เข้าร่วมอบรมรวม 450 คน	เป้าหมาย 2,250 คน ผู้เข้าร่วมอบรมรวม 2,867 คน	เป้าหมาย 50 คน ผู้เข้าร่วมอบรมรวม 69 คน	เป้าหมาย 300 คน ผู้เข้าร่วมอบรมรวม 599 คน	เป้าหมาย 200 คน ผู้เข้าร่วมอบรมรวม 224 คน
Target 400 participants Actual participants 450 people	Target 2,250 participants Actual participants 2,867 people	Target 50 participants Actual participants 69 people	Target 300 participants Actual participants 599 people	Target 200 participants Actual participants 224 people

การแข่งขันทักษะทางไซเบอร์ Thailand Cyber Top Talent 2022

Thailand Cyber Top Talent 2022



สทศ. จัดการแข่งขัน Thailand Cyber Top Talent 2022 ในรูปแบบ Capture the flag เป็นปีที่ 2 เพื่อมุ่งหวังให้เป็นกิจกรรมผลักดันและขับเคลื่อนให้ประเทศไทยเกิดการพัฒนาระบบและเพิ่มจำนวนบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับความต้องการของประเทศ โดยมีเป้าหมายเป็นนักเรียน นิสิต นักศึกษา และประชาชนทั่วไป ที่เข้าร่วมการแข่งขัน เกิดการเรียนรู้ พัฒนาทักษะ และประสบการณ์ ให้กลายเป็นบุคลากรที่มีความรู้ความสามารถทัดเทียมในระดับสากล และเป็นการสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางด้านไซเบอร์ให้กับบุคคลทั่วไปมากขึ้น ตลอดจนเป็นการสร้างบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ออกสู่ตลาดแรงงานในอนาคตอีกด้วย

ซึ่งในปีนี้มีจำนวนทีมที่เข้าร่วมแข่งขันทั้งสิ้น

There are totally

393 ทีม
Teams

มีผู้เข้าแข่งขันมากกว่า

With more than 1,138 competitors

1,138 คน



ระดับมัธยมศึกษา

(Junior 166 ทีม)

116 teams in the junior level
487 competitors

จำนวน **487** คน

The NCSA held Thailand Cyber Top Talent 2022. It was a "Capture the Flag" competition aimed at developing cyber security personnel for Thailand to serve the country's demand. The target group was students and the general public who participated in the competition to develop skills and experience toward the international level. This competition also helped raise the awareness of cyber threats for the public and produce a cyber security workforce for the labor market in the future.

ระดับอุดมศึกษา (Senior 110 ทีม)

110 teams in the senior level 325 competitors

จำนวน **325** คน

ระดับประชาชนทั่วไป

117 teams in the open level 326 competitors

(Open 117 ทีม)

จำนวน **326** คน

การสนับสนุนและเข้าร่วมประชุม กับหน่วยงานภายนอก

Supporting and attending meetings with external agencies



สทกมช. ได้สนับสนุนบุคลากรเข้าร่วมการประชุมในโอกาสต่างๆ ที่เกี่ยวข้องตามคำเชิญของหน่วยงาน อาทิ การประชุมประชาคมไซเบอร์กองทัพไทย ครั้งที่ 4/2565 การประชุมพิจารณาแนวทางการดำเนินงานของ Regulator ด้านสาธารณสุขและการประชุมคณะกรรมการประเมินผลการฝึกการบริหารวิกฤตการณ์ระดับชาติ ประจำปี 2565 ครั้งที่ 2/2565 เป็นต้น

The NCSA deployed its representatives to attend meetings on various occasions upon invitation, such as the 4/2564 Cyber Community Meeting of the Royal Thai Army, the Review of Operation Guideline of Public Health Regulator, and the 2/2565 Subcommittee Meeting on Evaluation of National Crisis Management.



การบรรยายพิเศษร่วมกับภาคีเครือข่าย ในการเพิ่มทักษะและพัฒนาขีดความสามารถ ให้กับบุคลากรหน่วยงานควบคุมหรือกำกับ ดูแล หน่วยงานของรัฐ และหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

Special lectures with network partners in developing and enhancing competencies for personnel in regulatory agencies, government agencies, and critical information infrastructure organizations



CompTIA

จัดอบรมร่วมกับ The Computing Technology Industry Association (CompTIA)

- หัวข้อ "Two Sides of Same Coin: Investigating Critical Penetration Testing and Security Analytic Skills"
- การ Workshop: "Peeling back the onion: Taking Security Onion into battle"



kaspersky

จัดอบรมร่วมกับ Kaspersky Lab Singapore Pte. Ltd.

- หัวข้อ "Building a Safer Future for Thailand"



MANDIANT

จัดอบรมร่วมกับ Mandiant Thailand

- หัวข้อ "Briefing - HIVE Ransomware"



TREND MICRO

จัดอบรมร่วมกับ บริษัท เทรนด์ไมโคร (ประเทศไทย) จำกัด

โครงการความร่วมมือทางวิชาการเพื่อพัฒนาบุคลากรด้านไซเบอร์ จำนวน 3 หลักสูตร

- หลักสูตร Build a Strong Security Awareness Program (General), (Train The Trainer)
- หลักสูตร Next Gen Information Security Leaders
- หลักสูตร Cyber Security Capability Skill Building
- หัวข้อ "การคาดการณ์แนวโน้มและทิศทางของภัยคุกคามทางไซเบอร์ในปี พ.ศ. 2565"
- หัวข้อ "รายงานสถานการณ์ความปลอดภัยทางไซเบอร์สำหรับครึ่งแรกของปี พ.ศ. 2565" แนวทางการปกป้องพื้นที่การโจมตีที่ขยายตัวเพิ่มขึ้น



Microsoft

จัดอบรมร่วมกับ บริษัท ไมโครซอฟท์ (ประเทศไทย) จำกัด

- หัวข้อ "Microsoft Women@Cybersecurity"



จัดอบรมร่วมกับ สมาคมไอเอสซิสแควร์ ภาคพื้นที่กรุงเทพมหานคร

- หัวข้อ "(ISC)² Bangkok Chapter: August Event 2022"

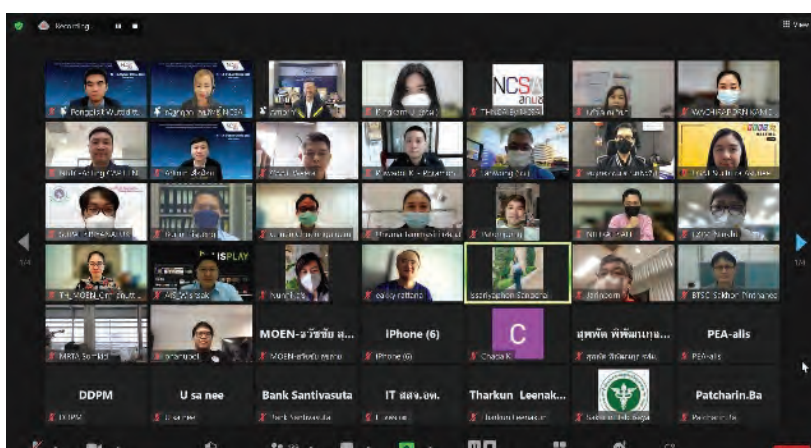


การจัดอบรมเพื่อเพิ่มทักษะและพัฒนา ขีดความสามารถให้กับบุคลากรหน่วยงาน ควบคุมหรือกำกับดูแล หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทาง สารสนเทศ (NCSA Cyber clinic)

Special lectures with network partners in developing and enhancing competencies for personnel of regulatory agencies, government agencies, and critical information infrastructure organizations (NCSA Cyber clinic)

สทศ.จัดอบรมต่อเนื่องตลอดทั้งปี เพื่อพัฒนาและยกระดับทักษะความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้กับบุคลากรหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และผู้แทนจากหน่วยงานที่สนใจ

The NCSA organized training (Cyber Clinic) continuously throughout the year to develop knowledge in cyber security for personnel regulatory agencies, government agencies, critical information infrastructure organizations, and representatives of interested organizations.



โดยมีผู้เข้าร่วมมากกว่า
With more than 1,800 participants

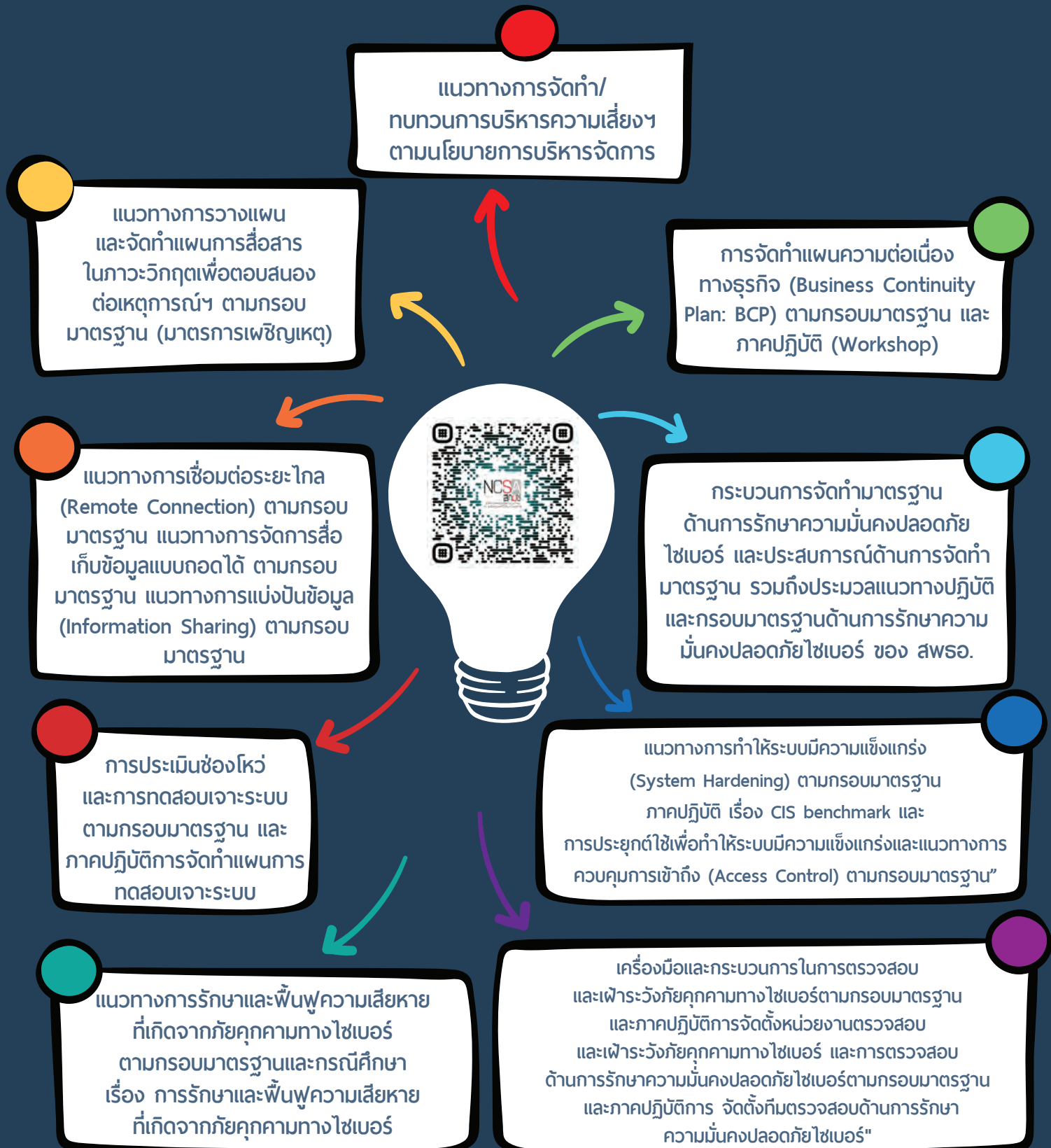
1,800 คน

จำนวนชั่วโมงรวมกว่า
Total training period more than 5,500 hours

5,500 ชั่วโมง

การจัดอบรมเพื่อเพิ่มทักษะและพัฒนาขีดความสามารถให้กับบุคลากร หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานของรัฐ และหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (NCSA Cyber clinic)

Special lectures with network partners in developing and enhancing competencies for personnel in regulatory agencies, government agencies, and critical information infrastructure organizations (NCSA Cyber Clinic)



6

การยกระดับ

Upgrading

การยกระดับหน่วยงานโครงสร้างพื้นฐานสำคัญ
ทางสารสนเทศและหน่วยงานของรัฐ

Upgrading critical information infrastructure agencies
and government agencies

Assessment Security for Critical Information Infrastructure Agencies and Government Agencies

The NCSA conducted a study to assess preparedness as the foundation to minimize the risks of cyberattacks against various organizations. The security assessment will assist agencies and organizations in outlining the strategies, measures, or response guidelines for preventing the risk of cyber threats that may compromise national security.



Countdown ประมวลแนวทางปฏิบัติและ กรอบมาตรฐานด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศ

A countdown to systematize the code of practice and frameworks
for cyber security maintenance for government agencies and
critical information infrastructure agencies

กิจกรรม Countdown ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เมื่อวันที่ 6 กรกฎาคม 2565 โดยมีผู้เข้าร่วมกิจกรรมรวมทั้งสิ้น 287 คน ทำให้ได้ทราบถึงแนวทางการดำเนินงานให้เป็นไปตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

A countdown activity was organized to systematize the guideline practice and frameworks for maintaining cyber security for government agencies, regulatory agencies, and critical information infrastructure agencies on 6 July 2022, with 287 participants to be aware of and comply with the notifications issued by the Cybersecurity Regulating Committee.

กิจกรรม Countdown
ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคง
ปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงาน
โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

08.55 น. กล่าวรายงาน โดย พลเอก ดร.ประยุทธ์ เจริญวัฒน์
เลขาธิการคณะกรรมการการรักษาความมั่นคง
ปลอดภัยไซเบอร์แห่งชาติ

นายชัชวาลย์ รณามานุสรณ์
รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

09.05 น. กล่าวเปิดงาน โดย นายชัชวาลย์ รณามานุสรณ์
รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

09.15 น. เสวนาเรื่อง แนวทางการดำเนินงานของหน่วยงานของรัฐ
และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
ตามประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและ
กรอบมาตรฐานฯ และแนวทางการดำเนินการของ
Sectoral CERT ตามประกาศ กนช. เรื่อง ลักษณะ: หน้าที่
และความรับผิดชอบของศูนย์ประสานฯ
โดย ตัวแทนหน่วยงานควบคุมหรือกำกับดูแล /
ตัวแทน Sectoral CERT / ผู้เชี่ยวชาญ จาก กนช.

10.40 น. เสวนาเรื่อง เครื่องมือสนับสนุนให้หน่วยงานของรัฐ
และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
สามารถปฏิบัติตามประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติ
และกรอบมาตรฐานฯ และ Sectoral CERT สามารถปฏิบัติ
ตามประกาศ กนช. เรื่อง ลักษณะ: หน้าที่และความรับผิดชอบของ
ศูนย์ประสานฯ

วันพุธที่ 6 กรกฎาคม 2565
รับชมผ่านช่องทาง
Facebook Live : NCSA Thailand

การให้คำปรึกษาด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์

Giving consultations on cyber security

สกมช.ได้ดำเนินการให้คำปรึกษา
แก่หน่วยงานต่าง ๆ ผ่านช่องทาง

The NCSA gives consultations to various
organizations via

cii@ncsa.or.th

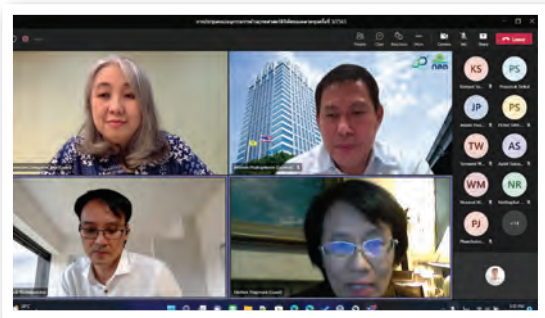
มีจำนวนหน่วยงาน **11** หน่วยงาน
With 11 organizations

จำนวนเคส **15** เคส
Having 15 cases

และผ่านช่องทางการประชุมและ
บรรยาย

And through meetings and lectures

มีจำนวนหน่วยงาน **27** หน่วยงาน
With 27 organizations



การพัฒนาขีดความสามารถกระบวนการปฏิบัติงานด้านไซเบอร์ตามมาตรฐานสากลของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

Development of cyber security competencies of critical information infrastructure agencies

การพัฒนาขีดความสามารถกระบวนการปฏิบัติงานด้านไซเบอร์ตามมาตรฐานสากลของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีการจัดอบรมหลักสูตรผู้นำการปฏิบัติการ(Lead Implementor) และหลักสูตรผู้นำตรวจสอบ (Lead Auditor) เพื่อส่งเสริมและสนับสนุนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ระหว่างวันที่ 9 พฤษภาคม 2565 ถึง 2 กันยายน 2565 จำนวนทั้งสิ้น

- Lead Implementor 4 รุ่น 230 คน
- Lead Auditor 3 รุ่น 138 คน

Training programs were organized for lead implementors and lead auditors to support the cyber operation competencies of critical information infrastructure agencies toward the international standard. The training courses extended from 9 May 2023 to 2 September 2023, including

- Four lead implementor training courses with a total of 230 participants
- Three lead auditor training courses with a total of 138 participants

หลักสูตรผู้นำการปฏิบัติ
ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

Lead Implementor

เพื่อเป็นการสร้างความเข้าใจเกี่ยวกับหลักการและสาระสำคัญของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และการจัดทำเอกสาร กระบวนการ การบริหารรักษาความมั่นคงปลอดภัยไซเบอร์

เปิดรับสมัคร "รุ่นที่ 1 - 3" รับสมัคร ตั้งแต่ 25 เมษายน 65 เป็นต้นไป รับจำนวนจำกัดรุ่นละ 55 ท่าน (ไม่รับค่าใช้จ่าย)

ลงทะเบียน รุ่นที่ 1
วันที่ 9 - 13 พฤษภาคม พ.ศ. 2565

ลงทะเบียน รุ่นที่ 2
วันที่ 17 - 20 / 23 พฤษภาคม พ.ศ. 2565

ลงทะเบียน รุ่นที่ 3
วันที่ 20 - 24 มิถุนายน พ.ศ. 2565

ลงทะเบียน รุ่นที่ 4
วันที่ 18 - 22 กรกฎาคม พ.ศ. 2565

ความรู้พื้นฐานที่ผู้เข้าอบรมควรมี

- มีความเข้าใจเบื้องต้นเกี่ยวกับข้อกำหนดในการมาตรฐานระบบบริหาร จัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001
- มีความเข้าใจเบื้องต้นเกี่ยวกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

บุคลากรที่รับผิดชอบ
ผู้รับผิดชอบหลักสูตร
ผู้รับผิดชอบหลักสูตร
ผู้รับผิดชอบหลักสูตร
ผู้รับผิดชอบหลักสูตร

สอบถามข้อมูลเพิ่มเติมได้ที่ โทร: 06-5240-5405 e-mail: contact@it-fit.com

หลักสูตรผู้นำตรวจสอบ
ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

LEAD AUDITOR

เพื่อเป็นการเสริมสร้างทักษะ การวางแผน การเตรียมตัว ก่อนการตรวจ การดำเนินการตรวจ การรายงานผลการตรวจประเมินระบบบริหารความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ให้แก่องค์กรที่จำเป็นต้องได้รับการตรวจประเมินความสอดคล้องตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ 2562

ความรู้พื้นฐานที่ผู้เข้าอบรมควรมี

- มีพื้นฐานด้านเทคโนโลยีกฎหมายดิจิทัล
- มีทักษะการเป็นผู้ตรวจสอบ (จะเป็นประโยชน์)

ลงทะเบียน รุ่นที่ 1
วันที่ 25 - 27 กรกฎาคม / 1 - 2 สิงหาคม พ.ศ. 2565

ลงทะเบียน รุ่นที่ 2
วันที่ 6 - 19 สิงหาคม พ.ศ. 2565

ลงทะเบียน รุ่นที่ 3
วันที่ 29 - 31 สิงหาคม 1 - 2 กันยายน พ.ศ. 2565

เปิดรับสมัคร "รุ่นที่ 1 - 3" รับสมัคร ตั้งแต่ 25 เมษายน 65 เป็นต้นไป รับจำนวนจำกัดรุ่นละ 45 ท่าน (ไม่รับค่าใช้จ่าย)

สอบถามข้อมูลเพิ่มเติมได้ที่ โทร: 06-5240-5405 e-mail: contact@it-fit.com

บุคลากรที่รับผิดชอบ
ผู้รับผิดชอบหลักสูตร
ผู้รับผิดชอบหลักสูตร
ผู้รับผิดชอบหลักสูตร

การจัดทำร่างมาตรฐานวิชาชีพ ผู้ปฏิบัติงานด้านไซเบอร์

Preparation of Cybersecurity Professional Standard



มีการจัดทำร่างมาตรฐานวิชาชีพผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นการกำหนดมาตรฐานวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งจะส่งผลต่อการพัฒนาบุคลากรด้านไซเบอร์การจัดการศึกษาอบรม การกำหนดการฝึกทักษะ รวมไปถึงการพัฒนาการจัดการศึกษาให้สอดคล้องกับตำแหน่งงาน และการเจริญเติบโตตามสายงานที่เกี่ยวข้อง



The standard of the cybersecurity profession was drafted as the guideline for this career. It will be helpful in developing cyber security personnel, skill and knowledge training, and education design to be suitable for the positions and promotion in related professions.



การฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ Thailand's National Cyber Exercise 2022

Thailand's National Cyber Exercise 2022

การฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ Thailand's National Cyber Exercise 2022 ระหว่างวันที่ 22-24 ธันวาคม 2564 มีการจัดฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ เพื่อให้หน่วยงานที่เข้าร่วมการฝึกมีความรู้ความเข้าใจเพิ่มมากขึ้นเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 โดยมีผู้แทนจากหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จำนวน 66 หน่วยงาน รวมจำนวนทั้งสิ้น 486 คน

Thailand's National Cyber Exercise 2022 was organized from 22 – 24 December 2021 to test the cyber competencies of critical information infrastructure agencies and educate the participating agencies about cyber threats according to the Cyber Security Act B.E. 2562 (2019). The event was attended by 486 participants from 66 critical information infrastructure agencies.



การจัดงาน Prime Minister Awards : Thailand Cybersecurity Excellence Award 2022

Prime Minister Awards: Thailand Cybersecurity Excellence Award 2022

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้เล็งเห็นถึงความสำคัญในการยกระดับความสามารถของหน่วยงานภาครัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) หน่วยงานเอกชน รวมไปถึงหน่วยงานอื่น ๆ จึงได้ดำเนินการจัดกิจกรรม Prime Minister Awards: Thailand Cybersecurity Excellence Awards 2022 เพื่อส่งเสริมการดำเนินงาน และ ทำกับดูแลตลอดจนสร้างความตระหนัก และ การรับรู้ถึงภัยคุกคามทางไซเบอร์ให้สอดคล้องกับกับแนวทางของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และเป็นไปตามมาตรฐานสากล

ทั้งนี้ สกมช. ได้เชิญกรรมการผู้ทรงคุณวุฒิ ด้านต่าง ๆ หลากหลายสาขาอาชีพ พิจารณาประเมินเกณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์จะเป็นการอ้างอิงจากพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และ ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่องประมวลแนวทางปฏิบัติ และ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐ และ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 และ ในเกณฑ์ประเมินด้านความร่วมมือและด้านการพัฒนาศักยภาพ เป็นการอ้างอิงจากดัชนีตัวชี้วัดระดับการพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ระดับโลก (The Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ในหัวข้อการพัฒนาศักยภาพ (Capacity Development) และหัวข้อความร่วมมือ (Cooperative)

ทั้งนี้ ในปี พ.ศ. 2565 มีหน่วยงานที่เข้าร่วมจำนวนทั้งสิ้น 127 หน่วยงาน ซึ่งจากการพิจารณาของคณะกรรมการผู้ทรงคุณวุฒิที่ สกมช. ได้แต่งตั้งขึ้นมา



The National Cyber Security Agency (NCSA) acknowledges the necessity to improve the competencies of government agencies, CII agencies, and other private organizations. The Prime Minister Awards: Cybersecurity Excellence Awards 2022 was organized to promote the operations and regulations, to raise awareness of cyber threats according to the Cyber Security Act B.E. 2562, and to achieve international standards.

Honorary judges were invited from several professional disciplines. The criteria of cyber security were referenced from the Cyber Security Act B.E. 2562 and the Notification of the National Cyber Security Committee on the procedures, guideline practice, and standards for maintaining cyber security for government agencies and critical information infrastructure agencies B.E. 2564 (2021). The criteria of



กรรมการตัดสินรางวัล



ดร.ปริญญญา หอมเอนก

ประธานกรรมการ

ผู้ทรงคุณวุฒิด้านการรักษาความมั่นคงปลอดภัยไซเบอร์



นายไพบุลย์ อมรวิญญูเกียรติ

กรรมการ

ผู้ทรงคุณวุฒิด้านกฎหมาย



รศ.ดร.สุดสงวน จามสุริยโรจน์

กรรมการ

อาจารย์ประจำกลุ่มวิชาวิทยาการคอมพิวเตอร์
คณะเทคโนโลยีสารสนเทศและการสื่อสาร (ICT)
มหาวิทยาลัยมหิดล



ดร.น.พ.บดินทร์ ทรัพย์สมบูรณ์

กรรมการ

อาจารย์ประจำวิชาคณะแพทยศาสตร์ศิริราชพยาบาล
มหาวิทยาลัยมหิดล



ดร.ศิวรักษ์ คิวโมภธรรม

กรรมการ

ผู้อำนวยการศูนย์เทคโนโลยีเพื่อความมั่นคงของประเทศ
และการประยุกต์เชิงพาณิชย์ (NSD) สวทช.



นายชัชวณันท์ อัครวงศ์

กรรมการ

ประธานกรรมการศูนย์ประสานงานด้านความมั่นคงปลอดภัย
เทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT)



ดร.ชาลี วรกุลพัฒน์

กรรมการ

หัวหน้าทีมวิจัยความมั่นคงปลอดภัยสารสนเทศ
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
(NECTEC)

เพื่อพิจารณามีหน่วยงานที่ผ่านการประเมิน
ด้านความมั่นคงปลอดภัยและได้รับใบประกาศเกียรติคุณ
สำหรับหน่วยงานที่มีการดำเนินงานด้านความมั่นคงปลอดภัย
ไซเบอร์เป็นเลิศ (Certificate of Cyber safety)
จำนวน

36

หน่วยงาน
agencies

รวมถึงมีหน่วยงานที่ได้รับโล่รางวัลตามประเภทต่าง ๆ

Trophies were given to

23

หน่วยงาน
agencies

31

รวมทั้งสิ้น
Totally 31 awards
รางวัล



collaboration and capacity development were
referenced from the Global Cybersecurity Index
(GCI) by the International Telecommunication
Union (ITU) in the topics of Capacity Development
and Cooperative.

In 2022, a total of 127 participated in
the event. As a result of the judgments by
the honorary judges appointed by the NCSA
some agencies passed the qualifications on
cyber security and were awarded with the
Certificate of Cyber Safety.



องค์กรที่มีสมรรถนะสูง

High-performance organization

การพัฒนา สกมช. สู่การเป็นองค์กรที่มีสมรรถนะสูง
Developing NCSA into a high-performance organization

7

การจัดทำแผนกลยุทธ์การบริหาร และพัฒนาบุคลากร **ระยะ 3 ปี** (พ.ศ. 2565-2567)

Preparation of a three-year management strategy and personnel development plan (2022 – 2024)

วิสัยทัศน์ Vision

บริหารงานบุคคลและสร้างมาตรฐานการพัฒนาบุคลากรในทุกด้าน
ให้พร้อมปฏิบัติการทึงในการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับประเทศ

Personnel management and well-rounded human resources development
to be prepared for cyber security operations for the country



การพัฒนาขีดความสามารถ การปฏิบัติงานของบุคลากรของสำนักงาน

Development of operational competencies of the NCSA staff

การพัฒนาขีดความสามารถ
การปฏิบัติงานของบุคลากรของสำนักงาน
ได้จัดให้มีการพัฒนาขีดความสามารถ
การปฏิบัติงานของบุคลากรของสำนักงาน
ภายในอย่างต่อเนื่อง และตามความสนใจ
ของบุคลากร เพื่อส่งเสริมการเรียนรู้ใหม่ ๆ

Operational competency

development activities are organized
continuously to improve the skills
of the NCSA staff based on their
interests and promote learning new
things.



สภมช. จัดกิจกรรม CSR สร้างคุณค่ากลับสู่สังคม Corporate Social Responsibility (CSR)

NCSA organized corporate social responsibility (CSR) activities to return benefits to society



วาดภาพ วาดอนาคตเด็กไทย รู้ทันภัยไซเบอร์

เมื่อวันที่ 3 สิงหาคม 2565
ณ โรงเรียนวัดปรมาภัยกาฬ
อำเภอปากเกร็ด จังหวัดนนทบุรี

Painting of Thai children's future and cyber literacy
On 3 August 2022 At Wat Poramaiyikawat School
Pak Kret District, Nonthaburi



ทำบ้านปลา (ซึ่งเขือก) บ้านหอย (อ๊ะปะ)

เมื่อวันที่ 31 พฤษภาคม 2565
ณ ศูนย์ศึกษาธรรมชาติป่าชายเลน
อ่าวคุ้งกระเบน อำเภอกำแพง จังหวัดจันทบุรี

Making fish houses and clam houses
On 31 May 2022 At Kung Krabaen Bay Royal
Development Study Center
Tha Mai District, Chanthaburi



บำเพ็ญประโยชน์

เมื่อวันที่ 16 กุมภาพันธ์ 2565
ณ วัดชลประทานรังสฤษดิ์
พระอารามหลวง จังหวัดนนทบุรี

Volunteer activity
16 February 2022
At Wat Chonprathanrangsarit
A royal temple, Nonthaburi



ปันความสุขน้อง ๆ ผู้พิการทางสายตา

เมื่อวันที่ 16 สิงหาคม 2565
ณ โรงเรียนสอนคนตาบอด มกุฏคีรีวัน (เขาใหญ่)

Happiness Sharing with Visually
Impaired Children
16 August 2022
At Makut Khiriwan School for the Blind



นิทรรศการ ภัยใต้แนวคิด KUS stay cyber safe

ให้ความรู้ด้านภัยไซเบอร์
เมื่อวันที่ วันที่ 24- 25 สิงหาคม 2565
ณ โรงเรียนสาริตแห่งมหาวิทยาลัยเกษตรศาสตร์

Exhibition: KUS Stay Cyber Safe
Education about cyber threats
on 24 - 25 August 2022
Kasetsart University Laboratory School

การอบรมและสัมมนาเพื่อพัฒนาศักยภาพ ของผู้ปฏิบัติงานรักษาความมั่นคงปลอดภัยไซเบอร์

Training and seminars to develop the competencies of cyber security personnel



การอบรมและสัมมนาเพื่อพัฒนาศักยภาพของผู้ปฏิบัติงานรักษาความมั่นคงปลอดภัยไซเบอร์ มีวัตถุประสงค์เพื่อพัฒนาความรู้และความสามารถในการปฏิบัติงานของผู้ปฏิบัติงานในสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยมุ่งเน้นการเพิ่มความรู้และทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การทำงานเป็นทีมที่มีประสิทธิภาพ การสร้างความไว้วางใจซึ่งกันและกัน การสื่อสารที่มีประสิทธิภาพ การพัฒนากระบวนการคิด (Growth Mindset) และการเสริมสร้างภาวะการเป็นผู้นำให้ผู้ปฏิบัติงาน

การจัดอบรมเพื่อพัฒนาทักษะการสื่อสารภาษาอังกฤษ ภายใต้อชื้อ

The English communication training was entitled

“โครงการพัฒนาทักษะการสื่อสาร ภาษาอังกฤษสำหรับผู้ปฏิบัติงานของ สกมช.”

“English Communication Skill Development Training for NCSA Staff”

ในห้วงเดือนมิถุนายน – กันยายน 2565

From June – September 2022



The training and seminars to develop the competencies of cyber security personnel were aimed at improving NCSA staff's knowledge and operational capacity, particularly cyber knowledge, mutual trust, effective communication, growth mindset, and leadership skills.

ใบประกาศนียบัตรด้านไซเบอร์ที่พนักงานสำนักงาน คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

The Cyber Certificate was given to employees at
the National Cyber Security Agency (NCSA)

จากพนักงาน สกมช. จำนวน

Out of 41 employees

41

 คน

ประกาศนียบัตรสากล ขั้นสูง รับรองผู้ปฏิบัติงานด้านความมั่นคง
ปลอดภัยไซเบอร์ CASP+

Advanced international certificate for cyber security personnel CASP+

9

คน
employees

คิดเป็นร้อยละ

21.95

 percent

ประกาศนียบัตรสากล ขั้นกลาง สำหรับผู้ที่ปฏิบัติงานในด้านการรับมือ
เหตุการณ์ภัยคุกคาม CompTIA CySA+

Intermediate international certificate for cyber threat response personnel
CompTIA CySA+

12

คน
employees

คิดเป็นร้อยละ

29.26

 percent

ประกาศนียบัตรสากล ขั้นกลาง ด้านการเจาะระบบ CompTIA PenTest+

Intermediate international certificate for CompTIA PenTest+

15

คน
employees

คิดเป็นร้อยละ

36.59

 percent

ประกาศนียบัตรไซเบอร์ หลักสูตรพื้นฐาน

ความรู้ที่จำเป็นในการปฏิบัติงานทางด้านไซเบอร์ CompTIA Security+

Basic cyber certificate for necessary knowledge for cyber operations
CompTIA Security+

35

คน
employees

คิดเป็นร้อยละ

85.36

 percent

การสร้างวัฒนธรรมถ่ายทอดองค์ความรู้ และพัฒนาบุคลากรภายใน

Creating a culture of knowledge transfer and internal human resources development

การสร้างวัฒนธรรมถ่ายทอดองค์ความรู้และพัฒนาบุคลากรภายใน สกมช.อย่างต่อเนื่อง เพื่อให้เกิดการพัฒนาความรู้เพิ่มศักยภาพในการปฏิบัติงานตามภารกิจของสำนักงาน โดยจัดขึ้นทุกวันพุธ ของสัปดาห์

The culture of knowledge transfer and internal human resources development is gradually and continuously enhanced to improve the effectiveness of operations according to the mission. The culture is repeated on Wednesdays.

จำนวนรวมทั้งสิ้น Totally

33

หัวข้อ topics



พล.อ. ปรัชญา เจริญวัฒน์
ลธ. กมช.

JOIN US
เข้าร่วมผ่าน LINK ZOOM ด้านล่าง

KM Wednesday Talk

January 2022
Wednesday Talk
14.00 น.

5 Jan อาชญากรรมทางเทคโนโลยี
อาชญากรรมทางเทคโนโลยีคืออะไร มาเรียนรู้กับคุณเจม (สกม.) พ.ต.ท.สุระพงษ์ เหลาฤทธิ์

12 Jan Cloud security
Cloud security คืออะไร ทำไมถึงกลายเป็นกรอบความปลอดภัยใหม่ของโลกไซเบอร์ โดย Guest Speaker (สป.)

19 Jan Agile Process
Agile Process คืออะไร วิธีการทำงานแบบนี้จะนำไปสู่ประสิทธิภาพในการทำงานมากขึ้นหรือไม่ และวิธีการนี้จะเหมาะกับพวกเรา สกมช. หรือไม่ โดย สบก. นำมาพบกับ Guest Speaker (คุณเม่น ภัฏฐา ภัฏฐา)

26 Jan Leadership : Trust
Leadership Academy การเสริมทักษะคุณสมบัตินักบริหารผู้นำ Version 1 : Trust & Empathy เป้าหมายเรื่องราว โดย คุณเมย์ HR (สกม.)

ระบบ Back Office เพื่อสนับสนุนบริหารจัดการภายในสำนักงาน

The Back Office System to support internal management

การนำ ระบบ Back Office ช่วยสนับสนุนบริหารจัดการภายในสำนักงาน เพื่อให้กระบวนการทำงานมีความรวดเร็วและมีประสิทธิภาพ รวมถึงมีความมั่นคงปลอดภัยไซเบอร์ โดยมีรายละเอียดดังนี้

The Back Office System is introduced to support the internal management for fast and efficient operations and cyber security. The details are as follows:

1.1 ระบบโครงสร้างสารสนเทศพื้นฐาน (System Infrastructure)

1) จัดหาเครื่องคอมพิวเตอร์สำนักงานสำหรับผู้ปฏิบัติงานในสำนักงาน และชุดคำสั่งพื้นฐานสำหรับสำนักงาน

1) Office computers were acquired for office workers and installed with basic office commands.

2) ให้บริการระบบแชร์ไฟล์กลางของสำนักงาน NCSA Drive ให้แก่ผู้ปฏิบัติงานในสำนักงาน เพื่อเพิ่มความสะดวกในการแชร์ข้อมูลสำหรับการปฏิบัติงาน และลดปัญหาด้านความปลอดภัยของการใช้งาน Thumb Drive ที่มีความเสี่ยงด้านไวรัสและมัลแวร์

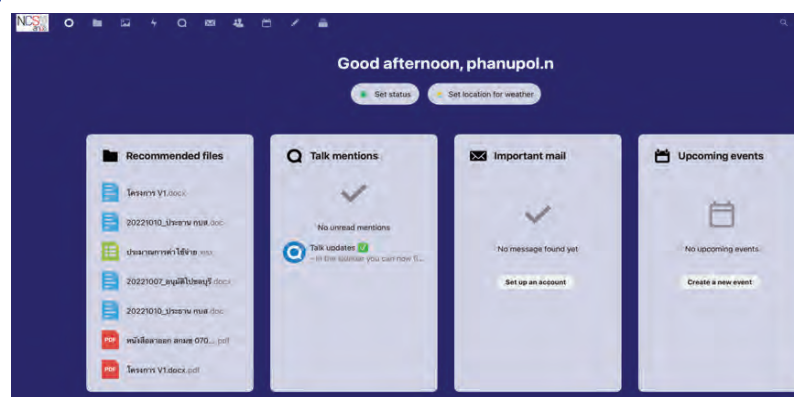
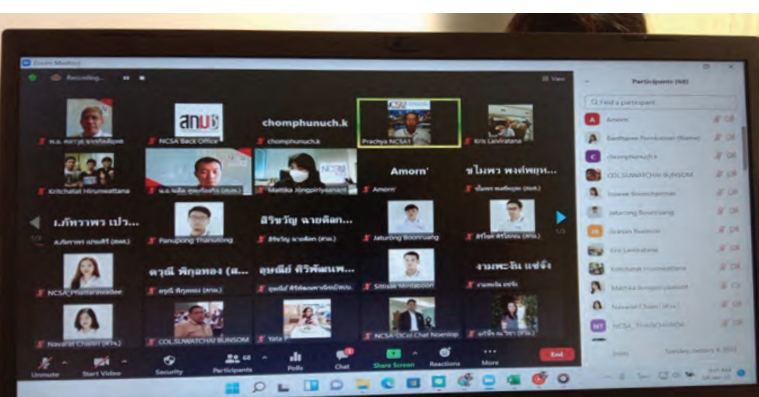
2) Files are shared in the NCSA drive to facilitate NCSA staff to share their data and provide more safety instead of using thumb drives, which are more vulnerable to viruses and malware.

3) จัดทำเอกสารขออนำอุปกรณ์ส่วนตัวเข้าใช้งานภายในสำนักงาน (BYOD) พร้อมกับลงทะเบียน พร้อมตรวจสอบความมั่นคงปลอดภัยให้แก่ผู้ปฏิบัติงานภายในสำนักงาน

3) The documentation system of BYOD (Bring Your Own Device) was established together with the registration system. Cyber security was verified for NCSA staff.

4) จัดหาและดูแลระบบซอฟต์แวร์ช่วยสนับสนุนการปฏิบัติการ ได้แก่ ระบบการประชุมออนไลน์ ระบบสารบรรณอิเล็กทรอนิกส์ ระบบอีเมลของสำนักงาน ระบบการจัดการบริหารงานบุคคล เป็นต้น

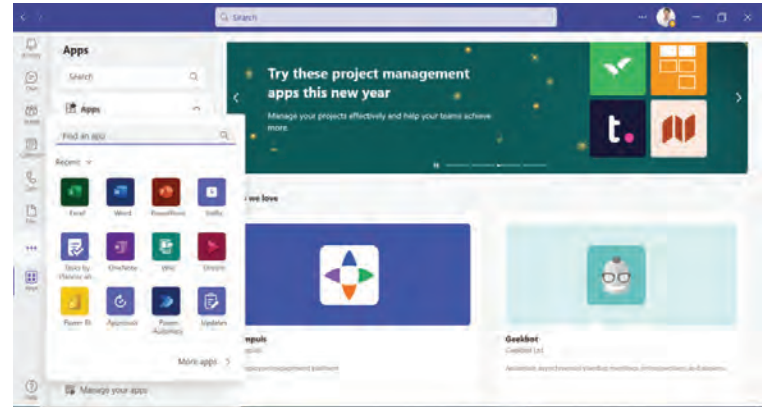
4) Supportive software and programs were acquired and administered, such as online meeting platforms, an electronic correspondence system, official emails, and a personnel management system.





5) จัดทำและให้บริการระบบ Active Directory สำนักงานพร้อมทั้งจัดสรรหมวดหมู่ของสำนักงาน และสิทธิในการเข้าถึงข้อมูลตามกลุ่ม (Role-base Access)

6) จัดหาและสนับสนุนอุปกรณ์รวมถึงเจ้าหน้าที่ที่มีความสามารถในการทำสื่อ การประชุมสัมมนา ระบบการถ่ายทอดสด ที่เกี่ยวกับการเผยแพร่ข้อมูลข่าวสาร ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์



5) An active directory system was established, along with agency categorization and role-based access.

6) Equipment and personnel were procured and supported to produce media, organize seminars and meetings, and live broadcasting related to cyber security

1.2 ระบบเครือข่ายคอมพิวเตอร์ (Computer Network)

1.) จัดสรรและแบ่งสัดส่วนระบบเครือข่ายคอมพิวเตอร์สำนักงาน โดยแบ่งเป็นสัดส่วน ได้แก่

1. ผู้ใช้งานภายในสำนักงาน
2. ผู้ใช้งานภายนอกผู้มาติดต่อที่เข้ามาใช้งานระบบสารสนเทศภายในสำนักงาน
3. ระบบโทรศัพท์สำนักงาน
4. ระบบกล้องวงจรปิด
5. โซนปลอดภัยพิเศษ (DMZ)
6. ระบบเครือข่ายของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (NCERT)

2.) ให้การบริการเครือข่ายไร้สาย WIFI ให้ครอบคลุมพื้นที่สำนักงาน

3.) ให้บริการเครื่องพิมพ์เอกสารผ่านระบบเครือข่ายคอมพิวเตอร์ด้วยระบบสารสนเทศขององค์กร

4. ให้บริการระบบโทรศัพท์สำนักงานด้วยระบบ IP-PHONE ที่รองรับระบบรับสายอัตโนมัติ (IVR)

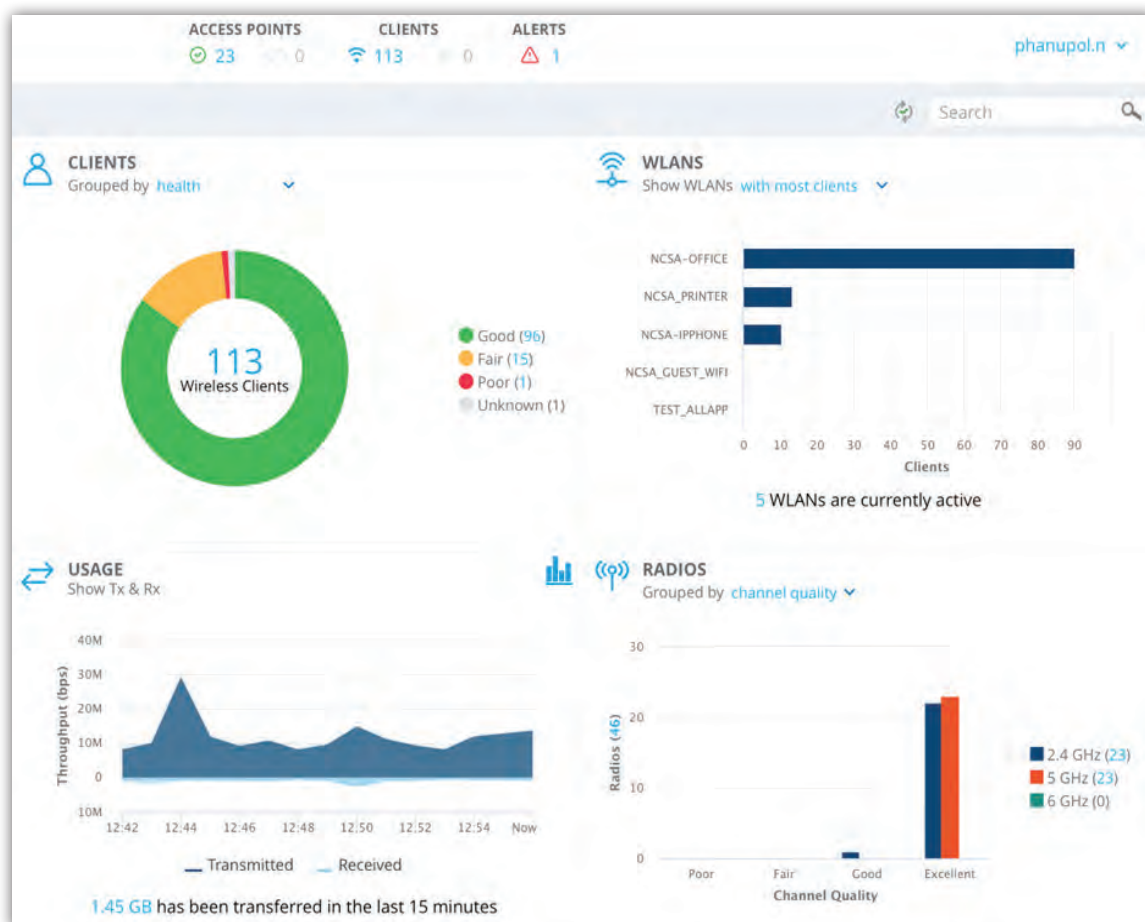
1) The office computer network was allocated for different users:

1. NCSA internal users
2. Visitors using the NCSA's internal IT system
3. Internal phone
4. Surveillance cameras
5. Demilitarized zone (DMZ)
6. The network system of the National Computer Emergency Response Team (NCERT)

2) WIFI service that covers the entire office area

3) Printer service through the computer network using the internal IT system

4) IP-PHONE with IVR support



1.3 ระบบด้านความมั่นคงปลอดภัยไซเบอร์ในส่วนของสำนักงาน (Internal cyber security system of NCSA)

1.) ติดตั้งระบบการป้องกันและตอบสนองต่อเหตุการณ์ที่มีความเสี่ยงทางไซเบอร์แก่เครื่องคอมพิวเตอร์สำนักงาน (End-Point Detection and Responses)

2.) ติดตั้งอุปกรณ์อินเทอร์เน็ตเกตเวย์ด้วย Next-Gen Firewall พร้อมทั้งจัดการความเสี่ยงในการป้องกัน Threat, Anti-Virus, Web Filtering และ Application Control

3.) ติดตั้ง DNS Sinkhole เพื่อใช้ในการกรอง Advertisement และ Tracking บางส่วน

1) Install an End-Point Detection and Responses system

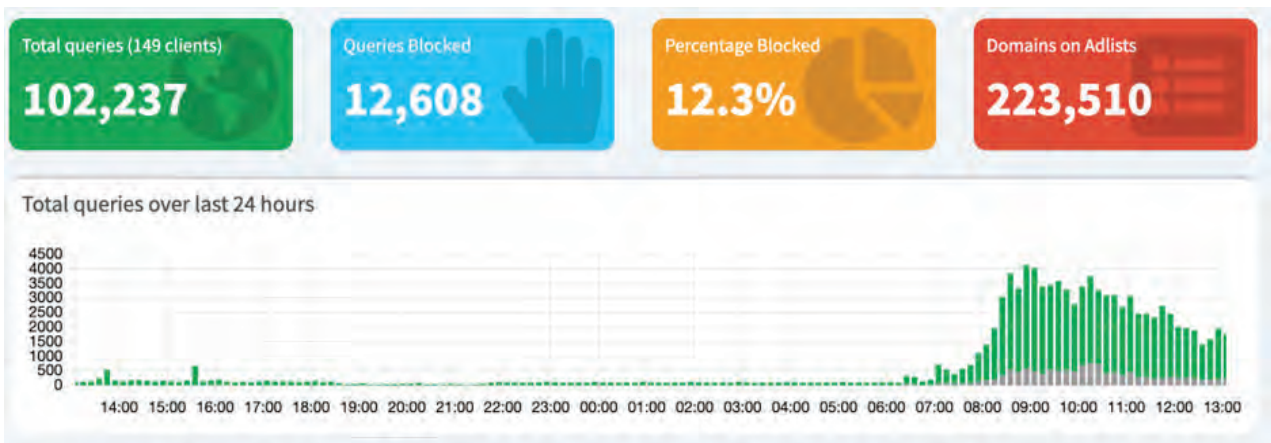
2) Install the internet gateway equipment using the Next-Gen Firewall and other threat protection systems, such as antivirus, web filtering, and application control

3) Install the DNS Sinkhole to filter some advertisements and tracking.

จากฐานข้อมูลกว่า From the database of more than

200,000

domains



การจัดทำแผนการตรวจสอบภายในระยะ 5 ปี (ปีงบประมาณ พ.ศ. 2565 – 2569)

Preparation of the 5-year Internal Audit Plan (Fiscal Years 2022-2026)

ฝ่ายตรวจสอบภายในได้จัดทำแผนการตรวจสอบภายในระยะยาวประจำปีงบประมาณ พ.ศ. 2565 – 2569 เพื่อเป็นทิศทางของการปฏิบัติงานตรวจสอบ และสอดคล้องกับเป้าหมาย โดยดำเนินการภายใต้มาตรฐานการตรวจสอบภายใน และนโยบายตามข้อ 16 (2) ของข้อบังคับคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)



The Internal Audit Division prepared a long-term audit plan for the fiscal years 2022-2026 as the guideline practice for audits and compliance with the goals. The audits will be conducted according to the internal audit standard and Item 16 (2) of the policy of the Executive Board of the Office of NCSA (EBO).

การจัดทำกฎบัตรคณะกรรมการตรวจสอบสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้จัดทำกฎบัตรคณะกรรมการตรวจสอบสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อเป็นแนวทางในการดำเนินงานของคณะกรรมการตรวจสอบให้มีประสิทธิภาพ และประสิทธิผล สร้างความมั่นใจแก่ทุกฝ่ายว่าสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีการบริหารความเสี่ยง และระบบการควบคุมภายในที่ดี และเหมาะสม



The NCSA prepared the charter of the auditors of the NCSA as the operation guideline for effective, efficient, and reliable outcomes to ensure that the NCSA manages risks and has appropriate internal control systems.



รายงานการเงิน



รายงานของผู้สอบบัญชีรับอนุญาต

เสนอ คณะกรรมการบริหาร

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ความเห็น

ข้าพเจ้าได้ตรวจสอบรายงานการเงินของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งประกอบด้วยงบแสดงฐานะการเงิน ณ วันที่ 30 กันยายน 2565 งบแสดงผลการดำเนินงานทางการเงิน และงบแสดงการเปลี่ยนแปลงสินทรัพย์สุทธิ/ส่วนทุนสำหรับปีสิ้นสุดวันเดียวกันและหมายเหตุประกอบงบการเงิน รวมถึงหมายเหตุสรุปนโยบายการบัญชีที่สำคัญ

ข้าพเจ้าเห็นว่า รายงานการเงินข้างต้นนี้แสดงฐานะการเงินของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ณ วันที่ 30 กันยายน 2565 และผลการดำเนินงาน สำหรับปีสิ้นสุดวันเดียวกันโดยถูกต้องตามที่ควรในสาระสำคัญตามมาตรฐานการบัญชีภาครัฐและนโยบายการบัญชีภาครัฐที่กระทรวงการคลังกำหนด

เกณฑ์ในการแสดงความเห็น

ข้าพเจ้าได้ปฏิบัติงานตรวจสอบเป็นไปตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินและมาตรฐานการสอบบัญชี ความรับผิดชอบของข้าพเจ้าได้กล่าวไว้ในวรรคความรับผิดชอบของผู้สอบบัญชีต่อการตรวจสอบรายงานการเงินในรายงานของข้าพเจ้า ข้าพเจ้ามีความเป็นอิสระจากหน่วยงานตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินที่กำหนดโดยคณะกรรมการตรวจเงินแผ่นดินและประมวลจรรยาบรรณของผู้ประกอบวิชาชีพบัญชี รวมถึงมาตรฐานเรื่องความเป็นอิสระที่กำหนดโดยสภาวิชาชีพบัญชี (ประมวลจรรยาบรรณของผู้ประกอบวิชาชีพบัญชี) ในส่วนที่เกี่ยวข้องกับการตรวจสอบรายงานการเงิน และข้าพเจ้าได้ปฏิบัติตามความรับผิดชอบด้านจรรยาบรรณอื่นๆ ซึ่งเป็นไปตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินและประมวลจรรยาบรรณของผู้ประกอบวิชาชีพบัญชี ข้าพเจ้าเชื่อว่าหลักฐานการสอบบัญชีที่ข้าพเจ้าได้รับเพียงพอและเหมาะสมเพื่อใช้เป็นเกณฑ์ในการแสดงความเห็นของข้าพเจ้า

ข้อมูลอื่น

ผู้บริหารเป็นผู้รับผิดชอบต่อข้อมูลอื่น ข้อมูลอื่นประกอบด้วยข้อมูลซึ่งรวมอยู่ในรายงานประจำปีแต่ไม่รวมถึงรายงานการเงินและรายงานของผู้สอบบัญชีที่อยู่ในรายงานนั้น ซึ่งคาดว่ารายงานประจำปีจะถูกจัดเตรียมให้ข้าพเจ้าภายหลังวันที่ในรายงานของผู้สอบบัญชีนี้

ความเห็นของข้าพเจ้าต่อรายงานการเงินไม่ครอบคลุมถึงข้อมูลอื่นและข้าพเจ้าไม่ได้ให้ความเชื่อมั่นต่อข้อมูลอื่น

ความรับผิดชอบของข้าพเจ้าที่เกี่ยวเนื่องกับการตรวจสอบรายงานการเงินคือ การอ่านและพิจารณาว่าข้อมูลอื่นมีความขัดแย้งที่มีสาระสำคัญกับรายงานการเงินหรือกับความรู้ที่ได้รับจากการตรวจสอบของข้าพเจ้า หรือปรากฏว่า ข้อมูลอื่นมีการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญหรือไม่

*****/2

เมื่อข้าพเจ้าได้อ่านรายงานประจำปี หากข้าพเจ้าสรุปได้ว่าการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญ ข้าพเจ้าต้องสื่อสารเรื่องดังกล่าวกับผู้มีหน้าที่ในการกำกับดูแล เพื่อให้ผู้มีหน้าที่ในการกำกับดูแลดำเนินการแก้ไขข้อมูลที่แสดงขัดต่อข้อเท็จจริง

ความรับผิดชอบของผู้บริหารและผู้มีหน้าที่ในการกำกับดูแลต่อรายงานการเงิน

ผู้บริหารมีหน้าที่รับผิดชอบในการจัดทำและนำเสนอรายงานการเงินเหล่านี้โดยถูกต้องตามที่ควรตามมาตรฐานการบัญชีภาครัฐและนโยบายการบัญชีภาครัฐที่กระทรวงการคลังกำหนด และรับผิดชอบเกี่ยวกับการควบคุมภายในที่ผู้บริหารพิจารณาว่าจำเป็นเพื่อให้สามารถจัดทำรายงานการเงินที่ปราศจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญไม่ว่าจะเกิดจากการทุจริตหรือข้อผิดพลาด

ในการจัดทำรายงานการเงิน ผู้บริหารรับผิดชอบในการประเมินความสามารถของหน่วยงานในการดำเนินงานต่อเนื่อง เปิดเผยเรื่องที่เกี่ยวข้องกับการดำเนินงานต่อเนื่องตามความเหมาะสม และการใช้เกณฑ์การบัญชีสำหรับการดำเนินงานต่อเนื่อง เว้นแต่มีข้อกำหนดในกฎหมายหรือเป็นนโยบายรัฐบาลที่จะเลิกหน่วยงานหรือหยุดดำเนินงานหรือไม่สามารถดำเนินงานต่อเนื่องต่อไปได้

ผู้มีหน้าที่ในการกำกับดูแลมีหน้าที่ในการกำกับดูแลกระบวนการในการจัดทำรายงานทางการเงินของหน่วยงาน

ความรับผิดชอบของผู้สอบบัญชีต่อการตรวจสอบรายงานการเงิน

การตรวจสอบของข้าพเจ้ามีวัตถุประสงค์เพื่อให้ได้ความเชื่อมั่นอย่างสมเหตุสมผลว่ารายงานการเงินโดยรวมปราศจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญหรือไม่ ไม่ว่าจะเกิดจากการทุจริตหรือข้อผิดพลาด และเสนอรายงานของผู้สอบบัญชีซึ่งรวมความเห็นของข้าพเจ้าอยู่ด้วย ความเชื่อมั่นอย่างสมเหตุสมผลคือความเชื่อมั่นในระดับสูงแต่ไม่ได้เป็นการรับประกันว่าการปฏิบัติงานตรวจสอบตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินและมาตรฐานการสอบบัญชีจะสามารถตรวจพบข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญที่มีอยู่ได้เสมอไป ข้อมูลที่ขัดต่อข้อเท็จจริงอาจเกิดจากการทุจริตหรือข้อผิดพลาดและถือว่ามีสาระสำคัญเมื่อคาดการณ์ได้อย่างสมเหตุสมผลว่ารายการที่ขัดต่อข้อเท็จจริงแต่ละรายการหรือทุกรายการรวมกันจะมีผลต่อการตัดสินใจทางเศรษฐกิจของผู้ใช้รายงานการเงินจากการใช้รายงานการเงินเหล่านี้

ในการตรวจสอบของข้าพเจ้าตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินและมาตรฐานการสอบบัญชี ข้าพเจ้าได้ใช้ดุลยพินิจและการสังเกตและสงสัยเยี่ยงผู้ประกอบวิชาชีพตลอดการตรวจสอบ การปฏิบัติงานของข้าพเจ้ารวมถึง

- ระบุและประเมินความเสี่ยงจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญในรายงานการเงินไม่ว่าจะเกิดจากการทุจริตหรือข้อผิดพลาด ออกแบบและปฏิบัติงานตามวิธีการตรวจสอบเพื่อตอบสนองต่อความเสี่ยงเหล่านั้น และได้หลักฐานการสอบบัญชีที่เพียงพอและเหมาะสมเพื่อเป็นเกณฑ์ในการแสดงความเห็นของข้าพเจ้า ความเสี่ยงที่ไม่พบข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญซึ่งเป็นผลมาจากการทุจริตจะสูงกว่าความเสี่ยงที่เกิดจากข้อผิดพลาด เนื่องจากการทุจริตอาจเกี่ยวกับการสมรู้ร่วมคิด การปลอมแปลงเอกสารหลักฐาน การตั้งใจละเว้นการแสดงข้อมูล การแสดงข้อมูลที่ไม่ตรงตามข้อเท็จจริงหรือการแทรกแซงการควบคุมภายใน

*****/3

- ทำความเข้าใจในระบบการควบคุมภายในที่เกี่ยวข้องกับการตรวจสอบ เพื่อออกแบบวิธีการตรวจสอบที่เหมาะสมกับสถานการณ์ แต่ไม่ใช่เพื่อวัตถุประสงค์ในการแสดงความเห็นต่อความมีประสิทธิภาพของการควบคุมภายในของหน่วยงาน

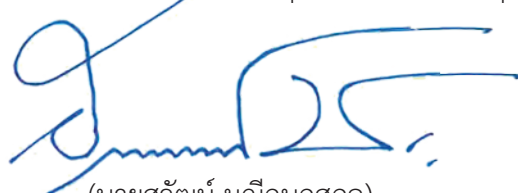
- ประเมินความเหมาะสมของนโยบายการบัญชีที่ผู้บริหารใช้และความสมเหตุสมผลของประมาณการทางบัญชีและการเปิดเผยข้อมูลที่เกี่ยวข้องซึ่งจัดทำขึ้นโดยผู้บริหาร

- สรุปลักษณะเกี่ยวกับความเหมาะสมของการใช้เกณฑ์การบัญชีสำหรับการดำเนินงานต่อเนื่องของผู้บริหารและจากหลักฐานการสอบบัญชีที่ได้รับ สรุปว่ามีความไม่แน่นอนที่มีสาระสำคัญเกี่ยวกับเหตุการณ์ หรือสถานการณ์ที่อาจเป็นเหตุให้เกิดข้อสงสัยอย่างมีนัยสำคัญต่อความสามารถของหน่วยงานในการดำเนินงานต่อเนื่องหรือไม่ ถ้าข้าพเจ้าได้ข้อสรุปว่ามีความไม่แน่นอนที่มีสาระสำคัญ ข้าพเจ้าต้องกล่าวไว้ในรายงานของผู้สอบบัญชีของข้าพเจ้าโดยให้ข้อสังเกตถึงการเปิดเผยข้อมูลในรายงานการเงินที่เกี่ยวข้อง หรือถ้าการเปิดเผยข้อมูลดังกล่าวไม่เพียงพอ ความเห็นของข้าพเจ้าจะเปลี่ยนแปลงไป ข้อสรุปของข้าพเจ้าขึ้นอยู่กับหลักฐานการสอบบัญชีที่ได้รับจนถึงวันที่ในรายงานของผู้สอบบัญชีของข้าพเจ้า อย่างไรก็ตามเหตุการณ์หรือสถานการณ์ในอนาคตอาจเป็นเหตุให้หน่วยงานต้องหยุดการดำเนินงานต่อเนื่อง

- ประเมินการนำเสนอโครงสร้างและเนื้อหาของรายงานการเงินโดยรวม รวมถึงการเปิดเผยข้อมูลว่ารายงานการเงินแสดงรายการและเหตุการณ์ในรูปแบบที่ทำให้มีการนำเสนอข้อมูลโดยถูกต้องตามที่ควรหรือไม่

ข้าพเจ้าได้สื่อสารกับผู้บริหารและผู้มีหน้าที่ในการกำกับดูแลในเรื่องต่างๆ ที่สำคัญ ซึ่งรวมถึงขอบเขตและช่วงเวลาของการตรวจสอบตามที่ได้วางแผนไว้ ประเด็นที่มีนัยสำคัญที่พบจากการตรวจสอบรวมถึงข้อบกพร่องที่มีนัยสำคัญในระบบการควบคุมภายในหากข้าพเจ้าได้พบในระหว่างการตรวจสอบของข้าพเจ้า

ผู้สอบบัญชีที่รับผิดชอบงานสอบบัญชีและนำเสนอรายงานฉบับนี้คือ นายสุวัฒน์ มณีกนกสกุล



(นายสุวัฒน์ มณีกนกสกุล)
ผู้สอบบัญชีรับอนุญาต ทะเบียนเลขที่ 8134

บริษัท สอบบัญชีธรรมนิติ จำกัด

กรุงเทพมหานคร

วันที่ 28 กุมภาพันธ์ 2566

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

งบแสดงฐานะการเงิน

ณ วันที่ 30 กันยายน 2565

National Cyber Security Agency

Financial Statement

As of 30 September 2022

4

		บาท Bath	
	หมายเหตุ Note	2565 2022	2564 2021
สินทรัพย์ Asset			
สินทรัพย์หมุนเวียน Current asset			
เงินสดและรายการเทียบเท่าเงินสด Cash and cash equivalents	5	96,675,385.01	28,354,116.76
ลูกหนี้ระยะสั้น Short-term receivable	6	43,791.78	114,871.08
วัสดุคงเหลือ Remaining material		727,995.17	185,584.80
รวมสินทรัพย์หมุนเวียน Total current asset		97,447,171.96	28,654,572.64
สินทรัพย์ไม่หมุนเวียน Non-current asset			
ที่ดิน อาคารและอุปกรณ์ Land, property, and equipment	7	16,461,228.65	1,371,436.30
สินทรัพย์ไม่มีตัวตน Intangible asset	8	5,076,595.93	-
รวมสินทรัพย์ไม่หมุนเวียน Total non-current asset		21,537,824.58	1,371,436.30
รวมสินทรัพย์ Net asset		118,984,996.54	30,026,008.94
หนี้สินและสินทรัพย์สุทธิ/ส่วนทุน Liabilities and Net Asset/Equity			
หนี้สินหมุนเวียน Current liabilities			
เจ้าหนี้ระยะสั้น Short-term creditor	9	1,783,074.75	189,545.66
เงินรับฝากระยะสั้น Short-term deposit	10	2,288,697.90	401,250.00
หนี้สินหมุนเวียนอื่น Other current liabilities	11	323,308.12	85,411.81
รวมหนี้สินหมุนเวียน Net current liabilities		4,395,080.77	676,207.47
รวมหนี้สิน Net liabilities		4,395,080.77	676,207.47
สินทรัพย์สุทธิ/ส่วนทุน Net Asset/Equity			
ทุน Capital		-	-
รายได้สูงกว่าค่าใช้จ่ายสะสม Revenue exceeding cumulative expense		114,589,915.77	29,349,801.47
รวมสินทรัพย์สุทธิ/ส่วนทุน Total net asset/equity		114,589,915.77	29,349,801.47
รวมหนี้สินและสินทรัพย์สุทธิ/ส่วนทุน Total liabilities and net asset/equity		118,984,996.54	30,026,008.94



(นางมัตติกา จงพิริยะอนันต์)
(Mrs. Muttika Jongpiriyaanan)

ผู้อำนวยการสำนักงานการเงินและกลยุทธ์องค์กร
Director of the Office of Finance and Corporate Strategy

พลอากาศตรี
Air vice-marshal



(อมร ชมเชย)
(Amorn Chomchoei)

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัย
ไซเบอร์แห่งชาติ
Secretary-General of the National Cyber Security Agency

หมายเหตุประกอบงบการเงินเป็นส่วนหนึ่งของรายงานการเงินนี้
The notes to the financial statements form an integral part of this financial report.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

5

งบแสดงผลการดำเนินงานทางการเงิน
สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2565

National Cyber Security Agency

Statement of Financial Performance

For the fiscal year ending 30 September 2022

		บาท Bath	
	หมายเหตุ Note	สำหรับปีสิ้นสุด วันที่ 30 กันยายน 2565 For the fiscal year ending 30 September 2022	สำหรับรอบระยะเวลาบัญชี ตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้ง) ถึงวันที่ 30 กันยายน 2564 For the accounting period from January 1, 2021 (the date of registration of the establishment) to 30 September 2021
รายได้ Revenue			
รายได้จากงบประมาณ Budget revenue	12	163,544,100.00	41,591,500.00
รายได้รับบริจาค Donation revenue		108,245.00	-
รวมรายได้ Total revenue		163,652,345.00	41,591,500.00
ค่าใช้จ่าย Expense			
ค่าใช้จ่ายบุคลากร Personnel expenses	13	40,007,560.83	2,375,000.00
ค่าตอบแทน Compensation	14	1,719,496.16	4,420,939.32
ค่าใช้จ่ายสอย Sundry expenses	15	29,022,682.53	4,484,891.91
ค่าวัสดุ Equipment expenses	16	2,873,801.15	487,896.94
ค่าสาธารณูปโภค Utility expenses	17	622,810.76	355,871.36
ค่าเสื่อมราคา Depreciation	18	4,165,879.27	117,099.00
รวมค่าใช้จ่าย Total expenses		78,412,230.70	12,241,698.53
รายได้สูงกว่าค่าใช้จ่ายสุทธิ Revenue exceeding total expense		85,240,114.30	29,349,801.47



(นางมัตติกา จงพิริยะอนันต์)
(Mrs. Muttika Jongpiriyaanan)

ผู้อำนวยการสำนักงานการเงินและกลยุทธ์องค์กร

Director of the Office of Finance and Corporate Strategy

พลอากาศตรี
Air vice-marshal



(อมร ชมเชย)
(Amorn Chomchoei)

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัย
ไซเบอร์แห่งชาติ

Secretary-General of the National Cyber Security Agency

หมายเหตุประกอบงบการเงินเป็นส่วนหนึ่งของรายงานการเงินนี้

The notes to the financial statements form an integral part of this financial report.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
 งบแสดงการเปลี่ยนแปลงสินทรัพย์สุทธิ/ส่วนทุน
 สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2565
 National Cyber Security Agency
 Statement of changes in net assets/equity
 For the fiscal year ending 30 September 2022

6

		บาท Bath		
	หมายเหตุ Note	ทุน Capital	รายได้สูงกว่า ค่าใช้จ่ายสะสม Revenue exceeding cumulative expense	รวมสินทรัพย์สุทธิ ส่วนทุน Total net asset / equity
ยอดคงเหลือ ณ วันที่ 1 มกราคม 2564 Balance as of 1 January 2021				
		-	-	-
รายได้สูงกว่าค่าใช้จ่ายสำหรับงวด Revenue exceeding annual expense				
		-	29,349,801.47	29,349,801.47
ยอดคงเหลือ ณ วันที่ 30 กันยายน 2564 Balance as of 30 September 2021				
		-	29,349,801.47	29,349,801.47
รายได้สูงกว่าค่าใช้จ่ายสำหรับงวด Revenue exceeding annual expense				
		-	85,240,114.30	85,240,114.30
ยอดคงเหลือ ณ วันที่ 30 กันยายน 2565 Balance as of 30 September 2022				
		-	114,589,915.77	114,589,915.77



(นางมัตติกา จงพิริยะอนันต์)

(Mrs. Muttika Jongpiriyaanan)

ผู้อำนวยการสำนักการเงินและกลยุทธ์องค์กร

Director of the Office of Finance and Corporate Strategy

พลอากาศตรี

Air vice-marshal



(อมร ชมเชย)

(Amorn Chomchoei)

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัย
ไซเบอร์แห่งชาติ

Secretary-General of the National Cyber Security Agency

หมายเหตุประกอบงบการเงินเป็นส่วนหนึ่งของรายงานการเงินนี้

The notes to the financial statements form an integral part of this financial report.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

รายงานฐานะเงินงบประมาณรายจ่ายประจำปี

สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2565

National Cyber Security Agency

Budget Expenditure Report

For the fiscal year ending 30 September 2022

(หน่วย: บาท)

(Unit: Baht)

รายงานฐานะเงินงบประมาณรายจ่ายปี 2565 Budget Expenditure Report of 2022

รายการ List	งบสุทธิ Net Statement	ใบสั่งซื้อ/สัญญา Purchase Order/Contract	เบิกจ่าย Disbursemen	คงเหลือ Remaining
แผนงบประมาณ Budget plan				
งบอุดหนุน Subsidy budget				
ค่าใช้จ่ายบุคลากร Personnel expenses	20,820,000.00	-	20,820,000.00	-
ค่าใช้จ่ายดำเนินงาน Operating expenses	18,447,457.70	1,322,765.00	17,124,692.70	-
ค่าครุภัณฑ์และสิ่งก่อสร้าง Expenses of durable goods and construction	50,587,212.00	42,988,142.80	7,599,068.20	1.00
ค่าใช้จ่ายดำเนินงานตามแผนโครงการ Project operating expenses	54,495,230.30	49,792,146.40	4,703,083.90	-
งบกลาง Central budget				
ค่าใช้จ่ายบุคลากร Personnel expenses	19,194,200.00	-	19,192,620.83	1,579.17
รวม Total	163,544,100.00	94,103,054.20	69,439,465.63	1,580.17

รายงานฐานะเงินงบประมาณรายจ่ายปี 2564 Budget Expenditure Report of 2021

(หน่วย: บาท)

(Unit: Baht)

รายการ List	งบสุทธิ Net Statement	ใบสั่งซื้อ/สัญญา Purchase Order/Contract	เบิกจ่าย Disbursemen	คงเหลือ Remaining
แผนงบประมาณ Budget plan				
งบอุดหนุน Subsidy budget				
ค่าใช้จ่ายบุคลากร Personnel expenses	2,375,000.00	-	2,375,000.00	-
ค่าใช้จ่ายดำเนินงาน Operating expenses	10,412,014.42	550,191.63	9,860,926.75	896.04
ค่าครุภัณฑ์และสิ่งก่อสร้าง Expenses of durable goods and construction	19,863,243.58	18,374,708.28	1,488,535.30	-
ค่าใช้จ่ายดำเนินงานตามแผนโครงการ Project operating expenses	8,941,242.00	8,941,242.00	-	-
รวม Total	41,591,500.00	27,866,141.91	13,724,462.05	896.04

หมายเหตุประกอบงบการเงินเป็นส่วนหนึ่งของรายงานการเงินนี้

The notes to the financial statements form an integral part of this financial report.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หมายเหตุประกอบงบการเงิน สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2565

หมายเหตุที่ 1 ข้อมูลทั่วไป

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีผลใช้บังคับเมื่อวันที่ 28 พฤษภาคม 2562 แต่ทางหน่วยงานได้มีการเริ่มดำเนินงานในวันที่ 1 มกราคม 2564 เมื่อทางหน่วยงานได้มีการดำเนินการครบตามองค์ประกอบในการจัดตั้งหน่วยงาน โดยมีวัตถุประสงค์เพื่อกำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับองค์กรภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ รวมทั้งให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นองค์กรรับผิดชอบงานตามพระราชบัญญัติ และประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์ที่เป็นภัยต่อความมั่นคงอย่างร้ายแรง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

สถานที่ตั้งหลักสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) 120 หมู่ 3 อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210 สกมช. “เป็นผู้นำในการขับเคลื่อนในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศที่มีประสิทธิภาพพร้อมตอบสนองต่อภัยคุกคามไซเบอร์ทุกมิติ” ทำหน้าที่กำหนดนโยบาย ระเบียบ มาตรการ มาตรฐานขั้นต่ำ แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับองค์กรภาครัฐและภาคเอกชนที่เป็นองค์กรโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการเฝ้าระวัง ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบและสร้างความเดือดร้อนต่อประชาชน ตลอดจนความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ โดยประสานงาน เฝ้าระวัง รับมือและแก้ไขภัยคุกคามทางไซเบอร์ เมื่อมีเหตุภัยคุกคามเกิดขึ้นอย่างมีนัยสำคัญให้องค์กรโครงสร้างพื้นฐานสำคัญทางสารสนเทศดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคาม และรายงานต่อองค์กรและองค์กรควบคุมหรือกำกับดูแลโดยเร็ว และสำหรับองค์กรที่เกี่ยวข้องหากพบการโจมตีทางไซเบอร์

หมายเหตุที่ 2 เกณฑ์การจัดทำรายการทางการเงิน

รายการทางการเงินฉบับนี้ จัดทำขึ้นตามพระราชบัญญัติวินัยการเงินการคลัง พ.ศ. 2561 รายการที่ปรากฏในรายการทางการเงินฉบับนี้เป็นไปตามมาตรฐานการบัญชีภาครัฐ และนโยบายการบัญชีภาครัฐที่กระทรวงการคลังประกาศใช้ และการจัดทำรายการทางการเงินถือปฏิบัติตามหลักเกณฑ์และวิธีการจัดทำรายการทางการเงินประจำปีตามหนังสือกระทรวงการคลัง ที่ กค 0410.2/ว 15 ลงวันที่ 4 กุมภาพันธ์ 2563 และแสดงรูปแบบการนำเสนอรายการทางการเงินของหน่วยงานภาครัฐ ตามหนังสือกรมบัญชีกลาง ที่ กค 0410.2/ว 479 ลงวันที่ 2 ตุลาคม 2563

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หมายเหตุประกอบงบการเงิน (ต่อ)

สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2565

หมายเหตุที่ 3 มาตรฐานการบัญชีภาครัฐและนโยบายการบัญชีภาครัฐฉบับใหม่ และมาตรฐานการบัญชีภาครัฐและนโยบายการบัญชีภาครัฐที่ปรับปรุงใหม่

มาตรฐานการบัญชีภาครัฐและนโยบายการบัญชีภาครัฐ ที่มีผลบังคับใช้สำหรับรอบระยะเวลาบัญชีที่เริ่มในหรือหลังวันที่ 1 ตุลาคม 2564 ดังนี้

- นโยบายการบัญชีภาครัฐ เรื่อง บัตรภาษี

นโยบายการบัญชีภาครัฐฉบับใหม่ ข้างต้นไม่มีผลกระทบอย่างเป็นสาระสำคัญต่อรายงานการเงินในงวดปัจจุบัน

หมายเหตุที่ 4 สรุปนโยบายการบัญชีที่สำคัญ

4.1 เงินสดและรายการเทียบเท่าเงินสด

เงินสด หมายถึง เงินสดในมือ เช็ค ดราฟต์และธนาคาติ หน่วยงานจะรับรู้เงินสดและเงินฝากธนาคารในราคาตามมูลค่าที่ตราไว้ และแสดงรายการดังกล่าวไว้ในเงินสดและรายการเทียบเท่าเงินสดในงบแสดงฐานะการเงิน

รายการเทียบเท่าเงินสด หมายถึง เงินลงทุนระยะสั้นที่มีสภาพคล่องสูงซึ่งพร้อมที่จะเปลี่ยนเป็นเงินสดในจำนวนเงินที่เท่ากันหรือใกล้เคียงกับมูลค่าเดิม ซึ่งความแตกต่างในมูลค่าดังกล่าวไม่มีนัยสำคัญ

4.2 ลูกหนี้ระยะสั้น

ลูกหนี้จากการให้บริการ หมายถึง จำนวนเงินที่หน่วยงานมีสิทธิได้รับชำระจากบุคคลภายนอกหรือหน่วยงานอื่น ซึ่งเกิดจากการให้บริการอันเป็นส่วนหนึ่งของการดำเนินงานปกติของหน่วยงาน หน่วยงานจะรับรู้ลูกหนี้จากการให้บริการตามมูลค่าสุทธิที่จะได้รับโดยมีการประมาณการค่าเผื่อหนี้สงสัยจะสูญสำหรับลูกหนี้ส่วนที่คาดว่าจะไม่สามารถเรียกเก็บเงินได้

ค่าเผื่อหนี้สงสัยจะสูญ ประมาณขึ้นจากการพิจารณาประสบการณ์ที่ผ่านมาเกี่ยวกับจำนวนลูกหนี้ที่เก็บเงินไม่ได้ และสถานะทางการเงินของลูกหนี้ในปัจจุบัน โดยคำนวณตามอัตราร้อยละของยอดลูกหนี้คงค้าง ณ วันสิ้นงวดแยกตามกลุ่มของอายุลูกหนี้ที่ค้างชำระ/ ของยอดลูกหนี้คงค้างทั้งหมด

ลูกหนี้เงินยืม หมายถึง ลูกหนี้ภายในหน่วยงานกรณีให้ข้าราชการ พนักงาน หรือเจ้าหน้าที่ยืมเงินไปใช้จ่ายในการปฏิบัติงานโดยไม่มีดอกเบี้ย เช่น ลูกหนี้เงินงบประมาณ ลูกหนี้เงินนอกงบประมาณแสดงตามมูลค่าที่จะได้รับโดยไม่ตั้งบัญชีค่าเผื่อหนี้สงสัยจะสูญ

4.3 วัสดุคงเหลือ

วัสดุคงเหลือ หมายถึง สินทรัพย์ที่หน่วยงานมีไว้เพื่อใช้ในการดำเนินงานตามปกติ โดยทั่วไปมีมูลค่าไม่สูง และไม่มีลักษณะคงทนถาวร หน่วยงานวัดมูลค่าวัสดุคงเหลือในราคาทุนตามวิธีเข้าก่อนออกก่อน

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
หมายเหตุประกอบงบการเงิน (ต่อ)
สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2565

4.4 อาคาร และอุปกรณ์

หน่วยงานแสดงรายการอาคารและอุปกรณ์ตามราคาทุนหักค่าเสื่อมราคาสะสม และค่าเผื่อการด้อยค่า (ถ้ามี)

หน่วยงานรับรู้รายการอุปกรณ์ เฉพาะรายการที่มีมูลค่าขั้นต่ำต่อหน่วยหรือต่อชุดตั้งแต่ 10,000 บาท ขึ้นไป

ราคาทุนรวมต้นทุนทางตรงที่เกี่ยวข้องกับการจัดหาสินทรัพย์ เพื่อให้สินทรัพย์นั้นอยู่ในสภาพและสถานที่ที่พร้อมจะใช้งานได้ตามความประสงค์ของฝ่ายบริหาร ราคาทุนของสินทรัพย์ที่ก่อสร้างขึ้นเองประกอบด้วยต้นทุนค่าวัสดุ ค่าแรงงานทางตรง และต้นทุนทางตรงอื่น ๆ ที่เกี่ยวข้องกับการจัดหาสินทรัพย์

ส่วนประกอบของรายการที่ดิน อาคาร และอุปกรณ์แต่ละรายการที่มีรูปแบบและอายุการให้ประโยชน์ที่แตกต่างกัน และมีต้นทุนที่มีนัยสำคัญจะบันทึกส่วนประกอบนั้นแยกต่างหากจากกัน

ต้นทุนที่เกิดขึ้นในภายหลัง ต้นทุนในการเปลี่ยนแทนส่วนประกอบจะรับรู้เป็นส่วนหนึ่งของมูลค่าตามบัญชีของรายการที่ดิน อาคาร และอุปกรณ์ เมื่อมีความเป็นไปได้ค่อนข้างแน่ที่จะได้รับประโยชน์เชิงเศรษฐกิจในอนาคตหรือศักยภาพในการให้บริการเพิ่มขึ้นจากรายการนั้น และสามารถวัดมูลค่าต้นทุนของรายการนั้นได้อย่างน่าเชื่อถือ และตัดมูลค่าของชิ้นส่วนที่ถูกเปลี่ยนแทนออกมาจากบัญชีด้วยมูลค่าตามบัญชี ส่วนต้นทุนที่เกิดขึ้นในการซ่อมบำรุงที่ดิน อาคาร และอุปกรณ์ที่เกิดขึ้นเป็นประจำจะรับรู้เป็นค่าใช้จ่ายเมื่อเกิดขึ้น

ค่าเสื่อมราคابันทักเป็นค่าใช้จ่ายในงบแสดงผลการดำเนินงานทางการเงิน คำนวณโดยวิธีเส้นตรงตามอายุการให้ประโยชน์โดยประมาณ ตามหนังสือกรมบัญชีกลาง ที่ กค 0410.3/ว 43 ลงวันที่ 29 มกราคม 2562 เรื่อง คู่มือการบัญชีภาครัฐ เรื่อง ที่ดิน อาคาร และอุปกรณ์ ดังนี้

อายุการให้ประโยชน์โดยประมาณของสินทรัพย์มีดังนี้

ครุภัณฑ์สำนักงาน	3 ปี
ครุภัณฑ์ไฟฟ้าและวิทยุ	5 ปี
ยกเว้น เครื่องกำเนิดไฟฟ้า	15 ปี
ครุภัณฑ์โฆษณาและเผยแพร่	5 ปี
ครุภัณฑ์โรงงาน	2 ปี
ครุภัณฑ์ก่อสร้าง	2 ปี
ครุภัณฑ์การแพทย์และวิทยาศาสตร์	5 ปี
ครุภัณฑ์คอมพิวเตอร์	3 ปี
ครุภัณฑ์งานบ้านงานครัว	2 ปี

ไม่มีการคิดค่าเสื่อมราคาสำหรับสินทรัพย์ระหว่างก่อสร้าง

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
หมายเหตุประกอบงบการเงิน (ต่อ)
สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2565

4.5 สินทรัพย์ไม่มีตัวตน

สินทรัพย์ไม่มีตัวตน ได้แก่ ต้นทุนที่เกี่ยวข้องโดยตรงในการพัฒนาโปรแกรมคอมพิวเตอร์ รวมถึงระบบต่าง ๆ และต้นทุนเว็บไซต์ ทั้งที่ได้มาจากการจัดซื้อ และการพัฒนาขึ้น โดยหน่วยงานมีสิทธิ์ควบคุมการใช้ประโยชน์จากทรัพย์สินนั้น และคาดว่าจะได้รับประโยชน์เชิงเศรษฐกิจเหนือศักยภาพในการให้บริการจากทรัพย์สินนั้นเกินกว่าหนึ่งปี หน่วยงานแสดงรายการสินทรัพย์ไม่มีตัวตนตามราคาทุนหักค่าตัดราคาจำหน่ายสะสม

สินทรัพย์ไม่มีตัวตนแสดงในราคาทุนหักด้วยค่าตัดจำหน่ายสะสมและขาดทุนจากการลดมูลค่า (ถ้ามี) สินทรัพย์ไม่มีตัวตนถูกตัดจำหน่ายและบันทึกในงบแสดงผลการดำเนินงานทางการเงินโดยวิธีเส้นตรงตามระยะเวลาที่คาดว่าจะได้รับประโยชน์เชิงเศรษฐกิจนับจากวันที่อยู่ในสภาพพร้อมใช้งานระยะเวลาที่คาดว่าจะได้รับประโยชน์เชิงเศรษฐกิจแสดงได้ดังนี้

โปรแกรมคอมพิวเตอร์

2 ปี

4.6 การรับรู้รายได้

รายได้จากเงินงบประมาณรับรู้ตามเกณฑ์ดังนี้

- (1) กรณีที่เบิกจ่ายเงินเข้าบัญชีของหน่วยงานเพื่อนำไปจ่ายต่อให้แก่ผู้มีสิทธิรับเงินของหน่วยงานรับรู้รายได้จากเงินงบประมาณเมื่อรับโอนเงินเข้าบัญชีจากการขอเบิกเงินจากคลังในระบบ GFMIS
- (2) กรณีที่เบิกหักส่งหรือเบิกจ่ายตรงจากรัฐบาลให้แก่ผู้มีสิทธิรับเงินของหน่วยงานโดยหน่วยงานไม่ได้รับตัวเงิน รับรู้รายได้จากเงินงบประมาณเมื่อได้รับอนุมัติคำขอเบิกเงินจากคลัง
- (3) รายได้อื่นรับรู้ตามเกณฑ์คงค้าง

4.7 การรับรู้ค่าใช้จ่าย

- (1) ค่าใช้จ่ายจากเงินงบประมาณรับรู้ตามเกณฑ์คงค้าง
- (2) ค่าใช้จ่ายอื่นรับรู้ตามเกณฑ์คงค้าง

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หมายเหตุประกอบงบการเงิน (ต่อ)

สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2565

หมายเหตุที่ 5 เงินสดและรายการเทียบเท่าเงินสด

	บาท	
	2565	2564
เงินฝากธนาคาร - ในงบประมาณ	94,426,641.31	27,952,866.76
เงินฝากธนาคาร - นอกงบประมาณ	2,248,743.70	401,250.00
รวมเงินสดและรายการเทียบเท่าเงินสด	96,675,385.01	28,354,116.76

เงินฝากธนาคาร ณ วันที่ 30 กันยายน 2565 และ 2564 จำนวน 96,675,385.01 บาท และจำนวน 28,354,116.76 ซึ่งฝากไว้ที่ธนาคารกรุงไทย ประเภทกระแสรายวัน ประกอบด้วย

	บาท	
	2565	2564
1. เลขบัญชี 955-6-00528-5 ชื่อบัญชีสำนักงานคณะกรรมการ		
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (เงินงบประมาณ)	94,426,641.31	27,952,866.76
2. เลขบัญชี 955-6-00529-3 ชื่อบัญชีสำนักงานคณะกรรมการ		
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (เงินนอกงบประมาณ)	2,248,743.70	401,250.00
รวม	96,675,385.01	28,354,116.76

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หมายเหตุประกอบงบการเงิน (ต่อ)

สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2565

หมายเหตุที่ 6 ลูกหนี้ระยะสั้น

	บาท	
	2565	2564
ลูกหนี้เงินยืม	-	65,600.00
ค่าใช้จ่ายจ่ายล่วงหน้า	43,791.78	49,271.08
รวมลูกหนี้ระยะสั้น	43,791.78	114,871.08

ลูกหนี้เงินยืม ณ วันสิ้นปี แยกตามอายุหนี้ ดังนี้

ลูกหนี้เงินยืม	บาท				รวม
	ยังไม่ถึงกำหนดชำระ	เกินกำหนดชำระไม่เกิน 30 วัน	เกินกำหนดชำระเกินกว่า 30 วัน		
2564	65,600.00	-	-		65,600.00

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
หมายเหตุประกอบงบการเงิน (ต่อ)
สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2565

หมายเหตุที่ 7 อาคาร และอุปกรณ์

	บาท				
	ยอดคงเหลือ ณ วันที่ 30 ก.ย. 64	จำนวนที่เพิ่มขึ้น	จำนวนที่ลดลง	รับโอน (โอนออก)	ยอดคงเหลือ ณ วันที่ 30 ก.ย. 65
ราคาทุน					
ครุภัณฑ์สำนักงาน	513,013.20	6,172,024.44	-	-	6,685,037.64
ครุภัณฑ์โฆษณาและเผยแพร่	109,936.50	3,092,085.16	-	-	3,202,021.66
ครุภัณฑ์คอมพิวเตอร์	737,230.00	4,301,961.76	-	-	5,039,191.76
ครุภัณฑ์งานบ้านงานครัว	128,355.60	77,920.00	-	-	206,275.60
ครุภัณฑ์ไฟฟ้าและวิทยุ	-	85,129.64	-	-	85,129.64
ครุภัณฑ์โรงงาน	-	36,599.92	-	-	36,599.92
ครุภัณฑ์ทางการแพทย์และวิทยาศาสตร์	-	79,500.00	-	-	79,500.00
ครุภัณฑ์ก่อสร้าง	-	7,000.00	-	-	7,000.00
งานระหว่างก่อสร้าง	-	4,145,887.85	-	-	4,145,887.85
รวม	1,488,535.30	17,998,108.77	-	-	19,486,644.07
หัก ค่าเสื่อมราคาสะสม					
ครุภัณฑ์สำนักงาน	(11,313.64)	(1,567,341.49)	-	-	(1,578,655.13)
ครุภัณฑ์โฆษณาและเผยแพร่	(1,461.38)	(352,427.65)	-	-	(353,889.03)
ครุภัณฑ์คอมพิวเตอร์	(103,679.94)	(888,911.62)	-	-	(992,591.56)
ครุภัณฑ์งานบ้านงานครัว	(644.04)	(86,500.74)	-	-	(87,144.78)
ครุภัณฑ์ไฟฟ้าและวิทยุ	-	(7,823.40)	-	-	(7,823.40)
ครุภัณฑ์โรงงาน	-	(1,469.42)	-	-	(1,469.42)
ครุภัณฑ์ทางการแพทย์และวิทยาศาสตร์	-	(3,267.00)	-	-	(3,267.00)
ครุภัณฑ์ก่อสร้าง	-	(575.10)	-	-	(575.10)
งานระหว่างก่อสร้าง	-	-	-	-	-
รวม	(117,099.00)	(2,908,316.42)	-	-	(3,025,415.42)
อาคารและอุปกรณ์ - สุทธิ	1,371,436.30				16,461,228.65

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
หมายเหตุประกอบงบการเงิน (ต่อ)
สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2565

	บาท				
	ยอดคงเหลือ ณ วันที่ 30 ก.ย. 63	จำนวนที่เพิ่มขึ้น	จำนวนที่ลดลง	รับโอน (โอนออก)	ยอดคงเหลือ ณ วันที่ 30 ก.ย. 64
ราคาทุน					
ครุภัณฑ์สำนักงาน	-	513,013.20	-	-	513,013.20
ครุภัณฑ์โฆษณาและเผยแพร่	-	109,936.50	-	-	109,936.50
ครุภัณฑ์คอมพิวเตอร์	-	737,230.00	-	-	737,230.00
ครุภัณฑ์งานบ้านงานครัว	-	128,355.60	-	-	128,355.60
ครุภัณฑ์ไฟฟ้าและวิทยุ	-	-	-	-	-
ครุภัณฑ์โรงงาน	-	-	-	-	-
ครุภัณฑ์ทางการแพทย์และวิทยาศาสตร์	-	-	-	-	-
ครุภัณฑ์ก่อสร้าง	-	-	-	-	-
งานระหว่างก่อสร้าง	-	-	-	-	-
รวม	-	1,488,535.30	-	-	1,488,535.30
หัก ค่าเสื่อมราคาสะสม					
ครุภัณฑ์สำนักงาน	-	(11,313.64)	-	-	(11,313.64)
ครุภัณฑ์โฆษณาและเผยแพร่	-	(1,461.38)	-	-	(1,461.38)
ครุภัณฑ์คอมพิวเตอร์	-	(103,679.94)	-	-	(103,679.94)
ครุภัณฑ์งานบ้านงานครัว	-	(644.04)	-	-	(644.04)
ครุภัณฑ์ไฟฟ้าและวิทยุ	-	-	-	-	-
ครุภัณฑ์โรงงาน	-	-	-	-	-
ครุภัณฑ์ทางการแพทย์และวิทยาศาสตร์	-	-	-	-	-
ครุภัณฑ์ก่อสร้าง	-	-	-	-	-
งานระหว่างก่อสร้าง	-	-	-	-	-
รวม	-	(117,099.00)	-	-	(117,099.00)
อาคารและอุปกรณ์ - สุทธิ	-				1,371,436.30

ค่าเสื่อมราคาสำหรับปี 2565 และ 2564 จำนวน 2,908,316.42 บาท และ 117,099.00 บาท
ตามลำดับ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
 หมายเหตุประกอบงบการเงิน (ต่อ)
 สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2565

หมายเหตุที่ 8 สินทรัพย์ไม่มีตัวตน

	บาท			
	ยอดตามบัญชี ณ 30 ก.ย. 64	จำนวนที่ เพิ่มขึ้น	จำนวนที่ ลดลง	ยอดตามบัญชี ณ 30 ก.ย. 65
ราคาทุน				
สินทรัพย์ไม่มีตัวตน	-	6,334,158.78	-	6,334,158.78
รวม	-	6,334,158.78	-	6,334,158.78
หัก ค่าตัดจำหน่ายสะสม	-		-	-
สินทรัพย์ไม่มีตัวตน	-	(1,257,562.85)	-	(1,257,562.85)
รวม	-	(1,257,562.85)	-	(1,257,562.85)
	-			5,076,595.93

หมายเหตุที่ 9 เจ้าหนี้ระยะสั้น

	บาท	
	2565	2564
ค่าใช้จ่ายค้างจ่าย	1,783,074.75	189,128.66
รายได้ค่าปรับอื่น รอนำส่ง	-	417.00
รวมเจ้าหนี้ระยะสั้น	1,783,074.75	189,545.66

หมายเหตุที่ 10 เงินรับฝากระยะสั้น

	บาท	
	2565	2564
เงินประกันอื่น	2,288,697.90	401,250.00
รวมเงินรับฝากระยะสั้น	2,288,697.90	401,250.00

หมายเหตุที่ 11 หนี้สินหมุนเวียนอื่น

	บาท	
	2565	2564
เจ้าหนี้กรมสรรพากร	323,308.12	85,411.81
รวมหนี้สินหมุนเวียนอื่น	323,308.12	85,411.81

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
หมายเหตุประกอบงบการเงิน (ต่อ)
สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2565

หมายเหตุที่ 12 รายได้จากงบประมาณ

	บาท	
	สำหรับรอบระยะเวลาบัญชีตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้ง) ถึงวันที่ 30 กันยายน 2564	สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2565
รายได้จากงบอุดหนุน	-	144,349,900.00
รายได้จากงบกลาง	41,591,500.00	19,194,200.00
รวมรายได้จากงบประมาณ	41,591,500.00	163,544,100.00

หมายเหตุที่ 13 ค่าใช้จ่ายบุคลากร

	บาท	
	สำหรับรอบระยะเวลาบัญชีตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้ง) ถึงวันที่ 30 กันยายน 2564	สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2565
เงินเดือนและค่าจ้าง	2,375,000.00	37,496,229.06
ค่าเบี้ยประกันสุขภาพ	-	461,644.02
เงินสมทบกองทุนสำรองเลี้ยงชีพพนักงาน	-	1,135,726.00
ค่าใช้จ่ายบุคลากรอื่น	-	913,961.75
รวมค่าใช้จ่ายบุคลากร	2,375,000.00	40,007,560.83

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
หมายเหตุประกอบงบการเงิน (ต่อ)
สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2565

หมายเหตุที่ 14 ค่าตอบแทน

	บาท	
	สำหรับรอบ ระยะ เวลาบัญชี ตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียน จัดตั้ง) ถึงวันที่ 30 กันยายน 2564	สำหรับปีสิ้นสุด วันที่ 30 กันยายน 2565
ค่าตอบแทนการปฏิบัติ	4,420,939.32	1,116,451.00
ค่าตอบแทนอื่น	-	603,045.16
รวมค่าตอบแทน	4,420,939.32	1,719,496.16

หมายเหตุที่ 15 ค่าใช้สอย

	บาท	
	สำหรับรอบระยะ เวลาบัญชีตั้งแต่ วันที่ 1 มกราคม 2564 (วันจด ทะเบียนจัดตั้ง) ถึงวันที่ 30 กันยายน 2564	สำหรับปีสิ้นสุด วันที่ 30 กันยายน 2565
ค่าใช้จ่ายด้านการฝึกอบรม-ในประเทศ	206,800.00	255,374.00
ค่าใช้จ่ายเดินทางภายในปท.	9,309.00	-
ค่าจ้างเหมาบริการ-บุคคลภายนอก	1,341,791.90	11,531,334.41
ค่าจ้างเหมาบริการ-บุคคลภาครัฐ	-	1,136,200.00
ค่าธรรมเนียม	4,000.00	4,000.00
ค่าจ้างที่ปรึกษา	-	11,277,251.00
ค่าใช้จ่ายในการจัดประชุม	1,337,936.00	2,394,111.00
ค่าเช่าเบ็ดเตล็ด	17,120.00	751,321.03

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
 หมายเหตุประกอบงบการเงิน (ต่อ)
 สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2565

หมายเหตุที่ 15 ค่าใช้สอย (ต่อ)

	บาท	
	สำหรับรอบ ระยะ เวลาบัญชี ตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียน จัดตั้ง) สำหรับปีสิ้นสุด วันที่ 30 กันยายน 2565	ถึงวันที่ 30 กันยายน 2564
ค่าประชาสัมพันธ์	-	480,000.00
ค่าใช้จ่ายผลิตส่ง	896.04	-
ค่าใช้สอยอื่นๆ	1,558,195.05	1,011,935.01
ค่าสอบบัญชี	114,000.00	76,000.00
รวมค่าใช้สอย	<u>29,022,682.53</u>	<u>4,484,891.91</u>

หมายเหตุที่ 16 ค่าวัสดุ

	บาท	
	สำหรับรอบระยะ เวลาบัญชีตั้งแต่ วันที่ 1 มกราคม 2564 (วันจด ทะเบียนจัดตั้ง) สำหรับปีสิ้นสุด วันที่ 30 กันยายน 2565	ถึงวันที่ 30 กันยายน 2564
ค่าวัสดุ	2,873,801.15	487,896.94
รวมค่าวัสดุ	<u>2,873,801.15</u>	<u>487,896.94</u>

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
 หมายเหตุประกอบงบการเงิน (ต่อ)
 สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2565

หมายเหตุที่ 17 ค่าสาธารณูปโภค

	บาท	
	สำหรับรอบระยะเวลาบัญชีตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้ง) ถึงวันที่ 30 กันยายน 2565	สำหรับรอบระยะเวลาบัญชีตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้ง) ถึงวันที่ 30 กันยายน 2564
ค่าไฟฟ้า	522,742.08	291,953.16
ค่าโทรศัพท์	5,033.28	3,076.36
ค่าบริการสื่อสารและโทรคมนาคม	48,492.40	23,617.84
ค่าบริการไปรษณีย์	46,543.00	37,224.00
รวมค่าสาธารณูปโภค	622,810.76	355,871.36

หมายเหตุที่ 18 ค่าเสื่อมราคา

	บาท	
	สำหรับรอบระยะเวลาบัญชีตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้ง) ถึงวันที่ 30 กันยายน 2565	สำหรับรอบระยะเวลาบัญชีตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้ง) ถึงวันที่ 30 กันยายน 2564
ครุภัณฑ์	2,908,316.42	117,099.00
สินทรัพย์ไม่มีตัวตน	1,257,562.85	-
รวมค่าเสื่อมราคา	4,165,879.27	117,099.00

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
 หมายเหตุประกอบงบการเงิน (ต่อ)
 สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2565

หมายเหตุที่ 19 ภาระผูกพัน

- 19.1 หน่วยงานมีภาระผูกพันตามสัญญาจ้างเหมาบริการ คงเหลือเป็นจำนวนเงิน 49,792,146.40 บาท
 19.2 หน่วยงานมีภาระผูกพันตามสัญญาจ้างก่อสร้าง ปรับปรุง และจัดหาสินทรัพย์ คงเหลือเป็นจำนวนเงิน 42,988,142.80 บาท
 19.3 หน่วยงานมีภาระผูกพันตามสัญญาจ้างบริการ คงเหลือเป็นจำนวนเงิน 1,322,765.00 บาท

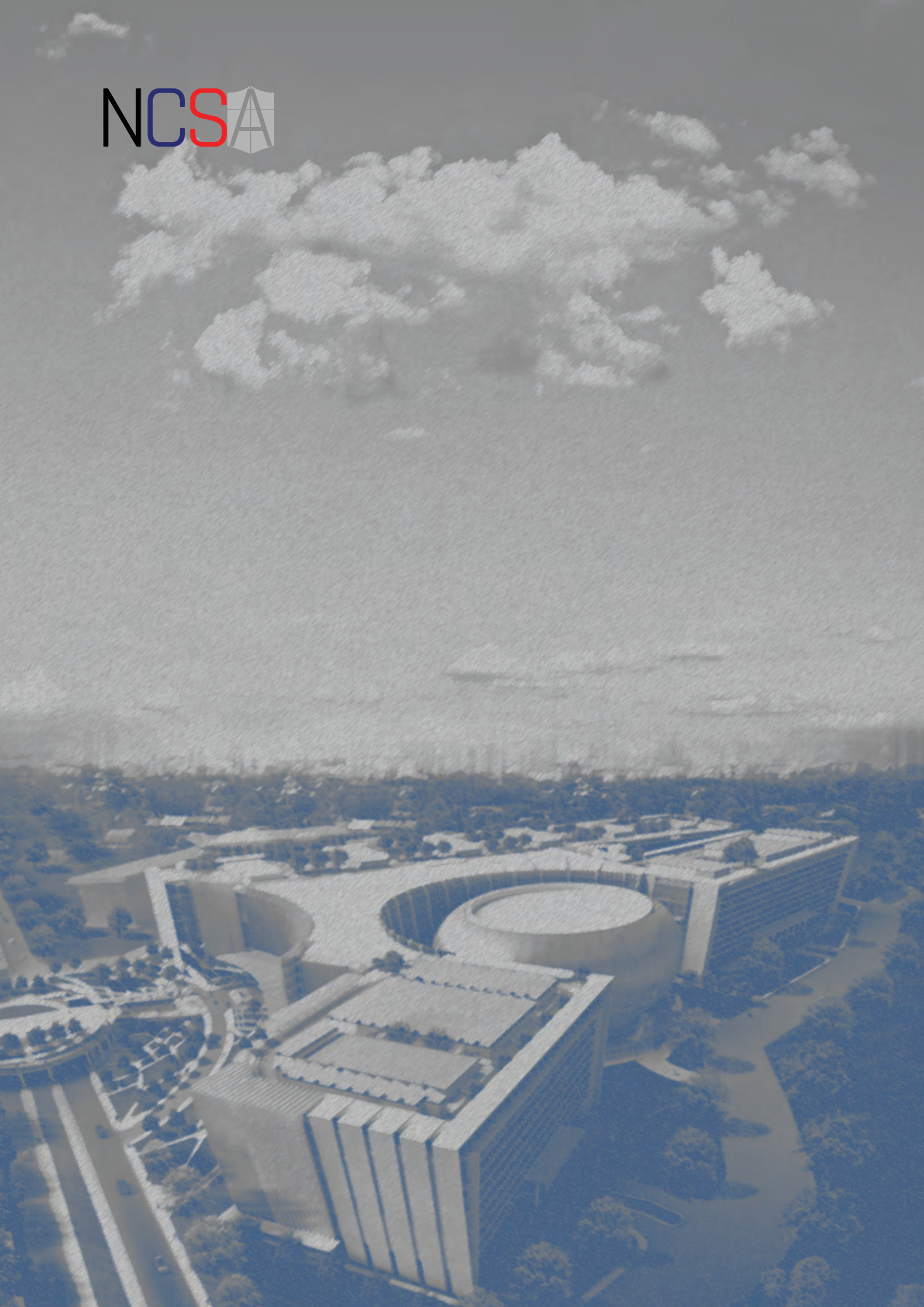
หมายเหตุที่ 20 การจัดประเภทรายการใหม่

ข้อมูลเปรียบเทียบในรายงานการเงิน ปี 2564 มีการจัดประเภทใหม่เพื่อให้สอดคล้องกับการจัดประเภทและการแสดงรายการในรายงานการเงิน ปี 2565

	(หน่วย: บาท)		
	ก่อนจัดประเภทใหม่	เพิ่ม (ลด)	หลังจัดประเภทใหม่
<u>งบแสดงผลการดำเนินงานทางการเงิน</u>			
สำหรับปีสิ้นสุดวันที่ 30 กันยายน 2564			
- ค่าตอบแทน	5,758,875.32	(1,337,936.00)	4,420,939.32
- ค่าใช้สอย	3,146,955.91	1,337,936.00	4,484,891.91

รายงานการประเมินผลการ ดำเนินงานของสำนักงานที่ ประเมินโดยบุคคลภายนอก





รายงานสรุปผลการประเมินการดำเนินงานของสำนักงาน คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประจำปี 2565

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือ “สกมช.” หรือ “NCSA” เป็นองค์การมหาชนที่จัดตั้งตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อกำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ รวมทั้งเป็นหน่วยงานรับผิดชอบงานตามพระราชบัญญัติ และประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์ที่เป็นภัยต่อความมั่นคงอย่างร้ายแรง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

ตามมาตรา 39 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดให้ สกมช. ดำเนินการจัดทำรายงานประจำปี โดยแสดงผลงานและรายการการประเมินผลการดำเนินงานของสำนักงานโดยบุคคลภายนอกที่ กบส. ให้ความเห็นชอบ ทั้งนี้ บริษัท วินทูเกเตอร์ จำกัด ได้รับการมอบหมายให้เป็นหน่วยงานที่ดำเนินการประเมิน โดยบริษัทฯ ได้ใช้กรอบในการประเมินผลการดำเนินงานองค์กรในปีแรกผ่านแนวคิดการประเมินในมุมมอง 4 มิติ ตาม “2E2S” ดังนี้

Figure ที่ 1 แสดงแนวทางการประเมินใน 4 ด้าน



มิติด้านประสิทธิผล (Effectiveness) และ มิติด้านประสิทธิภาพ (Efficiency)

จะประเมินตามแนวทางของสำนักงาน ก.พ.ร. ตามมาตรา 22 เพื่อเปรียบเทียบกับวัตถุประสงค์ของการจัดตั้งองค์กร

- 1 เสนอแนะและสนับสนุนในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์
- 2 จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เสนอต่อ กกม. เพื่อให้ความเห็นชอบ
- 3 ประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CIIT)
- 4 ประสานงานและให้ความร่วมมือในการตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ในประเทศและต่างประเทศในส่วนที่เกี่ยวข้องกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์
- 5 ดำเนินการและประสานงานกับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ตามที่ได้รับมอบหมายจากคณะกรรมการ
- 6 เผื่อระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์
- 7 ปฏิบัติการ ประสานงาน สนับสนุน และให้ความช่วยเหลือหน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ หรือตามคำสั่งของคณะกรรมการ
- 8 ดำเนินการและให้ความร่วมมือหรือช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- 9 เสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการสร้างความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ร่วมกันเพื่อให้มีการดำเนินการเชิงปฏิบัติการที่มีลักษณะบูรณาการและเป็นปัจจุบัน
- 10 เป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมทั้งเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชน

- 11 เป็นศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐและหน่วยงานเอกชนทั้งในประเทศและต่างประเทศ
- 12 ทำความตกลงและร่วมมือกับองค์กรหรือหน่วยงานทั้งในประเทศและต่างประเทศในกิจการที่เกี่ยวข้องกับการดำเนินการตามหน้าที่และอำนาจของสำนักงาน เมื่อได้รับความเห็นชอบจากคณะกรรมการ
- 13 ศึกษาและวิจัยข้อมูลที่เป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ
- 14 ส่งเสริม สนับสนุน และดำเนินการในการเผยแพร่ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์
- 15 รายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้ รวมทั้ง ปัญหาและอุปสรรค เสนอต่อคณะกรรมการเพื่อพิจารณาดำเนินการโดยจะใช้กรอบแนวคิดของสำนักงาน ก.พ.ร. ดังนี้



หลักการประเมินองค์การมหาชน ประจำปีงบประมาณ พ.ศ. 2565 ดังนี้

- มุ่งเน้นการประเมินผลการดำเนินงานตามวัตถุประสงค์การจัดตั้งขององค์การมหาชน รวมทั้งนโยบายสำคัญของรัฐบาล ดัชนีชี้วัดสากล (International KPIs) และประเมินการบริหารงานให้รองรับกับเทคโนโลยีและการเปลี่ยนแปลงต่าง ๆ ตลอดจนการดำเนินงานให้สอดคล้องต่อความคาดหวังต่อผลงานขององค์การมหาชน (Statement of Direction) ของรัฐบาลและผู้มีส่วนเกี่ยวข้อง
- ให้ความสำคัญกับเป้าหมายตามยุทธศาสตร์ แผนงาน นโยบายสำคัญหรือแผนปฏิบัติการ
- ให้ความสำคัญต่อบทบาทของคณะกรรมการองค์การมหาชนในการกำกับดูแลและติดตามการบริหารของผู้อำนวยการองค์การมหาชนและองค์การมหาชนอย่างใกล้ชิดมากขึ้น
- ให้ความสำคัญในการกำกับและติดตามผลกระทบจากการดำเนินงานขององค์การมหาชน (Impact) ซึ่งไม่สามารถวัดผลได้ในรอบปีการประเมิน โดยให้องค์การมหาชนรายงานผลสำเร็จของการดำเนินงานตามวัตถุประสงค์การจัดตั้งมายังสำนักงาน ก.พ.ร. เป็นข้อมูลสะสมสำหรับการประเมินความคุ้มค่า ในการจัดตั้งองค์การมหาชนทุก 5 ปี และใช้ในการวิเคราะห์แนวโน้มการปฏิบัติงานขององค์การมหาชนทั้งใน ระยะสั้นและระยะยาวได้อย่างต่อเนื่อง

กรอบการประเมินองค์การมหาชน ประจำปีงบประมาณ พ.ศ. 2565

ส่วนที่ 1 องค์ประกอบการประเมินผลการปฏิบัติงาน			น้ำหนักร้อยละ
การประเมินประสิทธิภาพ ประสิทธิผลของการดำเนินงาน (Performance Perspective)	องค์ประกอบที่ 1 ประสิทธิภาพการดำเนินงาน		40
	1.1	ตัวชี้วัดที่สอดคล้องกับการกิจตามวัตถุประสงค์การจัดตั้งที่แสดงให้เห็นการเชื่อมโยงจากยุทธศาสตร์ชาติ นโยบายและแผนระดับชาติ (ไม่จำกัดจำนวนแต่ให้มีตัวชี้วัดที่ครอบคลุมทุกวัตถุประสงค์การจัดตั้ง)	30
	1.2	ตัวชี้วัดที่สอดคล้องกับนโยบายสำคัญหรือแผนปฏิบัติการของกระทรวง ที่มุ่งเน้นการขับเคลื่อนการบูรณาการร่วมกันระหว่างหน่วยงานภายในกระทรวงเพื่อบรรลุเป้าหมายร่วมกัน	10
	องค์ประกอบที่ 2 ประสิทธิภาพและความคุ้มค่าในการทำงาน		30
	2.1	ตัวชี้วัดที่แสดงถึงประสิทธิภาพในการบริหารงาน/ความคุ้มค่าในการดำเนินงานเช่น ความสามารถทางการหารายได้เพื่อลดประมาณภาครัฐ อัตราส่วนของรายได้จากการดำเนินงานต่อต้นทุนคงที่ ร้อยละที่ลดลงของต้นทุนต่อหน่วยผลผลิตเป้าหมาย	25
	2.2	ร้อยละค่าใช้จ่ายด้านบุคลากรขององค์การมหาชน (ตัวชี้วัดบังคับ)	5
การประเมินศักยภาพการดำเนินงานเพื่อบรรลุเป้าหมาย (Potential Perspective)	องค์ประกอบที่ 3 ศักยภาพขององค์การมหาชน		20
	3.1	ผลการพัฒนาศักยภาพองค์การสู่การเป็นระบบราชการ 4.0 (ตัวชี้วัดบังคับ)	
	3.1.1	การพัฒนาองค์การสู่ดิจิทัล (เลือก 1 จาก 2 ตัวชี้วัดย่อยต่อไปนี้) 1) การพัฒนาระบบบัญชีข้อมูล (Data Catalog) เพื่อนำไปสู่การเปิดเผยข้อมูลภาครัฐ 2) การให้บริการผ่านระบบอิเล็กทรอนิกส์ (e-Service)	10
	3.1.2	การประเมินสถานะของหน่วยงานภาครัฐในการเป็นระบบราชการ 4.0 (PMQA 4.0)	10
	องค์ประกอบที่ 4 การควบคุมดูแลกิจการของคณะกรรมการองค์การมหาชน		10
	4.1	ร้อยละความสำเร็จของการพัฒนาด้านการควบคุมดูแลกิจการของคณะกรรมการองค์การมหาชน (ตัวชี้วัดบังคับ)	10

มิติด้านการตอบสนองต่อประชาชน (Service)

จะใช้ผลการสำรวจและประเมินการรับรู้และความพึงพอใจของหน่วยงานที่เกี่ยวข้องหรือผู้มีส่วนได้ส่วนเสีย (ตามหัวข้อ 2.2)

มิติด้านความยั่งยืน (Sustainability)

ในปีที่แล้วจะใช้ตัวชี้วัดของ กพร. ที่ใช้ประเมินองค์การมหาชน คือ ความสำเร็จของการควบคุมดูแลกิจการของคณะกรรมการองค์การมหาชน แต่เนื่องจากจะซ้ำซ้อนกับหัวข้อแรกที่ใช้ตัวชี้วัดของ ก.พ.ร. ไปแล้ว จึงจะใช้ผลการประเมิน ITA และความสำเร็จในการพัฒนาแผนทรัพยากรบุคคลเพื่อความยั่งยืนของ สกมช.

การสำรวจและประเมินการรับรู้และความพึงพอใจของหน่วยงานที่เกี่ยวข้องหรือผู้มีส่วนได้ส่วนเสีย

การวัดความพึงพอใจ เป็นการวัดความรู้สึกของบุคคลที่มีต่อสิ่งหนึ่งสิ่งใดในลักษณะหนึ่งลักษณะใด การที่เราจะทราบว่าบุคคลนั้นมีความพึงพอใจหรือไม่ สามารถสังเกตโดยการแสดงออกที่ค่อนข้างซับซ้อน จึงเป็นการยากที่จะวัดความพึงพอใจได้โดยตรง การที่จะวัดความคิดเห็นของบุคคลเหล่านั้นจะต้องตรงกับความรู้สึกที่แท้จริงจึงจะสามารถวัดความพึงพอใจที่แท้จริงได้ มีนักวิชาการได้ให้ทัศนะเกี่ยวกับการวัดความพึงพอใจไว้หลายท่าน ดังนี้

การวัดคุณภาพบริการในกระบวนการของการให้บริการสิ่งที่ธุรกิจคาดหวัง คือ ความพึงพอใจของลูกค้าที่มีต่อการบริการที่ได้รับ ดังนั้นเพื่อให้ผู้ใช้บริการรับรู้ถึงคุณภาพของการบริการ ธุรกิจสามารถพิจารณาตัวชี้วัดคุณภาพของบริการ ซึ่งสรุปได้ดังนี้

- 1 **ความสามารถ (Competence)** หมายถึง ความสามารถ ทักษะ และความรู้ของผู้ให้บริการและสามารถใช้สิ่งเหล่านั้นในการดำเนินการด้านบริการ
- 2 **ความน่าเชื่อถือ (Reliability)** หมายถึง ความสม่ำเสมอในการบริการได้อย่างถูกต้องเป็นที่น่าเชื่อถือหรือเป็นที่ไว้วางใจของผู้รับบริการ
- 3 **การตอบสนอง (Responsiveness)** หมายถึง ความพร้อมที่จะให้บริการเพื่อเป็นการตอบสนองลูกค้าได้ตรงเวลาหรือภายในเวลาที่ลูกค้าต้องการ
- 4 **ความเข้าถึงได้ (Accessibility)** หมายถึง ผู้รับบริการสามารถที่จะติดต่อกับผู้ให้บริการได้สะดวก
- 5 **ความเข้าใจผู้รับบริการ (Understanding)** หมายถึง ผู้ให้บริการจะต้องมีความเข้าใจ ความต้องการของผู้รับบริการและพร้อมที่จะเสนอตอบความต้องการดังกล่าว

6 การติดต่อสื่อสาร (Communication) หมายถึง ผู้รับบริการจะต้องเป็นผู้ฟังถึงปัญหาของผู้รับบริการ และมีความสามารถที่จะแจ้งให้เกิดความเข้าใจได้กล่าวอีกนัยหนึ่งได้ว่า ผู้ให้บริการต้องเข้าใจภาษาของผู้รับบริการเพื่อจะได้สื่อสารระหว่างกันได้เข้าใจและเกิดความพึงพอใจที่จะรับบริการต่อไป

7 ความไว้วางใจ (Creditability) หมายถึง ผู้ให้บริการควรให้บริการด้วยความซื่อสัตย์ ไม่ปิดบัง แต่ต้องโปร่งใสตรวจสอบได้

8 ความปลอดภัย (Security) หมายถึง การให้บริการด้วยความปลอดภัยต่อผู้รับบริการทั้งทางด้าน กายภาพและการเงิน

9 ความสุภาพอ่อนโยน (Courtesy) หมายความว่า มารยาทที่ดีงาม ความอ่อนน้อม การพูดจา ที่ไพเราะ ความเป็นมิตร และความเอาใจใส่ดูแลเป็นอย่างดีในขณะที่ให้บริการผู้รับบริการ

10 การจับต้องได้ (Tangibility) หมายความว่า เครื่องมือและอุปกรณ์ในการให้บริการ บุคลิกภาพ และการแสดงออกของผู้ให้บริการ สิ่งอำนวยความสะดวกต่าง ๆ เป็นต้น

ทั้งนี้ความพึงพอใจผู้รับบริการและผู้มีส่วนได้ส่วนเสีย หมายถึง ความรู้สึกของผู้รับบริการ ผู้มีส่วนได้ส่วนเสีย ไม่ว่าจะเป็นความประทับใจหรือไม่ประทับใจหลังจากการใช้ผลิตภัณฑ์และบริการโดยเปรียบเทียบกับความคาดหวังที่มีต่อผลิตภัณฑ์หรือบริการดังกล่าวความสัมพันธ์

ความพึงพอใจลูกค้า = ความคาดหวัง + บริการที่ได้รับ

นักวิชาการหลาย ๆ ท่านแสดงให้เห็นว่ามีมาตรวัดความพึงพอใจสามารถกระทำได้หลายวิธี ได้แก่

◆ การใช้แบบสอบถาม ซึ่งเป็นวิธีที่นิยมใช้กันอย่างแพร่หลาย โดยให้กลุ่มบุคคลที่ต้องการวัดแสดงความคิดเห็นลงในแบบสอบถามที่กำหนด เพื่อต้องการทราบความคิดเห็นซึ่งสามารถทำได้ในลักษณะที่กำหนดคำตอบให้เลือกหรือตอบคำถามอิสระ คำถามดังกล่าวอาจถามความพึงพอใจในด้านต่าง ๆ

◆ การสัมภาษณ์ เป็นวิธีวัดความพึงพอใจทางตรงทางหนึ่ง ซึ่งต้องอาศัยเทคนิคความชำนาญพิเศษของผู้สัมภาษณ์และวิธีการที่ดีจึงจะทำให้ผู้ตอบคำถามตอบตามข้อเท็จจริง ได้ข้อมูลที่เป็นจริงได้

◆ การสังเกต เป็นวิธีการวัดความพึงพอใจโดยสังเกตพฤติกรรมของบุคคลเป้าหมาย ไม่ว่าจะเป็นแสดงออกจากการพูด กิริยาท่าทาง วิธีนี้จะต้องอาศัย

การกระทำอย่างจริงจังและการสังเกตอย่างมีระเบียบแบบแผน

จะเห็นได้ว่า การวัดความพึงพอใจต่อการให้บริการนั้นสามารถกระทำได้หลายวิธี ขึ้นอยู่กับความสะดวก เหมาะสมตลอดจนจุดมุ่งหมายของการวัดด้วย จึงจะส่งผลให้การวัดนั้นมีประสิทธิภาพและน่าเชื่อถือได้

ความพึงพอใจในการบริการที่เกิดขึ้นในกระบวนการบริการระหว่างผู้ให้บริการและ ผู้รับบริการ เป็นผลของการรับรู้และประเมินคุณภาพของการบริการในสิ่งที่ผู้รับบริการคาดหวังว่า ควรจะได้รับ และสิ่งที่ผู้รับบริการได้รับจริงจากการบริการในแต่ละสถานการณ์การบริการหนึ่ง ซึ่งระดับของความพึงพอใจอาจไม่คงที่ผันแปรไปตามช่วงเวลาที่แตกต่างกันได้ ทั้งนี้ความพึงพอใจในการบริการ จะประกอบด้วยองค์ประกอบ 2 ประการ คือ

1 องค์ประกอบด้านการรับรู้คุณภาพของผลิตภัณฑ์บริการ ผู้รับบริการจะรับรู้ว่าคุณภาพของผลิตภัณฑ์บริการที่ได้รับ มีลักษณะตามพันธะสัญญาของกิจการบริการแต่ละประเภทตามที่ควรจะเป็นมากน้อยเพียงใด เช่น แยกที่เข้าพักในโรงแรมจะได้พักในห้องพักที่จองไว้ ลูกค้ายที่เข้าไปในภัตตาคารจะได้รับอาหารตามที่สั่ง ผู้โดยสารจะสามารถเดินทางจากที่หนึ่งไปสู่จุดหมายปลายทาง หนึ่ง หรือลูกค้าธนาคารจะได้รับการช่วยเหลือด้านสินเชื่อ ผู้รับบริการได้รับการคุ้มครองและแก้ไขความปลอดภัยไซเบอร์ เป็นต้น สิ่งเหล่านี้เป็นผลิตภัณฑ์บริการที่ผู้รับบริการควรจะได้รับตามลักษณะของการบริการแต่ละประเภท ซึ่งจะสร้างความพึงพอใจให้กับลูกค้าในสิ่งที่ลูกค้าต้องการ

2 องค์ประกอบด้านการรับรู้คุณภาพของการนำเสนอบริการ ผู้รับบริการจะรับรู้ว่ามีวิธีการนำเสนอบริการในกระบวนการบริการของผู้ให้บริการมีความเหมาะสมมากน้อยเพียงใด ไม่ว่าจะเป็นความสะดวกในการเข้าถึงบริการ พฤติกรรมการแสดงออกของผู้ให้บริการตามบทบาท หน้าที่ และปฏิภิกิริยาการตอบสนองการบริการของผู้ให้บริการต่อผู้รับบริการ ในด้านความรับผิดชอบต่องาน การใช้ภาษาสื่อความหมายและการปฏิบัติตนในการให้บริการ เช่น พนักงานโรงแรมต้อนรับแขกด้วยอัธยาศัยไมตรีจิตอันดีและช่วยเหลือแขกเรื่องสัมภาระ พนักงานธนาคารช่วยชี้แจงระเบียบข้อบังคับการยื่นขอสินเชื่อด้วยความเอาใจใส่ เจ้าหน้าที่ให้ความรู้เกี่ยวกับการรักษาความปลอดภัยไซเบอร์ด้วยความเชี่ยวชาญ เป็นต้น สิ่งเหล่านี้เกี่ยวข้องกับการสร้างความพึงพอใจให้กับลูกค้าด้วยโมตรจิตของการบริการที่แท้จริง

สรุปได้ว่า ความพึงพอใจในการบริการเกิดจากการประเมินคุณค่า การรับรู้คุณภาพของการบริการเกี่ยวกับผลิตภัณฑ์บริการตามลักษณะของการบริการ และกระบวนการนำเสนอบริการในวงจรของการให้บริการระหว่างผู้ให้บริการและผู้รับบริการ ซึ่งถ้าตรงกับสิ่งที่ผู้รับบริการมีความต้องการหรือตรงกับความคาดหวังที่มีอยู่หรือประสบการณ์ที่เคยได้รับการบริการตาม องค์ประกอบดังกล่าว ย่อมนำมาซึ่งความพึงพอใจในการบริการนั้น หากเป็นไปในทางตรงกันข้าม การรับรู้ สิ่งที่ได้รับบริการได้รับจริง ไม่ตรงกับการรับรู้สิ่งที่ผู้รับบริการคาดหวัง ผู้รับบริการย่อมเกิดความไม่พึงพอใจต่อผลิตภัณฑ์บริการและการนำเสนอบริการนั้นได้ ทั้งนี้ สามารถสรุปแนวทางการประเมินความพึงพอใจต่อการให้บริการดังนี้

ตัวแปร	เกณฑ์ที่ใช้ประเมิน
1. สิ่ง que เห็นได้ด้วยตา (tangibles)	สิ่งอำนวยความสะดวกทางกายภาพ บุคลากรที่ให้บริการ อุปกรณ์หรือเครื่องมือในการให้บริการ
2. ความน่าเชื่อถือ (reliability)	ความถูกต้องของการเรียกเก็บเงินและการจดบันทึกข้อมูล การบริการตรงตามข้อตกลง การบริการอย่างมีความน่าเชื่อถือ และถูกต้อง
3. การตอบสนองต่อลูกค้า (responsive)	การติดต่อกับลูกค้า การให้บริการอย่างรวดเร็วทันใจ การปฏิบัติตามข้อเรียกร้องที่เร่งด่วนของลูกค้า การยินดีช่วยเหลือลูกค้า

ตัวแปร	เกณฑ์ที่ใช้ประเมิน
4. การให้ความรู้สึก เชื่อมมั่น (assurance)	ความรู้และทักษะของพนักงาน ความมีชื่อเสียงขององค์กร บุคลิกภาพของผู้ให้บริการ สมรรถนะ ความสุภาพ และการให้ความรู้สึกปลอดภัยของพนักงาน
5. การเอาใจใส่ (empathy)	การรับฟังความต้องการของลูกค้า การให้บริการเป็นรายบุคคล มีการติดต่อสื่อสารที่ดี และมีความเข้าใจผู้รับบริการ

การประเมินองค์การมหาชนและผู้อำนวยการองค์การมหาชน แบบการรายงานตัวชี้วัด Monitor สรุปผลการดำเนินงานจำแนกตามรายวัตถุประสงค์

วัตถุประสงค์ ประสงค์ จัดตั้ง	ตัวชี้วัด	น้ำหนัก (ร้อยละ)	เกณฑ์การประเมิน			ผลการดำเนินงาน		
			เป้าหมาย ขั้นต่ำ (50 คะแนน)	เป้าหมาย มาตรฐาน (75 คะแนน)	เป้าหมาย ขั้นสูง (100 คะแนน)	ผลการดำเนินงาน	คะแนนที่ได้ (เทียบจากค่า เป้าหมาย)	คะแนนถ่วง น้ำหนัก
องค์ประกอบที่ 1 ประสิทธิภาพ								
1.1 ตัวชี้วัดที่สอดคล้องกับการกิจตามวัตถุประสงค์การจัดตั้งที่แสดงให้เห็นการเชื่อมโยงยุทธศาสตร์ชาติ นโยบายระดับชาติ								
ข้อ 1, 2	1.1.1 ความสำเร็จของการจัดทำนโยบาย/แผน/กฎหมาย/กฎระเบียบ/ประกาศ/มาตรการ/มาตรฐานที่สนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ	5	4 เรื่อง	5 เรื่อง และดำเนินการ ได้ตามแผน ปฏิบัติการ 3 ปี สกมช. ร้อยละ 50	6 เรื่อง และดำเนินการ ได้ตามแผน ปฏิบัติการ 3 ปี สกมช. ร้อยละ 60	มีการจัดทำนโยบาย/แผนโดยนับจากเรื่องที่ กกม. และ กมช. พิจารณาให้ความเห็นชอบแล้ว จำนวน 6 เรื่อง	100	5
ข้อ 3, 4, 7, 11	1.1.2 ร้อยความสำเร็จการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (National CERT)	4	ร้อยละ 70	ร้อยละ 85	ร้อยละ 100	ร้อยละ 100 ตามแผนคือ 1) มีรายงานแนวโน้มภัยคุกคามและความเสี่ยงต่อภัยคุกคามไซเบอร์ในภาพรวมของประเทศรายไตรมาส 2) มีหน่วยงานเป้าหมาย ติดตั้งระบบรักษาความมั่นคงปลอดภัยทางไซเบอร์ภายในองค์กร (Threat Detection System) พร้อมทั้งติดตั้งระบบ Log Collector เพื่อส่งข้อมูล Log มายัง NSCA จำนวน 3 หน่วยงาน คือ การรถไฟฯ สกม. และ อก. 3) มีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (National CERT) ที่มีเครื่องมือเพียงพอต่อการปฏิบัติงานรองรับหน่วยงาน CII	100	4

วัตถุประสงค์ จัดตั้ง	ตัวชี้วัด	น้ำหนัก (ร้อยละ)	เกณฑ์การประเมิน			ผลการดำเนินงาน		
			เป้าหมาย ขั้นต่ำ (50 คะแนน)	เป้าหมาย มาตรฐาน (75 คะแนน)	เป้าหมาย ขั้นสูง (100 คะแนน)	ผลการดำเนินงาน	คะแนนที่ได้ (เทียบจากค่า เป้าหมาย)	คะแนนถ่วง น้ำหนัก
ข้อ 6, 10	1.1.3 ร้อยละความสำเร็จการจัด ตั้งห้องปฏิบัติการความมั่นคง ปลอดภัยไซเบอร์ (Cyber Secu- rity Lab)	4	ร้อยละ 70	ร้อยละ 85	ร้อยละ 100	ร้อยละ 100 คือ 1) มีเครื่องมือการตรวจพิสูจน์ หลักฐานทางดิจิทัล เครื่อง ทดสอบการเจาะระบบ เครื่องมือ วิเคราะห์ข่าวกรองทางไซเบอร์ และเครื่องมือวิเคราะห์พฤติกรรม กลุ่มแฮกเกอร์ จำนวน 21 จาก เป้าหมาย 15 เครื่องมือ ในการ ช่วยรับมือภัยคุกคามทาง ไซเบอร์ที่เกิดขึ้น 2) มีรายงานการกำหนดยุทธการ ตอบสนองเหตุการณ์ด้านความ มั่นคงปลอดภัยทางไซเบอร์ที่ ออกไปปฏิบัติการให้หน่วยงาน ต่าง ๆ ที่เกิดเหตุการณ์โจมตีทาง ไซเบอร์ จำนวน 5 ฉบับตามเปา หมาย (EGAT, รฟท. ศาลรัฐธรรมนูญ สฟพ. และ อภ.) 3) มีหน่วยงานเป้าหมาย ที่ได้ ทำการตรวจพิสูจน์หลักฐานทาง ดิจิทัล จำนวน 11 หน่วยจาก เป้าหมาย 5 หน่วยงาน ได้แก่ 1) กรมการแพทย์ 2) กรมที่ดิน 3) โรงพยาบาลตะกั่วป่า 4) ส. คณะกรรมการสิทธิ มนุษยชน (สทม.) 5) กรมควบคุมโรค 6) สำนักงาน ปปช. 7) สำนักงานเขตพื้นที่ 8) คณะวิทยาศาสตร์ ม. รามคำแหง 9) กรมทรัพย์สินทางปัญญา 10) กรมส่งเสริมการค้า ระหว่างประเทศ 11) ศูนย์ปราบปราม อาชญากรรมทางเทคโนโลยี สารสนเทศ สำนักงานตำรวจ แห่งชาติ 4) มีหน่วยงานเป้าหมาย ที่ได้ ทำการทดสอบความปลอดภัย ของระบบ ด้วยวิธีการเจาะระบบ (Penetration Test) จำนวน 20 หน่วยงานตามเป้าหมาย จำนวน 10 หน่วยงาน (11 หน่วยงานตามรายชื่อด้านบน และหน่วยงานอื่น ทั้งภาครัฐและ เอกชน ได้แก่ WHA, โรงพยาบาลกรุงเทพ สสจ.สุราษฎร์ธานี สสจ. ศรีสะเกษ ศูนย์ฝึกอบรมตำรวจภูธรภาค 6 ม.ธุรกิจบัณฑิตย์ บริษัท น้ำันพิชไทย จำกัด โรงเรียน นวมินทราชินูทิศ โรงเรียนสิงห์สมุทร บริษัท สหวิริยาстил อินดัสตรี จำกัด)	100	4

วัตถุประสงค์ จัดตั้ง	ตัวชี้วัด	น้ำหนัก (ร้อยละ)	เกณฑ์การประเมิน			ผลการดำเนินงาน		
			เป้าหมาย ขั้นต่ำ (50 คะแนน)	เป้าหมาย มาตรฐาน (75 คะแนน)	เป้าหมาย ขั้นสูง (100 คะแนน)	ผลการดำเนินงาน	คะแนนที่ได้ (เทียบจากค่า เป้าหมาย)	คะแนนถ่วง น้ำหนัก
ข้อ 5, 8, 16	1.1.4 ร้อยละความสำเร็จใน	4	ร้อยละ 70	ร้อยละ 85	ร้อยละ 100	มีห้องศูนย์รับความช่วยเหลือ (Help Desk) รวมถึงอบรมเจ้าหน้าที่ผู้ดูแลระบบและผู้ใช้ งาน พร้อมช่องทางให้ หน่วย งานโครงการพื้นฐานสำคัญทางสารสนเทศ จำนวน 220 มีช่องทางในการแจ้งปัญหา และขอรับการสนับสนุนในกรณีเกิดเหตุภัยคุกคาม เช่น Website สกมช. Face book https://www.facebook.com/NCSA.Thailand Line: "National CERT NCSA" โอเพนแชต และช่องทางกิจกรรมอื่น ๆ นอกสถานที่ เช่น ในงาน Defense & Security 2022	100	4
ข้อ 6	1.1.5 ร้อยละความสำเร็จใน	4	ร้อยละ 70	ร้อยละ 85	ร้อยละ 100	เกินเป้าหมายคือเจ้าหน้าที่ของ สกมช.ที่ปฏิบัติหน้าที่ในห้องปฏิบัติการร่วมทางไซเบอร์ (NCSA War room) มีการประชุมหรือ จัดทำรายงานการปฏิบัติ ร่วมกับหน่วยงานต่าง ๆ จำนวน 21 หน่วยงาน (มากกว่าเป้าหมายที่กำหนดไว้คือประชุมร่วมมากกว่า 10 หน่วยงาน และติดตามผลไม่น้อยกว่า 20 หน่วยงาน	100	4
ข้อ 12	1.1.6 ความสำเร็จด้าน	1	40 ครั้ง	60 ครั้ง	80 ครั้ง	ดำเนินงานด้านความร่วมมือระหว่างประเทศ จำนวน 95 ครั้ง ทั้งรูปแบบพหุภาคี (APEC, APT, ASEAN, EU, IPEF, UN, WTO) และรูปแบบทวิภาคี (ออสเตรเลีย ฝรั่งเศส เยอรมัน ไอร์แลนด์ ญี่ปุ่น นิวซีแลนด์ สิงคโปร์ เกาหลี อังกฤษ อเมริกา) รวมถึงการประชุมในเวทีนานาชาติ เช่น การหารือด้าน Cyber-security ร่วมกับสำนักงานสภาความมั่นคงแห่งชาติ และสำนักข่าวกรองกลาง สหรัฐอเมริกา	100	1

วัตถุประสงค์ จัดตั้ง	ตัวชี้วัด	น้ำหนัก (ร้อยละ)	เกณฑ์การประเมิน			ผลการดำเนินงาน		
			เป้าหมาย ขั้นต่ำ (50 คะแนน)	เป้าหมาย มาตรฐาน (75 คะแนน)	เป้าหมาย ขั้นสูง (100 คะแนน)	ผลการดำเนินงาน	คะแนนที่ได้ (เทียบจากค่า เป้าหมาย)	คะแนนถ่วง น้ำหนัก
ข้อ 9	1.1.7 ความสำเร็จด้าน การเผยแพร่ประชาสัมพันธ์ และ สร้างความตระหนักรู้ ด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์	2	ร้อยละ 70	ร้อยละ 85	ร้อยละ 100	สำเร็จเกินกว่า เป้าหมายที่กำหนดไว้ (20,000 ราย) โดยมี ยอดผู้เข้าร่วมกิจกรรมทั้งสิ้น รวม 41,225 คน โดยจาก (1) งานสัมมนา Thailand National Cyber Week 2021 จำนวน 4,365 ราย (2) การเพิ่มทักษะผ่าน Cyber Clinic การบรรยายพิเศษ งานบริการ วิชาการ งาน Cybersecurity Knowledge Sharing จำนวน 37,860 คน	100	2
ข้อ 15	1.1.8 ความสำเร็จการประเมิน ความเสี่ยงต่อภัยคุกคามไซเบอร์ ของประเทศ	3	ร้อยละ 70	ร้อยละ 85	ร้อยละ 100	ได้ร้อยละ 90 จากเป้าหมาย กล่าวคือมีผลการจัดทำ ร่างประกาศจากผลการ ศึกษาและจัดทำประเมิน ความพร้อมในการรับมือ ความเสี่ยงต่อภัยคุกคาม ทางไซเบอร์จำนวน 3 ฉบับ โดยได้ผ่านการรับฟังความ เห็นจากผู้ที่มีส่วนเกี่ยวข้อง จำนวน 463 รายและรับ ความเห็นชอบจาก ฝ่ายบริหาร แต่ยังไม่ได้เผยแพร่ประกาศทั้ง 3 ฉบับ แก่ หน่วยงานภาครัฐนำไปใช้เป็น ทางปฏิบัติ	79.41	2.38
ข้อ 13	1.1.9 ความสำเร็จการจัดการฝึก เพื่อทดสอบขีดความสามารถทาง ไซเบอร์ต่อหน่วยงานโครงสร้าง พื้นฐานสำคัญทางสารสนเทศ	3	100 คน	150 คน	150 คน	มีรายงานผลการฝึกเพื่อ ทดสอบขีดความสามารถ ทางไซเบอร์ฯ ตามบันทึก ข้อความที่ สกมช 0600/21 โดยเป็นการฝึกรูปแบบ Hybrid โดยจำแนกผู้เข้าร่วม ฝึกตามบทบาทคือ MSEL Manager, Game Master, White Team และ Support Team โดยมีผู้เข้าร่วมฝึก ประกอบด้วยผู้แทนจากหน่วย งานควบคุมหรือกำกับดูแล หน่วยงานของรัฐ หน่วย CII ทั้ง 7 Sectors รวม 418 ราย	100	3

วัตถุประสงค์ ประสงค์ จัดตั้ง	ตัวชี้วัด	น้ำหนัก (ร้อยละ)	เกณฑ์การประเมิน			ผลการดำเนินงาน		
			เป้าหมาย ขั้นต่ำ (50 คะแนน)	เป้าหมาย มาตรฐาน (75 คะแนน)	เป้าหมาย ขั้นสูง (100 คะแนน)	ผลการดำเนินงาน	คะแนนที่ได้ (เทียบจากค่า เป้าหมาย)	คะแนนถ่วง น้ำหนัก
1.2 ตัวชี้วัดที่สอดคล้องกับนโยบายสำคัญหรือแผนปฏิบัติการของกระทรวงที่มุ่งเป็นการขับเคลื่อนการบูรณาการร่วมกัน ระหว่างหน่วยงานภายในกระทรวงเพื่อบรรลุเป้าหมายร่วมกัน								
ข้อ 14	1.2.1 ความสำเร็จการดำเนินการโครงการยกระดับทักษะบุคลากรภาครัฐเพื่อตอบสนองความต้องการของประเทศ กิจกรรม พัฒนาขีดความสามารถผู้ปฏิบัติงานตามมาตรฐานสากล	20	จำนวนผู้ได้รับการพัฒนา 300 คน และ ผู้ได้รับการพัฒนาผ่านเกณฑ์ การประเมิน ไม่น้อยกว่า ร้อยละ 60	จำนวนผู้ได้รับการพัฒนา 350 คน และ ผู้ได้รับการพัฒนาผ่านเกณฑ์ การประเมิน ไม่น้อยกว่า ร้อยละ 70	จำนวนผู้ได้รับการพัฒนา 400 คน และ ผู้ได้รับการพัฒนาผ่านเกณฑ์ การประเมิน ไม่น้อยกว่า ร้อยละ 80	มีการศึกษาการพัฒนากำลังคนด้านความมั่นคงปลอดภัยไซเบอร์ หลักสูตรความมั่นคงปลอดภัยไซเบอร์ ในระดับสากล จำนวน 3 ประเทศ และมีการจัดพัฒนาในหลักสูตรต่าง ๆ เช่น Linux+ Cloud+ Cysa+ Pentest+ ฯลฯ เป็นต้น โดยมีผู้ได้รับการพัฒนารวมทั้งสิ้น 451 รายปี และสอบผ่านการประเมินจำนวน 422 รายคิดเป็นร้อยละ 93.56	100	10
องค์ประกอบที่ 2 ประสิทธิภาพและความคุ้มค่าในการดำเนินงาน								
2.1 ตัวชี้วัดที่แสดงถึงประสิทธิภาพในการบริหารงาน/ความคุ้มค่าในการดำเนินงาน								
ข้อ 14	2.1.1 โครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Intensive Cybersecurity Capacity Building Program) ระยะที่ 1	20	จำนวนบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้รับการพัฒนา ศักยภาพ 1,500 คน	จำนวนบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้รับการพัฒนา ศักยภาพ 2,000 คน	จำนวนบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้รับการพัฒนา ศักยภาพ 2,000 คน และ ผู้ที่ได้รับการพัฒนาสอบผ่านเกณฑ์ ไม่น้อยกว่า ร้อยละ 50	มีบุคลากรเข้าร่วมการฝึกอบรมรุ่นที่ 1-45 จำนวน 2,335 คน โดยเป็นผู้ได้รับสิทธิ ECSS จำนวน 1,384 คน(59.27%) แต่ไปลงทะเบียนสอบในสถาบัน EC-Council จำนวน 1,250 คน ผ่านการสอบได้รับประกาศนียบัตรในระดับสากลจำนวน 858 คน คิดเป็น 68.7% ของผู้ลงทะเบียนเข้าสอบทั้งหมด)	100	20
2.2 ร้อยละค่าใช้จ่ายด้านบุคลากรขององค์การมหาชน								
2.2	ร้อยละค่าใช้จ่ายด้านบุคลากรขององค์การมหาชน (ตัวชี้วัดบังคับ)	5	-	-	ไม่เกินร้อยละ 30 ของแผนการใช้จ่ายเงินประจำปีตามมติ ครม. ในการประชุมวันที่ 28 พฤษภาคม 2561	คำนวณได้ = 12.46	100	5

วัตถุประสงค์ ประสงค์ จัดตั้ง	ตัวชี้วัด	น้ำหนัก (ร้อยละ)	เกณฑ์การประเมิน			ผลการดำเนินงาน		
			เป้าหมาย ขั้นต่ำ (50 คะแนน)	เป้าหมาย มาตรฐาน (75 คะแนน)	เป้าหมาย ขั้นสูง (100 คะแนน)	ผลการดำเนินงาน	คะแนนที่ได้ (เทียบจากค่า เป้าหมาย)	คะแนนถ่วง น้ำหนัก
องค์ประกอบที่ 3 ศักยภาพขององค์การมหาชน								
3.1 ผลการพัฒนาศักยภาพองค์การสู่การเป็นระบบราชการ 4.0 (ตัวชี้วัดบังคับ)								
3.1.1	3.1.1 การพัฒนาองค์การสู่ดิจิทัล (เลือก 1 จาก 2 ตัวชี้วัดย่อยต่อไปนี้) 1) การพัฒนาระบบบัญชีข้อมูล (Data Catalog) เพื่อนำไปสู่การเปิดเผยข้อมูลภาครัฐ (Open Data)	10	มีรายชื่อชุดข้อมูล (Data Set) ที่สัมพันธ์กับ Focus Area	มีคำอธิบายข้อมูล (Meta Data) 14 รายการทุกชุดข้อมูลและมีระบบบัญชีข้อมูลหน่วยงานพร้อมแจ้ง URL	มีการประเมินคุณภาพชุดข้อมูลและการนำข้อมูลไปใช้ประโยชน์	จากผลการประเมินโดยสำนักงาน ก.พ.ร. ได้คะแนน 75 คะแนน	75	7.5
3.1.2	3.1.2 การประเมินสถานะของหน่วยงานภาครัฐในการเป็นระบบราชการ 4.0 (PMQA 4.0)	10	มี (ร่าง) ผลการประเมินตามแนวทางของ PMQA 4.0	ส่งผลการประเมินสถานะของหน่วยงานภาครัฐในการเป็นระบบราชการ 4.0 (PMQA 4.0)	ได้คะแนน >350 คะแนน	ส่งผลการประเมินสถานะของหน่วยงานภาครัฐในการเป็นระบบราชการ 4.0 (PMQA 4.0) ไปแล้วแต่ได้ 210 คะแนน (บันทึกข้อความที่ สกมช 0013/13)	75	7.5
องค์ประกอบที่ 4 การควบคุมดูแลกิจการของคณะกรรมการองค์การมหาชน								
4.1	ร้อยละความสำเร็จของการพัฒนาด้านการควบคุมดูแลกิจการของคณะกรรมการองค์การมหาชน (ตัวชี้วัดบังคับ)	10	ตามคะแนนความสำเร็จของการควบคุมดูแลกิจการของคณะกรรมการองค์การมหาชนตามประเด็นที่กำหนด รวมทั้งสิ้น 9 ประเด็น	ตามคะแนนความสำเร็จของการควบคุมดูแลกิจการของคณะกรรมการองค์การมหาชนตามประเด็นที่กำหนด รวมทั้งสิ้น 9 ประเด็น	ตามคะแนนความสำเร็จของการควบคุมดูแลกิจการของคณะกรรมการองค์การมหาชนตามประเด็นที่กำหนด รวมทั้งสิ้น 9 ประเด็น	ผลการประเมินความสำเร็จของการควบคุมดูแลกิจการของคณะกรรมการองค์การมหาชนได้ 87 คะแนน โดยต้องปรับปรุงในเรื่องการประเมินผลการปฏิบัติงานของ กมช. และการจัดทำแผนดิจิทัลระยะยาว	87	8.7
รวมคะแนน								91.83

การประเมินผลการดำเนินงานองค์กรในปีที่สองผ่านแนวคิดการประเมินตามองค์ประกอบ 4 ด้าน ได้แก่

องค์ประกอบที่ 1 ด้านประสิทธิภาพ ได้ระดับคะแนน 39.38 คะแนน จากคะแนนเต็ม 40 คะแนน

องค์ประกอบที่ 2 ด้านประสิทธิภาพ ได้ระดับคะแนน 28.75 คะแนน จากคะแนนเต็ม 30 คะแนน

องค์ประกอบที่ 3 ด้านศักยภาพขององค์การมหาชน ได้ระดับคะแนน 15 คะแนน จากคะแนนเต็ม 20 คะแนน

องค์ประกอบที่ 4 ด้านการควบคุมดูแลกิจการของคณะกรรมการองค์การมหาชน ได้ระดับคะแนน 8.7 คะแนน จากคะแนนเต็ม 10 คะแนน

รวมแล้วได้คะแนนผลการประเมินการดำเนินงาน ประจำปีงบประมาณ 2565 เท่ากับ **91.83** จากคะแนนเต็ม 100 คะแนน อยู่ในระดับ **ดีมาก**

ปัญหา/อุปสรรค การดำเนินงานที่ผ่านมา

งบประมาณในปี 2565 สกมช. ได้เสนอขอรับสนับสนุนงบประมาณ จำนวน 1,000 ล้านบาทเศษ ได้รับการจัดสรรรวมงบกลางจำนวน 163 ล้านบาทเศษ คิดเป็นร้อยละ 12.16 ของคำขอของงบประมาณ ในงบประมาณปี 2566 สกมช. ได้เสนอขอรับสนับสนุนงบประมาณ จำนวน 1,200 ล้านบาทเศษ ได้รับการจัดสรรจำนวน 318 ล้านบาทเศษ คิดเป็นร้อยละ 30.64 ของคำขอของงบประมาณ สรุปแล้วงบประมาณที่ สกมช. ได้รับเพิ่มขึ้นในปีงบประมาณ 2566 เมื่อเทียบกับปีงบประมาณ 2565 จำนวน 155 ล้านบาทเศษ มีเหตุผลและความจำเป็นเพื่อที่ สกมช. จะใช้ในการเสริมความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ดังนี้

1. ด้านบุคลากร

ในปีงบประมาณ 2565 สกมช. ได้รับงบประมาณด้านบุคลากรในงบประมาณประจำปีเพียง 20 ล้านบาทเศษ ซึ่งไม่เพียงพอต่อการบรรจุพนักงานให้ได้ตามแผนและปริมาณงานที่แท้จริงโดยเฉพาะบุคลากรภาครัฐจากหน่วยงานต่าง ๆ ที่คณะรัฐมนตรีมีมติอนุมัติให้มาช่วยราชการที่ สกมช. จำนวน 42 คน ซึ่งต่อมา สกมช. ได้รับการสนับสนุนงบประมาณเพิ่มเติมจากงบกลางของรัฐบาลเป็นเงิน 19 ล้านบาทเศษ เพื่อนำมาใช้ในการบรรจุพนักงานให้มีจำนวนเพียงพอในการปฏิบัติงานรวมเป็น สกมช. ได้รับการสนับสนุนงบประมาณด้านบุคลากรในปีงบประมาณ 2565 จำนวน 40 ล้านบาทเศษ โดยปัจจุบันได้บรรจุพนักงานแล้วจำนวน 48 คน ซึ่งส่วนใหญ่เป็นบุคลากรที่ยืมตัวมาจากหน่วยงานของรัฐตามที่กล่าวไว้แล้วข้างต้น สำหรับในปีงบประมาณ 2566 สกมช. ได้รับการจัดสรรงบประมาณด้านบุคลากร จำนวน 47 ล้านบาทเศษ เพิ่มขึ้นจากปีที่ผ่านมาจำนวน 7 ล้านบาทเศษ คิดเป็นร้อยละ 14.91 ซึ่งจะสามารถบรรจุพนักงานเพิ่มเติมได้อีกไม่มากนักเป็นผลให้ สกมช. ไม่สามารถบรรจุพนักงานได้ตามเป้าหมายที่กำหนดไว้จำนวน 120 อัตราจากอัตราเต็ม 480 อัตรา แต่อย่างไรก็ตาม สกมช. จะบริหารจัดการด้านบุคลากรให้มีประสิทธิภาพสูงสุดในจำนวนงบประมาณที่ได้รับการจัดสรร

2. ด้านโครงการสำคัญตามยุทธศาสตร์ปีงบประมาณ 2565

สกมช. ได้รับงบประมาณในการจัดตั้งสำนักงาน ในช่วงแรก จำนวน 112 ล้านบาทเศษ ทำให้การจัดตั้งสำนักงานในช่วงแรก ยังมีอุปกรณ์เครื่องมือในการป้องกันและรับมือภัยคุกคามทางไซเบอร์ไม่เพียงพอ เนื่องจากอุปกรณ์เครื่องมือที่จะต้องใช้ในการป้องกันภัยคุกคามทางไซเบอร์ มีราคาสูงและมีผู้ขายน้อยราย ในปีงบประมาณ 2566 สกมช. ได้รับการจัดสรรงบประมาณโครงการจำนวน 263 ล้านบาทเศษ ซึ่งเน้นไปทางด้านการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ National CERT ให้มีความสมบูรณ์มากขึ้น/และการจัดการฝึกให้กับหน่วยงานควบคุมหรือกำกับดูแลจำนวน 19 หน่วยงาน และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจำนวน 53 หน่วยงาน รวมถึงต้องใช้ในการเร่งรัดการพัฒนาศักยภาพบุคลากรด้านไซเบอร์ของหน่วยงานทั้งภาครัฐและภาคเอกชนโดยทั่วไปด้วย

3. ด้านการสนับสนุนภารกิจสำคัญตามยุทธศาสตร์ชาติ

แรกเริ่มดำเนินการ สกมช. มีได้เป็นหน่วยรับผิดชอบแผนและยุทธศาสตร์การแก้ไขปัญหาคความมั่นคง/ด้านไซเบอร์ของชาติ ซึ่งเป็นแผนระดับ 3 ตามยุทธศาสตร์ชาติ แต่ปัจจุบัน สภาความมั่นคงแห่งชาติได้มอบหมายให้ สกมช. เป็นหน่วยรับผิดชอบงานดังกล่าวด้วย จึงทำให้ ขณะนี้ สกมช. เป็นองค์การมหาชนแห่งเดียว ที่เข้ามารับผิดชอบงานตามยุทธศาสตร์ชาติ ในด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งต้องรับภาระงานในทุกด้าน เช่น การวางแผน การอำนวยความสะดวก การบูรณาการ และประสานงานกับหน่วยงานทั้งในประเทศและต่างประเทศทุกรูปแบบโดยเฉพาะงานความร่วมมือกับต่างประเทศในรูปแบบทวิภาคี พหุภาคี และภายใต้กรอบความร่วมมือกับประเทศต่าง ๆ ซึ่งในปีงบประมาณ 2566 สกมช. ไม่ได้รับการจัดสรรงบประมาณในการปฏิบัติการกิจด้านนี้เลย แต่เพื่อให้บรรลุผลตามเป้าหมายที่รัฐบาลกำหนดไว้ สกมช. จะแสวงหาความร่วมมือกับหน่วยงานต่าง ๆ ในการปฏิบัติหน้าที่นี้ให้ดีที่สุด

4. ด้านการขับเคลื่อนนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570)

ในคราวประชุมคณะรัฐมนตรี เมื่อวันที่ 20 กันยายน 2565 คณะรัฐมนตรีได้มีมติเห็นชอบนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565- 2570) ตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เสนอ และต่อมาคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กมช.) ได้อนุมัติให้นำนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังกล่าว ไปประกาศในราชกิจจานุเบกษา เล่มที่ 139 ตอนพิเศษ 254 ง ลงวันที่ 9 ธันวาคม 2565 และมีผลใช้บังคับตั้งแต่วันที่ 10 ธันวาคม 2565 เป็นต้นไป และสำนักงาน ได้แจ้งเวียนให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามที่กำหนดไว้ในนโยบายและแผนฯ เพื่อพิจารณาดำเนินการในส่วนที่เกี่ยวข้องต่อไป

ข้อเสนอแนะ

1. การเพิ่มขีดความสามารถของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ หรือ National CERT เพื่อให้มีขีดความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์การตรวจสอบทางนิติวิทยาศาสตร์ทางคอมพิวเตอร์การกำหนดมาตรการต่าง ๆ ที่จำเป็น ได้แก่ มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์และมาตรการการรักษาและฟื้นฟู ความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

2. การพัฒนาบุคลากรด้านไซเบอร์ของหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งหน่วยงานของรัฐอื่น ๆ ให้มีจำนวนและขีดความสามารถเพียงพอในการรับมือภัยคุกคามทางไซเบอร์ที่จะเกิดขึ้นในอนาคต

3. การสร้างความร่วมมือกับหน่วยงานทั้งภายในและภายนอกประเทศในทุกมิติ ซึ่งปัจจุบัน สกมช. ได้จัดทำความร่วมมือ กับหน่วยงานองค์กรทั้งภาครัฐ ภาคเอกชน ทั้งในและต่างประเทศ รวมทั้งสถาบันการศึกษาภายในประเทศในทุกระดับเพื่อสร้างหลักสูตรและองค์ความรู้ที่เหมาะสมให้กับ ครู อาจารย์ นักเรียน นักศึกษา ในสถานศึกษาทั้งระดับประถมศึกษา มัธยมศึกษา และอุดมศึกษา เพื่อให้มีความตระหนักรู้และให้รู้เท่าทันกับภัยคุกคามทางไซเบอร์ในด้านต่าง ๆ อาทิ Stop bully hate speech

4. การสร้างความตระหนักรู้และการรับรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับประชาชนโดยทั่วไป สกมช. ได้ตระหนักถึงความสำคัญของงานสื่อสารองค์กร หรืองานข่าวประชาสัมพันธ์ การเผยแพร่ข่าวสารที่เป็นประโยชน์ จึงได้กำหนดแผนในการจัดทำสื่อประชาสัมพันธ์ในรูปแบบต่าง ๆ รวมทั้งการจัดการบรรยาย อภิปรายและเสวนา เพื่อสร้างความตระหนักรู้และให้ความรู้ ทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แก่ประชาชนทั่วไป ผ่านทางออนไลน์อย่างต่อเนื่อง

5. การขับเคลื่อนนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570) ไปสู่การปฏิบัติ โดยการ ส่งเสริม สนับสนุน ขอความร่วมมือ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้แผนฯ ร่วมสร้างความมั่นคงปลอดภัยไซเบอร์ของประเทศอย่างมีประสิทธิภาพพร้อมตอบสนองต่อภัยคุกคามไซเบอร์ทุกมิติ



บทสรุปสังเขป รายงานประจำปี 2565 ของ สกมช.

ปี 2565 นับเป็นปีที่ 2 ของการก่อตั้ง สกมช. ถ้าวางปี 2 นี้ สกมช. ได้เปิดเผยตัวตน และ ชัดความสามารถสู่สาธารณะมากกว่าปีที่ผ่านมา กระบวนการในการจัดการภายในองค์กรเริ่มมีความมั่นคงถาวรและมีระบบการจัดการต่อภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพสูงขึ้น โดยปีงบประมาณ 2565 สกมช. ได้รับการจัดสรรงบประมาณจำนวน 318 ล้านบาทเศษ ซึ่ง สกมช. ได้ให้ความสำคัญกับการทำงานใน 4 บริบท ได้แก่ การสร้างสภาพแวดล้อมที่เอื้ออำนวยต่อการสร้างความมั่นคงปลอดภัยทางไซเบอร์ให้กับประเทศ การพัฒนาและเพิ่มขีดความสามารถให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การสร้างองค์ความรู้และความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ให้กับบุคลากรของรัฐและประชาชนโดยทั่วไป และสุดท้ายเป็นการพัฒนา สกมช. สู่การเป็นองค์กรที่มีสมรรถนะสูงเพื่อเป็นแกนหลักในการอำนวยการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยได้กำหนดแผนการปฏิบัติการมุ่งเน้นใน 7 ด้านได้แก่

1. การขับเคลื่อนนโยบายและแผนด้านความมั่นคงปลอดภัยไซเบอร์
2. การจัดทำกฎหมายลำดับรอง ประกาศ ระเบียบ ที่เกี่ยวข้อง
3. ส่งเสริมความร่วมมือกับหน่วยงาน องค์กร ทั้งภายในประเทศและระหว่างประเทศ
4. เฝ้าระวัง รับมือ ภัยคุกคามทางไซเบอร์
5. การพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ตลอดจนสร้างความตระหนักรู้ให้กับประชาชน
6. การยกระดับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานของรัฐ
7. การพัฒนา สกมช. สู่การเป็นองค์กรที่มีสมรรถนะสูง

ผลการปฏิบัติงานอย่างทุ่มเทของพนักงานและลูกจ้างของ สกมช. ทุกคน ในปี 2565 ทำให้ทุกองค์ประกอบของประเทศมีการยกระดับเกี่ยวกับการป้องกันภัยคุกคามทางไซเบอร์สูงขึ้น ความตระหนักรู้และองค์ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ขยายวงกว้างมากขึ้น เป็นผลให้ภาพรวมของประเทศในทุกภาคส่วน มีขีดความสามารถในการป้องกันภัยคุกคามทางไซเบอร์สูงขึ้นกว่าปีที่ผ่านมา ซึ่งส่งผลให้การเจริญเติบโตทางเศรษฐกิจของประเทศขยายตัวอย่างมั่นคง ความเสี่ยงด้านภัยคุกคามทางไซเบอร์ลดน้อยลง ประชาชนจึงได้รับประโยชน์มากขึ้นในทุก ๆ ด้าน เนื่องจากกิจกรรมส่วนใหญ่ของประชาชนและระบบเศรษฐกิจของประเทศ พึ่งพิงระบบสารสนเทศในการใช้ชีวิตประจำวันและการดำเนินธุรกิจสูงมากขึ้นทุกปี การสร้างสภาพแวดล้อมที่ปลอดภัยจากภัยคุกคามทางไซเบอร์จึงเป็นเรื่องสำคัญยิ่งที่ สกมช. จะต้องปฏิบัติให้สำเร็จเพื่อความมั่นคงปลอดภัยของประเทศและความสงบสุขของคนไทยทุกคน

Summary of the 2022 Annual Report of NCSA

As of 2022, it has been two years since the establishment of the NCSA. In this second year, NCSA declared its status and unleashed greater capabilities to the public than the previous year. The internal organization management process has become stable. The Agency had a higher response system against cyber threats. In the fiscal year of 2022, NCSA was granted an approximate budget of 318 million baht. The four areas of particular emphasis included creating an environment supportive to cyber security maintenance in the country, increasing the capacity of critical information infrastructure agencies, establishing knowledge and awareness of the cyber threats among government authorities and the general public, and finally, developing NCSA into a high-performance organization as the central unit in maintaining national cyber security. This year, the action plan focused on the following areas:

1. Implementation of policies and plans on cyber security
2. Enactment of minor laws, notifications, and regulations applicable
3. Promoting collaboration with domestic and international organizations
4. Vigilance and response to cyber threats
5. Development of cyber security personnel and public awareness
6. Upgrading critical information infrastructure agencies and government agencies
7. Developing NCSA into a high-performance organization

Thanks to the dedication of all employees and staff at NCSA in 2022, all elements of national cyber security have been elevated, along with greater awareness and extensive knowledge of cyber threats. In the overall picture of the country, all sectors have more immunity against cyber threats than the previous year, resulting in steadier economic growth and lower cyber security risks. The Thai people have benefited from all aspects because most daily activities and economic systems increasingly rely on information technology every year. Creating a cyber threat-free environment is a critical goal NCSA must achieve for national security and the peace of all Thai people.

DNA ของ NCSA

NATIONAL CYBER SECURITY AGENCY

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

National : สกมช.เป็นองค์กร ระดับชาติ มีหน้าที่ขับเคลื่อน
สร้างความมั่นคงปลอดภัยไซเบอร์ ให้ประเทศ และ เป็นศูนย์กลางความร่วมมือ
ทั้งหน่วยงานภาครัฐเอกชน ภายในและภายนอก ประเทศ

N

+

+

Competency : สกมช. เป็นองค์กร สมรรถนะสูง
ในระดับหน่วยงาน และ ระดับบุคคล

Customer Centric : มุ่งเน้นการบริการ ประเทศ
ประชาชน หน่วยงานรัฐ เอกชน regulators และ
CII ให้ประทับใจ เกินความคาดหว้ง

C

Strong/Synergy :

สกมช. ต้องเข้มแข็งด้วยความสามัคคี ในการผนึกกำลังขับเคลื่อนภารกิจ

S

Agility :

สกมช. มีความคล่องตัว พร้อมรับมือ
กับทุกความเปลี่ยนแปลงและทุกความท้าทาย

A



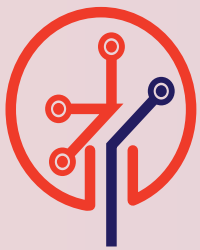
แผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566-2570)

วิสัยทัศน์ “เป็นผู้นำในการขับเคลื่อนในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์

พันธกิจ

เสนอแนะและขับเคลื่อนนโยบาย แผน ยุทธศาสตร์ และปรับปรุงกฎหมายว่าด้วยการรักษา ความมั่นคงปลอดภัยไซเบอร์ รวมทั้ง ศึกษาวิจัย กำหนดแนวทาง มาตรฐาน มาตรการ ที่เกี่ยวข้องให้สอดคล้องกับสถานการณ์ ทั้งในปัจจุบันและอนาคต

กำกับ ดูแล เฝ้าระวัง ติดตาม วิเคราะห์ ประมวลผล แจ้งเตือน และปฏิบัติการ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์



ยุทธศาสตร์ที่ 1

สร้าง **Ecosystem** ที่เอื้อต่อการรักษาความมั่นคง ปลอดภัยไซเบอร์

เป้าหมายยุทธศาสตร์

ประเทศไทยมี **Ecosystem** ที่เอื้อต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อการพึ่งพาตนเองในอนาคตอย่างยั่งยืน



ยุทธศาสตร์ที่ 2

ยกระดับและ เพิ่มขีดความสามารถในการ ประสานงานป้องกันและรับมือ ภัยคุกคามทางไซเบอร์ในทุกระดับและทุกกลุ่มเป้าหมาย

เป้าหมายยุทธศาสตร์

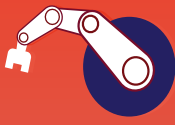
ประเทศไทยมีหน่วยงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และ หน่วยงานทุกภาคส่วนที่มีความพร้อมในการประสานงาน ป้องกันและรับมือภัยคุกคามทางไซเบอร์ในทุกมิติ

กลยุทธ์ที่ 1



พัฒนา และขับเคลื่อน นโยบาย แผนมาตรฐาน และแนวปฏิบัติ ว่าด้วยการ รักษาความมั่นคง ปลอดภัยไซเบอร์

กลยุทธ์ที่ 2



ส่งเสริมการให้บริการ และอุตสาหกรรม ด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์

กลยุทธ์ที่ 3



ส่งเสริมการวิจัย เพื่อสร้างองค์ความรู้ และเทคโนโลยีด้าน ความมั่นคง ปลอดภัยไซเบอร์

กลยุทธ์ที่ 4



ยกระดับศูนย์ประสาน การรักษาความมั่นคง ปลอดภัยระบบ คอมพิวเตอร์แห่งชาติ ในการประสานงาน ป้องกัน และรับมือ ภัยคุกคามทางไซเบอร์

กลยุทธ์ที่ 5



ขีดความสามารถ และสร้างแรงจูงใจ ให้กับหน่วยงานของรัฐ หน่วยงานควบคุมหรือ กำกับดูแล(Regulator) หน่วยงานโครงสร้าง พื้นฐานสำคัญทาง สารสนเทศ(CII) และ ส่วนงาน (Sectoral CERT) ในการประสานงาน ป้องกัน และรับมือ ภัยคุกคามทางไซเบอร์

กลยุทธ์ที่ 6



ทบทวน พัฒนา ปรับปรุง กฎหมายและมาตรการ การบังคับใช้ เพื่อให้มี เครื่องมือและกลไกใน การป้องกัน รับมือ และ ลดความเสี่ยงจาก ภัยคุกคามทางไซเบอร์ได้ อย่างมีประสิทธิภาพ

ของประเทศที่มีประสิทธิภาพพร้อมตอบสนองต่อภัยคุกคามไซเบอร์ทุกมิติ ”

เป็นศูนย์กลางในการประสานความร่วมมือ รวมทั้ง ส่งเสริม สนับสนุน และช่วยเหลือหน่วยงานภาครัฐ และเอกชน ทั้งในประเทศและต่างประเทศ เพื่อการรักษา ความมั่นคงปลอดภัยไซเบอร์

เผยแพร่ความรู้ ความเข้าใจ และสนับสนุนการพัฒนาบุคลากรด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์

ยุทธศาสตร์ที่



3

การสร้างความรู้ความตระหนักให้กับประชาชน และ การสานพลังเครือข่ายความร่วมมือ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เป้าหมายยุทธศาสตร์

ประชาชนทุกช่วงวัยมีความตระหนักรู้ด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์รวมทั้งมีการประสานงาน เครือข่ายเพื่อบูรณาการให้บุคลากรด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์ของทุกภาคส่วนมีขีด ความสามารถในการป้องกันและรับมือภัยคุกคามทาง ไซเบอร์ได้อย่างมีประสิทธิภาพ

ยุทธศาสตร์ที่



4

พัฒนาสู่ องค์กรสมรรถนะสูง
(High-Performance Organization: HPO)

เป้าหมายยุทธศาสตร์

สภมช. เป็นองค์กรชั้นนำมีบุคลากรที่มีสมรรถนะสูงและเป็นผู้ดำเนินการ ปฏิบัติงานด้วยเทคโนโลยีและนวัตกรรมที่ทันสมัยเป็นที่ยอมรับในระดับ สากล

กลยุทธ์ที่ 7



เสริมสร้างความรู้ ความเข้าใจและ สร้างความตระหนักรู้ แก่ประชาชน

กลยุทธ์ที่ 8



ขยายเครือข่ายความร่วมมือหน่วยงานรัฐ เอกชน และองค์กร ระหว่างประเทศหรือนานาชาติ เพื่อ สร้างความเข้มแข็ง ในการรักษาความมั่นคง ปลอดภัยไซเบอร์ ของประเทศ

กลยุทธ์ที่ 9



นำองค์กรด้วยเทคโนโลยี และนวัตกรรมที่ทันสมัย เพื่อการบริหารงาน ที่ยืดหยุ่นคล่องตัว และ มีประสิทธิภาพ

กลยุทธ์ที่ 10



พัฒนาระบบการจัดการ ทรัพยากรมนุษย์และ เพิ่มขีดความสามารถ บุคลากรสู่ความเป็น ผู้นำด้านการรักษา ความมั่นคงปลอดภัย ไซเบอร์

กลยุทธ์ที่ 11



แสวงหารายได้จากแหล่ง งบประมาณอื่น เพื่อ การพัฒนาที่ยั่งยืน

เรียบเรียงเนื้อหาโดย... สำนักการเงินและกลยุทธ์องค์กร
ออกแบบโดย...สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

คำจำกัดความ Definition

การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)

มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

Cybersecurity maintenance

Measures or operations established for preventing, handling, and reducing risks of internal and external cyber threats affecting national security, economic security, military security, and internal peace and order.

ไซเบอร์ (Cyber)

ข้อมูลและการสื่อสารที่เกิดจากการให้บริการ หรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

Cyber

Data and communications resulting from the provision of services, or the application of, a computer network, an internet system or a telecommunication network and also the regular provision of satellite services and similar networks of general connectivity

ภัยคุกคามทางไซเบอร์ (Cyber threat)

การกระทำหรือการดำเนินการใด ๆ โดยมีขอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมีมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง

Cyber threat

Any unlawful act or operation which is performed by the use of a computer or a computer system, or an undesirable program with an intent to cause an act of violence against a computer system, computer data, or other relevant data and which is an imminent danger causing damage to or affecting the functionality of a computer, a computer system or other relevant data.

หน่วยงานของรัฐ (Government agency)

ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์การฝ่ายนิติบัญญัติ องค์การฝ่ายตุลาการ องค์การอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ

"Government agencies"

Central administration, provincial administration, local administration, a state enterprise, a legislative organ, a judicial organ, an independent organ, a public organization and any other agency of the government

เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Incident)

เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มีขอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์หรือความมั่นคงปลอดภัยไซเบอร์คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

Cyber security incident

An incident resulting from any unlawful action or operation which is performed via a computer or a computer system and is likely to cause damage to or affect the cyber security maintenance or the cyber security of a computer, computer data, a computer system, or other data relating to a computer system a telecommunication network and also the regular provision of satellite services and similar networks of general connectivity

โครงสร้างพื้นฐานสำคัญ (Critical Infrastructure : CI)

บรรดาหน่วยงาน หรือองค์กร หรือส่วนงานหนึ่ง ส่วนงานใดของหน่วยงานหรือองค์กรซึ่งธุรกรรมทาง อิเล็กทรอนิกส์ของหน่วยงาน หรือองค์กร หรือส่วนงาน ของหน่วยงาน หรือองค์กรนั้นมีผลเกี่ยวเนื่องสำคัญต่อ ความมั่นคงหรือความสงบเรียบร้อยของประเทศหรือ ต่อสาธารณะชน

An agency or organization or any department of such an agency or organization whose electronic transactions have critical impacts on the peace and order of the country or the public

โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII)

คอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งหน่วยงานของรัฐ หรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับ การรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัย สาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือ โครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

A computer or computer system which is used by a government agency or a private agency in its affairs in connection with the maintenance of national security, public safety, national economic security, or infrastructure of public interests

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information infrastructure operator)

หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีการกิจหรือให้บริการ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ มาตรา 49 เป็นหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีดังนี้

1. ด้านความมั่นคงของรัฐ
2. ด้านบริการภาครัฐที่สำคัญ
3. ด้านการเงินการธนาคาร
4. ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม
5. ด้านการขนส่งและโลจิสติกส์
6. ด้านพลังงานและสาธารณูปโภค
7. ด้านสาธารณสุข
8. ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

A government agency or private agency which assumes missions or provides services in the following areas, according to Section 49, as critical information infrastructure agencies:

- (1) national security;
- (2) essential public services;
- (3) finance and banking;
- (4) information technology and telecommunication;
- (5) transport and logistics;
- (6) energy and public utilities;
- (7) public health;
- (8) other areas as additionally prescribed in the Notification of the Committee.

หน่วยงานควบคุมหรือกำกับดูแล (Regulator)

หน่วยงานของรัฐ หน่วยงานเอกชน หรือบุคคล ซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจใน การควบคุมหรือกำกับดูแลการดำเนินการของ หน่วยงานของรัฐหรือหน่วยงานโครงสร้าง พื้นฐานสำคัญทางสารสนเทศ

Regulatory or supervisory agency

A government agency, private agency or a person that is designated by law to have duties and powers to regulate or supervise the operation of affairs of government agencies or critical information infrastructure agencies

ผลิตภัณฑ์มวลรวมของประเทศ (Gross Domestic Product : GDP)

มูลค่าตลาดของสินค้าและบริการขั้นสุดท้ายที่ผลิตในประเทศในช่วงเวลาหนึ่ง โดยไม่คำนึงว่าผลผลิตนั้นจะเป็นผลผลิตที่ได้จากทรัพยากรภายในหรือภายนอกประเทศ ซึ่งผลิตภัณฑ์มวลรวมในประเทศสามารถใช้เป็นตัวบ่งชี้ถึงมาตรฐานการครองชีพของประชากรในประเทศ

The monetary value of all finished goods and services made within a country during a specific period, whether the goods are produced by using domestic or overseas resources. GDP can indicate the standard of living of the population in the country.

ปัญญาประดิษฐ์ (Artificial Intelligence : AI)

ระบบประมวลผลคอมพิวเตอร์ หุ่นยนต์ เครื่องจักรหรืออุปกรณ์อิเล็กทรอนิกส์ ต่างๆ ที่มีการวิเคราะห์เชิงลึกคล้ายความฉลาดของมนุษย์และสามารถ ก่อให้เกิดผลลัพธ์ที่เป็นการกระทำได้ เช่น การแปลภาษาเกิดจากการประมวลผลรับข้อความเข้าแล้วจึงแปลงออกมาเป็นภาษาหนึ่ง เป็นต้น

a computer system, robot, machine, or electronic device capable of performing tasks that typically require human intelligence and lead to various actions. For example, AI translation is done by processing input messages into a target language.

แพลตฟอร์ม (Platform)

ระบบโปรแกรมคอมพิวเตอร์ที่สามารถขยายขีดความสามารถอย่างไม่จำกัด มีการพัฒนาฟังก์ชัน หรือโมดูลใหม่ ๆ เสมอ และสามารถนำไปต่อเชื่อมกับระบบอื่นได้ แพลตฟอร์มไม่ได้จำกัดอยู่แค่ซอฟต์แวร์ แต่ยังรวมไปถึงเว็บไซต์ หรือบริการที่คนอื่นสามารถเขียนโปรแกรมมาต่อเชื่อมหรือ ดึงข้อมูลได้โดยอัตโนมัติ

A computer operating system that can expand its capacity unlimitedly with new functions and modules that can be linked with other systems. A platform is not limited only to software, but also websites or services that third parties can write computer codes to link or extract data automatically.

ดัชนีความมั่นคงปลอดภัยไซเบอร์โลก (Global Cybersecurity Index : GCI)

ดัชนีชี้วัดระดับของการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละประเทศ จัดทำโดยสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ดำเนินการร่วมกับสถาบัน ABI Research (Allied Business Intelligence) ซึ่งมีวัตถุประสงค์เพื่อสร้างแรงจูงใจให้แต่ละประเทศตระหนักถึงการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นวัฒนธรรมของโลก และหลอมรวมให้อยู่ในแก่นของเทคโนโลยีสารสนเทศและการสื่อสาร

a trusted reference that measures the commitment of countries to cybersecurity at a global level. GCI was established by the International Telecommunication Union (ITU) and operated collaboratively with ABI Research (Allied Business Intelligence) to raise each country's awareness of cybersecurity maintenance as a global culture and unite them in the core of information technology and communication.

ทีมรับมือกับสถานการณ์ฉุกเฉินที่เกี่ยวข้องกับคอมพิวเตอร์ (Computer Emergency Response Team: CERT)

กลุ่มผู้เชี่ยวชาญด้านความปลอดภัยข้อมูลที่ได้รับมอบหมายในการป้องกัน ตรวจสอบ และตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ขององค์กร CERT ซึ่งอาจมุ่งเน้นไปที่การแก้ไขเหตุการณ์ต่าง ๆ เช่น การละเมิดข้อมูลและการโจมตีแบบปฏิเสธการให้บริการ ตลอดจนการให้การแจ้งเตือนและแนวทางการจัดการเหตุการณ์ต่าง ๆ นอกจากนี้ CERT ยังดำเนินการรณรงค์สร้างความตระหนักรู้แก่สาธารณชนอย่างต่อเนื่อง และมีส่วนร่วมในการวิจัยที่มุ่งปรับปรุงระบบความปลอดภัยและเนื่องจาก CERT เป็นเครื่องหมายการค้าจดทะเบียน ดังนั้น ศูนย์ที่ทำหน้าที่ประสานและรับมือเหตุภัยคุกคามด้านความมั่นคงทางไซเบอร์ที่จัดตั้งขึ้นใหม่และต้องการใช้ชื่อที่มีคำว่า CERT จะต้องยื่นขอใบอนุญาต เสียก่อน เช่น ประเทศไทยมี Thai CERT

A group of experts specializing in protecting, detecting, and responding to cyber security. Their mission aims to warn relevant parties and solve threatening incidents, such as data breach and denial of service (DoS). In addition, CERT also launches campaigns to raise public awareness continuously and participate in research aiming to improve cyber security systems. Since CERT is a registered trademark, new cyber threat coordination and response center that wants to use the term 'CERT' is required to apply for a valid license, for example, Thai Cert in Thailand.

ทีมรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ (Computer Security Incident Response Team: CSIRT) หรือทีมรับมือสถานการณ์ที่เกี่ยวข้องกับคอมพิวเตอร์ (Computer Incident Response Teams: CIRT)

ศูนย์ประสานการรับมือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ที่สามารถรับมือและแก้ไขเหตุภัยคุกคาม ซึ่งประกอบด้วยบุคลากรที่มีความรู้และทักษะในการรับมือเหตุภัยคุกคาม ให้ความช่วยเหลือผู้รับบริการในการฟื้นตัวจากการเจาะระบบ นอกจากนี้ในการดำเนินการเชิงรุก CSIRT สามารถให้บริการตรวจสอบและประเมินช่องโหว่ของระบบสารสนเทศและความเสี่ยงต่าง ๆ รวมทั้งสร้างความตระหนักและให้ความรู้แก่ผู้เกี่ยวข้องในการพัฒนาและปรับปรุงการบริการเพื่อให้เกิดความมั่นคงปลอดภัยไซเบอร์

A cyber security threat coordination center that can address and solve threat incidents. A CSIRT has personnel with skills and knowledge for cyber threat response and assisting service users from hacking. For pro-active implementation, CSIRT can perform a PenTest and risk assessment and raise awareness of relevant individuals improving the service for higher cyber security.

APT (เอพีที)

APT ย่อมาจาก Advanced Persistent Threat คือ การที่ผู้โจมตีฝังตัวอยู่ในระบบของเหยื่อเป็นเวลานานเพื่อเฝ้าดูพฤติกรรมและดักจับข้อมูลโดยมีเป้าหมายเพื่อโจมตีหน่วยงานที่มีข้อมูลสำคัญ

A computer operating system that can expand its capacity unlimitedly with new functions and modules that can be linked with other systems. A platform is not limited only to software, but also websites or services that third parties can write computer codes to link or extract data automatically.

Data Breach (ดาต้าบริช)

การเจาะระบบและขโมยข้อมูลสำคัญออกไปขายหรือเผยแพร่โดยผู้ไม่ประสงค์ดีสามารถเข้าถึงระบบจัดเก็บข้อมูลของเหยื่อตั้งแต่ระดับบุคคลไปจนถึงระดับองค์กรได้โดยไม่ได้รับการอนุญาต เช่น การนำข้อมูลส่วนบุคคลของลูกค้าไปขาย หรือการล้วงข้อมูลงานวิจัยเพื่อแข่งขันทางการค้า เป็นต้น

Security violation, in which sensitive, protected, or confidential data of individuals or organizations are stolen, sold, or transmitted by an individual unauthorized to do so. For example, personal information of customers is sold, or research data is stolen for commercial purposes.

Fake Website (เฟค เว็บไซต์)

เป็นองค์ประกอบที่ Phisher สร้างขึ้นเพื่อล่อลวงข้อมูลโดยการสร้างเว็บไซต์ที่มีความเหมือนเว็บไซต์จริงมากที่สุดเพื่อให้ผู้ใช้งานหลงกลเข้ามาในระบบรอให้ผู้ใส่ข้อมูลส่วนตัวต่าง ๆ ทำให้ข้อมูลส่วนตัวที่ควรรักษาเป็นความลับ ถูกโจรกรรมข้อมูลไปได้ ซึ่งทำให้ผู้ใช้ได้รับผลกระทบเป็นอย่างมากเพราะข้อมูลอาจถูกนำไปใช้ในทางที่เสียหาย โดยที่เราไม่สามารถหยุดได้เลยเพราะข้อมูลเป็นข้อมูลจริงของผู้ใช้เอง ส่งผลเสียให้กับเหยื่อที่หลงกลเป็นอย่างมาก

An element that a phisher steals data by creating a website that looks like an authentic website as much as possible to phish users into the system and ask them to input personal information. As a result, confidential information is leaked, affecting a lot of users because their information might be used for a damaging purpose. The victims cannot stop the phisher because their data is real personal data. This kind of cyber threat incidents has significant impacts on the victims.

Fraud (ฟรอก)

คดีฉ้อโกง หมายถึง คดีอาญาที่ผู้กระทำความผิดมีเจตนาแสวงหาประโยชน์โดยมิชอบเอาจากผู้ถูกหลอกลวง โดยหลอกลวงด้วยการแสดงข้อความอันเป็นเท็จ หรือปกปิดข้อความจริงที่ควรบอก ซึ่งการหลอกลวงและปกปิดนั้น ผู้ถูกหลอกลวงต้องเสียทรัพย์สินให้แก่ผู้กระทำความผิดหรือทำให้ผู้ถูกหลอกลวงหรือบุคคลที่สามทำ ถอน หรือทำลายเอกสารสิทธิ นอกจากนี้ ถ้าผู้เสียหายมีจำนวน 1 คนขึ้นไป เช่นนี้เป็นคดีฉ้อโกงประชาชน (Public fraud) ซึ่งเป็นความผิดอันยอมความไม่ได้ภัยคุกคามประเภทฟรอก หรือการฉ้อโกงหลอกลวง สามารถแบ่งออกได้เป็น 2 ประเภท คือ Phishing (ฟิชซิง) คือการล่อลวงเหยื่อเข้าหน้าเว็บไซต์ปลอมซึ่งทำให้ดูคล้ายกับหน้าล็อกอินของเว็บไซต์จริง จุดประสงค์เพื่อขโมยพาสเวิร์ดและนำไปสู่การขโมยข้อมูลอื่น ๆ โดยเฉพาะในเรื่องธุรกรรมทางการเงิน Scam (สแคม) คือการแอบอ้างเพื่ออาศัยผลจากความเข้าใจผิด เช่น การสร้างหน้าเว็บไซต์ปลอมแอบอ้างว่าเป็นเว็บไซต์ของบริการที่มีชื่อเสียง หลอกให้ร่วมเล่นเกมเพื่อชิงรางวัล เพื่อขโมยข้อมูลส่วนบุคคล ซึ่งจะนำไปสู่การปลอมแปลงอื่น ๆ เพื่อผลประโยชน์ของผู้ไม่หวังดีต่อไป

Fraud is a criminal offense in which an offender exploits the victims by giving them false information or disclosing real information. As a result, the victim loses some assets to the offender, or a third party revokes or destroys title documents. If there is more than one victim, it is deemed as public fraud, which cannot be settled. Fraud offenses can be divided into two types.

Misconfiguration (มึสคอนฟิกูเรชัน)

การกำหนดค่าที่ไม่ถูกต้อง หรือไม่เหมาะสมของระบบข้อมูล หรือส่วนประกอบของระบบ ที่อาจนำไปสู่ช่องโหว่ หรือจุดอ่อนของระบบ

An incorrect or suboptimal configuration of an information system or system component that may lead to vulnerabilities

Ransomware (แรนซัมแวร์)

มัลแวร์เรียกค่าไถ่ เป็นมัลแวร์ที่เข้ารหัสลับข้อมูลในเครื่องเหยื่อ ทำให้ไม่สามารถเข้าถึงข้อมูลได้ และเรียกค่าไถ่จากเหยื่อ เพื่อแลกกับการถอดรหัสลับ

Ransomware is a type of malware encrypted in a victim's device. The malware blocks information access and demands ransom from the victim in exchange for the decryption code.

Penetration Test (เพนินทรซัน เทส)

Penetration Test หรือ PenTest เป็นวิธีการประเมินความเสี่ยงด้วยการทดสอบเจาะระบบเพื่อค้นหาจุดอ่อนในการเข้าถึงระบบต่างๆ โดยใช้ผู้เชี่ยวชาญช่วยให้สามารถประเมินความเสี่ยงของระบบเครือข่ายลูกค้าว่ามีความเสี่ยงตรงจุดใด ซึ่งจะเป็นการทดสอบเจาะระบบในเชิงลึก พร้อมแจ้งผลการทดสอบ และประเมินความเสี่ยงเพื่อเตรียมการป้องกันไว้ก่อน ซึ่งการตรวจหาช่องโหว่นี้เป็นหนึ่งในมาตรการป้องกันภัยคุกคามทางไซเบอร์ที่เหมาะสมสำหรับองค์กรที่ต้องการรักษาความปลอดภัยเป็นพิเศษ และจำเป็นต้องตรวจสอบระบบอย่างสม่ำเสมอ

Penetration test or PenTest is an authorized simulated attack performed by experts on a computer system to detect vulnerabilities. The test can assess the risk of a client's network system and identify vulnerable points. It is an in-depth hack, reports test results, and prepare preventive measures. Vulnerability identification is one of the preventive measures for organizations that need a high security level and regular system maintenance.

Social Engineering (โซเชียว อินเจเนริง)

วิศวกรรมสังคม เป็นเทคนิคการหลอกลวงโดยใช้หลักการพื้นฐานทางจิตวิทยาเพื่อให้เหยื่อเปิดเผยข้อมูล ซึ่งบางครั้งอาจไม่จำเป็นต้องใช้เทคโนโลยีเข้ามาเกี่ยวข้องเลย ผู้ที่ตกเป็นเหยื่อของ Social Engineering อาจจะตกเป็นเหยื่อโดยความตั้งใจหรือไม่ตั้งใจของผู้ไม่หวังดีก็ได้ กล่าวคือ ถ้าผู้ไม่หวังดีมีเป้าหมายเฉพาะเจาะจง เช่น ต้องการข้อมูลความลับขององค์กรใดองค์กรหนึ่ง เหยื่อในที่นี้ก็มักจะเป็นผู้ที่มีสิทธิในการเข้าถึงข้อมูลความลับขององค์กรนั้น แต่หากเป้าหมายของผู้ไม่หวังดีเป็นแบบที่ไม่ได้เจาะจงเหยื่อ เช่น ต้องการรหัสบัตรเครดิต หรือบัญชีผู้ใช้และรหัสผ่านของบริการต่าง ๆ ของใครก็ได้ เหยื่อของผู้ไม่หวังดีนี้จะเป็นใครก็ตามซึ่งหลงเชื่อการหลอกลวงนั้น

Social engineering use psychological principles to trick victims to disclose their information. They don't always use technology, and victims may be victimized with or without intention of the criminal. In other words, if a criminal has a specific target, such as confidential information of an organization, the victim could be someone who has access to such confidential information. However, if the target is not specific, such as credit card pins or account information and passwords of anybody, the victims could be anyone who is convinced by social engineering tricks.

Supply Chain Attack (ซัพพลายเชน แอทแทค)

การโจมตีไปที่ผู้พัฒนาซอฟต์แวร์ โดยมีจุดประสงค์เพื่อสอดแทรกมัลแวร์ลงในแอปพลิเคชัน ซึ่งจะทำให้ลูกค้าผู้ใช้งานแอปพลิเคชันนั้นตกเป็นเหยื่อได้โดยไม่รู้ตัว เนื่องจากมัลแวร์จะแฝงตัวมาในรูปของแอปพลิเคชันที่องค์กรซื้อใช้งานอยู่แล้ว หรืออาจจะกระจายตัวออกมาในรูปของอัปเดตสำหรับแอปนั้น จึงมีโอกาที่จะหลุดรอดจากการตรวจจับได้สูงกว่าปกติ และสามารถทำงานในเครือข่ายของเป้าหมายได้เสมือนเป็นแอปพลิเคชันดั้งเดิมที่องค์กรไว้วางใจ

A supply chain attack aims to attack software developers. The purpose is to install spying malware into an application which makes users become victims unknowingly. This is because the malware is already installed in the application that the organization is using or added later in the form of new updates. It is particularly probable that the malware to not be detected and can function in the target network similarly to an application trusted by the organization.

Website Defacement (เว็บไซต์ดีเฟซเมนต์)

การโจมตีเพื่อเปลี่ยนหน้าเว็บไซต์ของเป้าหมาย โดยที่เป้าหมายไม่อนุญาต ซึ่งผู้โจมตีมีวัตถุประสงค์เพื่อปรับเปลี่ยนหน้าเว็บไซต์แรกของเว็บไซต์เป้าหมายหรือทั้งเว็บไซต์จากเดิมไปเป็นหน้าเว็บไซต์ใหม่

Website defacement is a type of cybercrime that changes the appearance of a target website without the owner's permission. The purpose of cybercriminals is to change the home page or the whole website into a new one.

Website Phishing (ฟิชซิง)

คือคำที่ใช้เรียกเทคนิคการหลอกลวงโดยใช้อีเมลหรือหน้าเว็บไซต์ปลอมเพื่อให้ ได้มาซึ่งข้อมูล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่น ๆ เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือสร้างความเสียหายในด้านอื่น ๆ เช่น ด้านการเงิน เป็นต้น

It is a cybercriminal technique that tricks victims by using a fake email address or website to acquire such information as usernames, passwords, or other types of personal data. The acquired data is used for unauthorized access or cause other damage, such as financial damage.

คณะกรรมการจัดทำรายงานผลการดำเนินงานประจำปี พ.ศ. 2565

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
รองเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
ผู้เชี่ยวชาญด้านการจัดการองค์กร
ผู้เชี่ยวชาญด้านนโยบายและยุทธศาสตร์
ผู้ช่วยเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
ผู้ทรงคุณวุฒิพิเศษ
ผู้อำนวยการสำนัก/ ศูนย์/ ฝ่าย
ผู้อำนวยการสำนักการเงินและกลยุทธ์องค์กร
นางสาวสุกิสรา กู๊ดธราแม่
นางสาวชมพูนุท กันเขียว
นางสาวรัตนภรณ์ จันทรนาม

ประธานคณะกรรมการ
รองประธานคณะกรรมการ
คณะกรรมการ
คณะกรรมการ
คณะกรรมการ
คณะกรรมการ
คณะกรรมการและเลขานุการ
คณะกรรมการและผู้ช่วยเลขานุการ
คณะกรรมการและผู้ช่วยเลขานุการ
คณะกรรมการและผู้ช่วยเลขานุการ

ผู้รวบรวมข้อมูลและการออกแบบ

1. นางมัตติกา จงพิริยะอนันต์
2. นางสาวสุกิสรา กู๊ดธราแม่
3. นางสาวรัตนภรณ์ จันทรนาม
4. นางสาวชมพูนุท กันเขียว
5. นางสาวอรอุมา ธรรมศิริ
6. นายทศพล กลิ่นหอม
7. นายสมพล ไทยเจริญ

**“Protection
is better
than cure”**





E-Book



จัดทำโดย สำนักงานคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
พิมพ์ครั้งที่ 1 จำนวน 1,000 เล่ม
มีนาคม 2566
พิมพ์ที่ ห้างหุ้นส่วนจำกัด เพชรนครการพิมพ์
ปีที่พิมพ์ 2566
ISBN 978-616-94218-0-1

