EGAT for ALL

กฟผ. เป็นของทุกคน เพื่อทุกคน

EGAT

EGAT Information Security Management

2026

Information Security Management Policy

การบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

Information Security / Cybersecurity Policy

EGAT for ALL

ประกาศการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย
ที่ ๑๖/๒๕๖๗
เรื่อง นโยบายความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

โดยที่เห็นสมควรปรับปรุงประกาศ เรื่อง นโยบายความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ เนื่องจากมีการปรับปรุงนโยบายการบริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศของ กฟผ. เป็นไปอย่างมีประสิทธิภาพ สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ตลอดจนเกณฑ์การประเมินผลการดำเนินการรัฐวิสาหกิจด้านการพัฒนาเทคโนโลยีดิจิทัลของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) ผู้ว่าการการไฟฟ้าฝ่ายผลิตแห่งประเทศไทยออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ให้ยกเลิกประกาศการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย ที่ ๔๒/๒๕๖๕ เรื่อง นโยบายความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

ข้อ ๒ หน่วยงานสำคัญซึ่งปฏิบัติภารกิจหลักของ กฟผ. และหน่วยงานโครงสร้างพื้นฐานด้านเทคโนโลยีปฏิบัติการและเทคโนโลยีดิจิทัลของ กฟผ. ได้แก่ โรงไฟฟ้า ศูนย์ควบคุมระบบกำลังไฟฟ้า ศูนย์ปฏิบัติการภาคสถานีไฟฟ้า โครงข่ายระบบสื่อสาร การให้บริการเทคโนโลยีปฏิบัติการและเทคโนโลยีดิจิทัล มีหน้าที่ดำเนินการควบคุมและกำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

ข้อ ๓ ให้หน่วยงานตามข้อ ๒ ดำเนินการตามประมวลแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ ดังต่อไปนี้

(๑) เข้ารับการตรวจสอบด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศโดยผู้ตรวจสอบภายในอย่างน้อยปีละ ๑ ครั้ง ตามแผนการตรวจสอบประจำปีของสำนักงานตรวจสอบภายใน

(๒) ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

(๓) ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์และสารสนเทศ และฝึกซ้อมแผนการรับมือภัยคุกคามทางไซเบอร์และสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๔ ให้หน่วยงานตามข้อ ๒ ดำเนินการตามกรอบมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ ดังต่อไปนี้

(๑) ระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify) โดยครอบคลุมในเรื่อง ดังต่อไปนี้

(๑.๑) การจัดการทรัพย์สิน (Asset Management)

(๑.๒) การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

(๑.๓) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

(๑.๔) การจัดการผู้ให้บริการภายนอก (Third Party Management)

.../๒

(๒) ดำเนินการตามมาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect) โดยครอบคลุมในเรื่องดังต่อไปนี้

(๒.๑) การควบคุมการเข้าถึง (Access Control)

(๒.๒) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

(๒.๓) การเชื่อมต่อระยะไกล (Remote Connection)

(๒.๔) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

(๒.๕) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ (Information and Cybersecurity Awareness)

(๒.๖) การแบ่งปันข้อมูล (Information Sharing)

(๓) ดำเนินการตามมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์และสารสนเทศ (Detect) โดยมีกลไกและกระบวนการเพื่อตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

(๔) ดำเนินการตามมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์และสารสนเทศ (Respond) โดยครอบคลุมในเรื่อง ดังต่อไปนี้

(๔.๑) แผนการรับมือภัยคุกคามทางไซเบอร์และสารสนเทศ (Information and Cybersecurity Incident Response Plan)

(๔.๒) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

(๔.๓) การฝึกซ้อมความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ (Information and Cybersecurity Exercise)

(๕) ดำเนินการตามมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์และสารสนเทศ (Recover) โดยต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของ กฟผ. สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

ข้อ ๕ ผู้บริหารและผู้ปฏิบัติงานต้องได้รับการส่งเสริมความรู้ความตระหนักด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

ข้อ ๖ ผู้บริหารและผู้ปฏิบัติงานมีหน้าที่ปฏิบัติตามมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ กฟผ.

จึงประกาศมาเพื่อทราบและถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ ๒๐ มิถุนายน พ.ศ. ๒๕๖๗

(นายเทพรัตน์ เทพพิทักษ์)
ผู้ว่าการการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย

ฝ่ายกลยุทธ์เทคโนโลยีดิจิทัล
โทร. ๖๔๓๐๐

Link : https://it.egat.co.th/home/images/docsfiles/Digital-Risk/sar-smf/2567/cybersecurity-itc_2567.pdf

1.4 การจัดการผู้ให้บริการภายนอก (Third Party Management)

1. ต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ แม้ว่าผู้ให้บริการภายนอกจะการดำเนินงานใด ๆ ก็ตามในส่วนของบริการที่สำคัญของ กฟผ.
2. ต้องมีข้อกำหนดด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึง กระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของผู้ให้บริการภายนอก ในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก โดยข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้
    A. ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญของ กฟผ. และความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ
    B. ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญของ กฟผ. จากภัยคุกคามทางไซเบอร์
    C. ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์
    D. สิทธิ์ของ กฟผ. ในการตรวจสอบความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศของผู้ให้บริการภายนอก
3. ตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศในเงื่อนไขของสัญญา
4. เจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่

Link : https://it.egat.co.th/home/images/docsfiles/Digital-Risk/sar-smf/2568/EGAT-CS2568.pdf
https://it.egat.co.th/home/images/docsfiles/Digital-Risk/sar-smf/2568/DT_10_L2_1_68.pdf

เอกสารแนบท้ายขอบเขตของงาน (TOR) งานจัดซื้อจัดจ้างตาม พ.ร.บ.การจัดซื้อจัดจ้างและบริหารพัสดุภาครัฐ พ.ศ. 2560

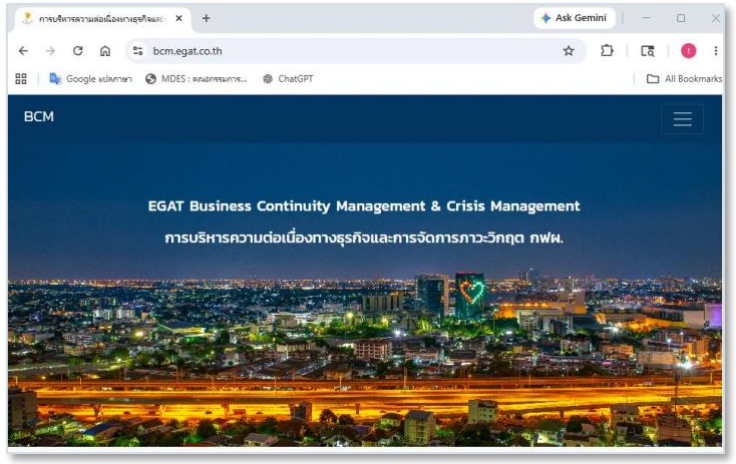
- เอกสารแนบ.... ข้อกำหนดการรักษาข้อมูลที่เป็นความลับ

Link : http://fmdiv.egat.co.th/wp-content/uploads/2026/05/เอกสารแนบท้ายขอบเขตของงาน-ข้อกำหนดการรักษาข้อมูลที่เป็นความลับ.pdf

Information Security Management Programs

การดำเนินการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

Link : https://bcm.egat.co.th

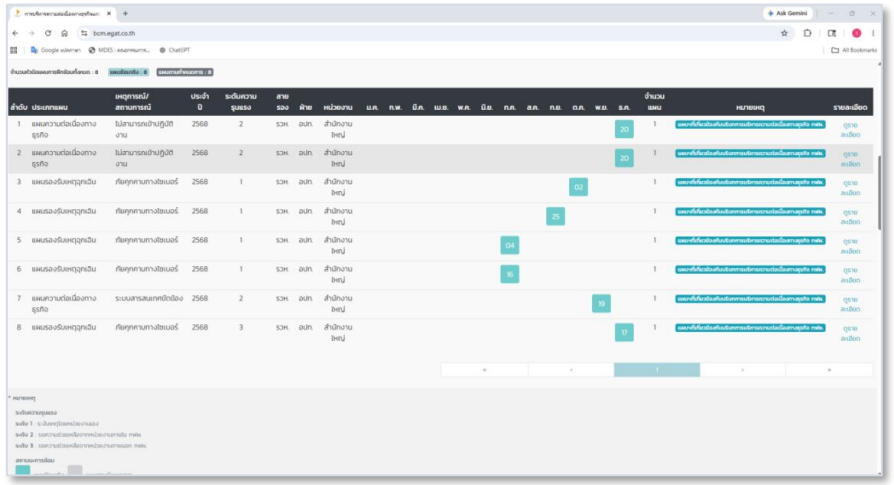


ความสำเร็จในการบริหารจัดการความต่อเนื่องทางธุรกิจด้านเทคโนโลยีดิจิทัล ประจำปี 2568

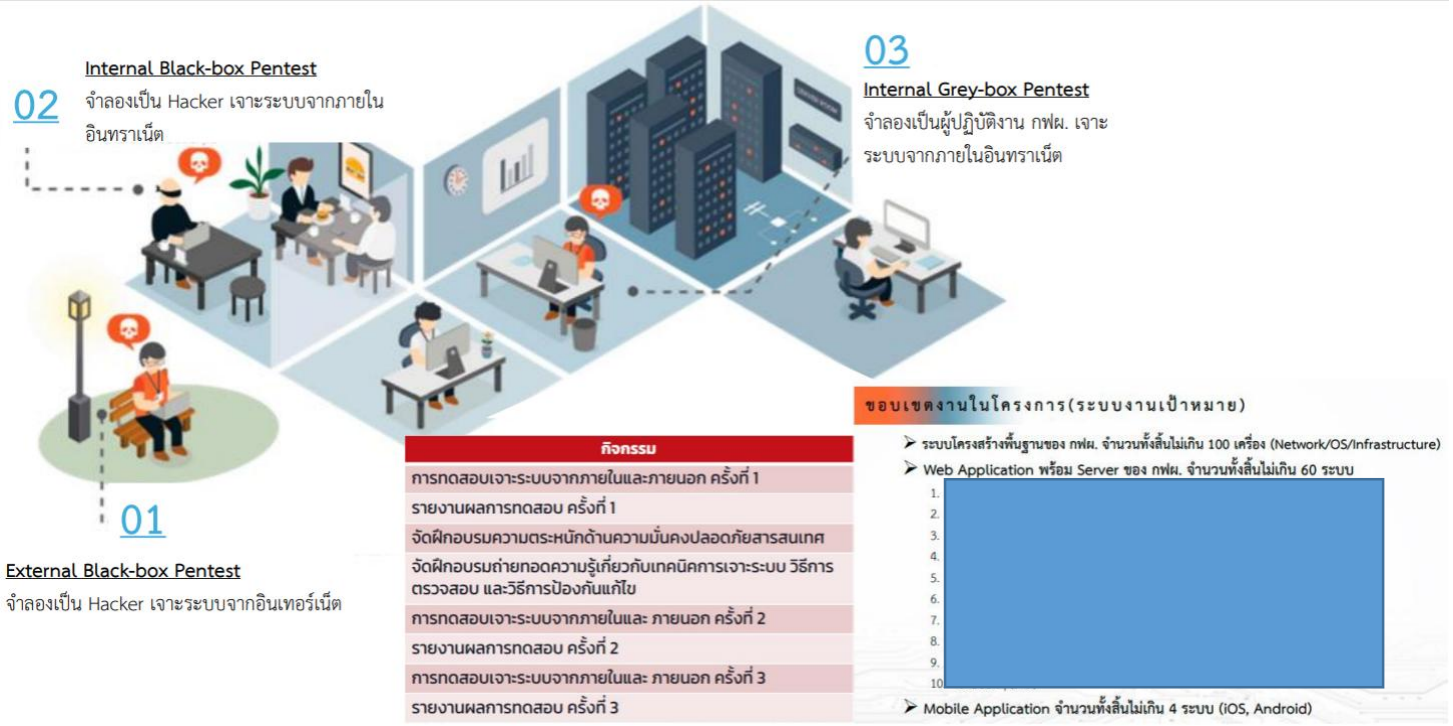
1. ทบทวนกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล
2. ทบทวนการจัดลำดับความสำคัญของระบบงาน
3. กำหนดกลยุทธ์แผนการบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีดิจิทัล
4. ทบทวน RTO/RPO
5. ดำเนินการซ้อมแผน

ความสำเร็จในการซ้อมแผนฯ ประจำปี 2568

1. แผนรองรับเหตุฉุกเฉินด้านเทคโนโลยีดิจิทัล (Incident Response Plan) จำนวน 2 แผน
2. แผนกู้คืนระบบ ณ ศูนย์สำรอง (Disaster Recovery Plan) จำนวน 1 แผน
3. แผนบริหารความต่อเนื่องทางธุรกิจ (BCP) จำนวน 1 แผน



Penetration Test / Vulnerability Analysis Scan

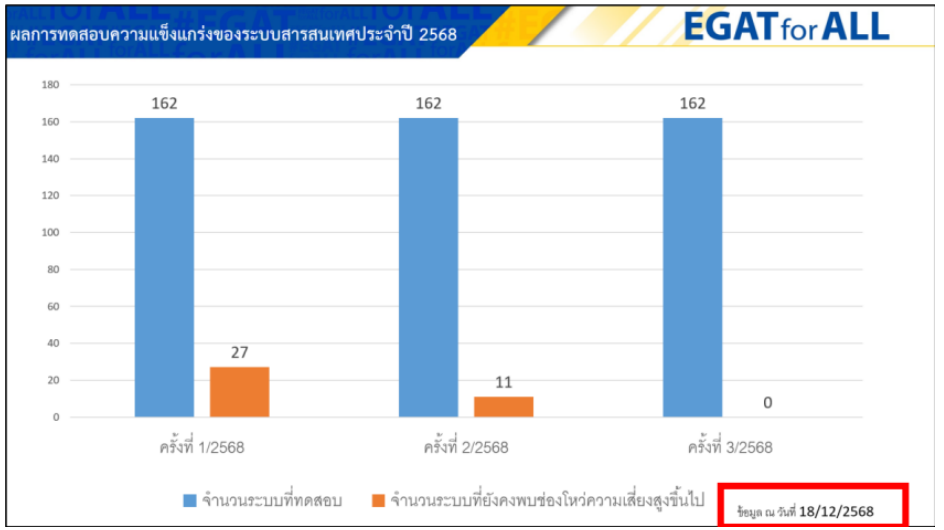


กิจกรรม
การทดสอบเจาะระบบจากภายในและภายนอก ครั้งที่ 1
รายงานผลการทดสอบ ครั้งที่ 1
จัดฝึกอบรมความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ
จัดฝึกอบรมถ่ายทอดความรู้เกี่ยวกับเทคนิคการเจาะระบบ วิธีการตรวจสอบ และวิธีการป้องกันแก้ไข
การทดสอบเจาะระบบจากภายในและ ภายนอก ครั้งที่ 2
รายงานผลการทดสอบ ครั้งที่ 2
การทดสอบเจาะระบบจากภายในและ ภายนอก ครั้งที่ 3
รายงานผลการทดสอบ ครั้งที่ 3

ขอบเขตงานในโครงการ(ระบบงานเป้าหมาย)

- ระบบโครงสร้างพื้นฐานของ กฟผ. จำนวนทั้งสิ้นไม่เกิน 100 เครื่อง (Network/OS/Infrastructure)
- Web Application พร้อม Server ของ กฟผ. จำนวนทั้งสิ้นไม่เกิน 60 ระบบ
- Mobile Application จำนวนทั้งสิ้นไม่เกิน 4 ระบบ (iOS, Android)

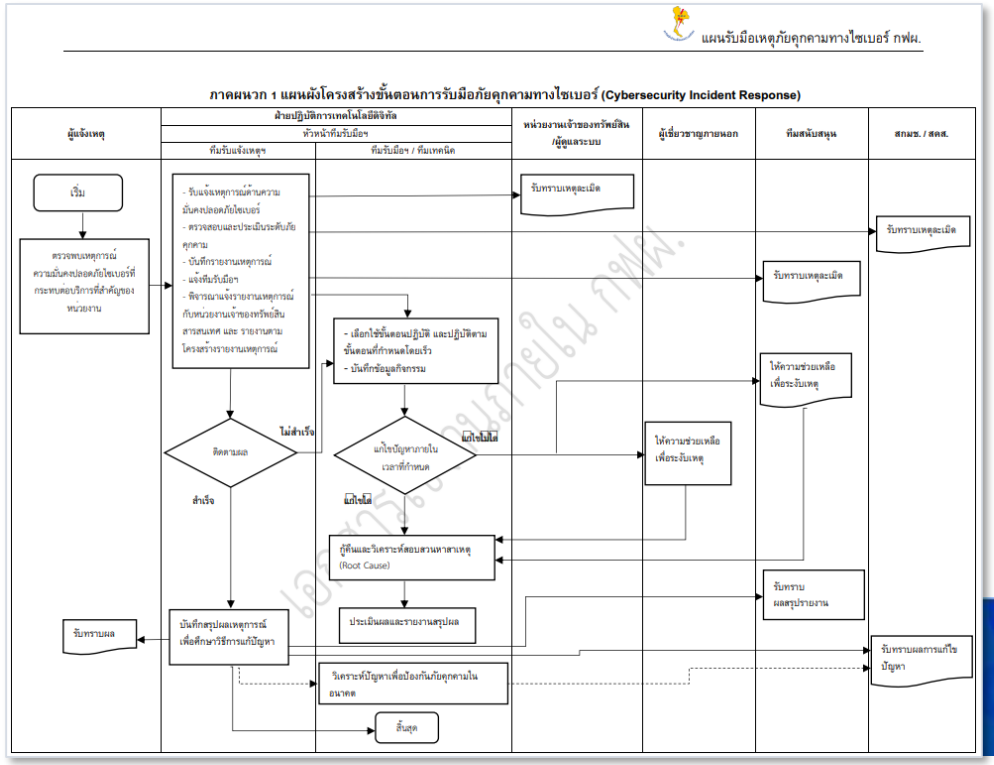
ผลการทดสอบความแข็งแกร่งของระบบประจำปี 2568 (Penetration Test 2025)



ข้อมูลจากเอกสาร :

“รายงานผลดำเนินงานทดสอบเจาะระบบ (Penetration Test) และงานประเมินช่องโหว่ (VA Scan)” นำเสนอ คณะกรรมการบริหารความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ (Head of Cyber and Information Security) ครั้งที่ 3/2568

Escalation process for employees to report incidents

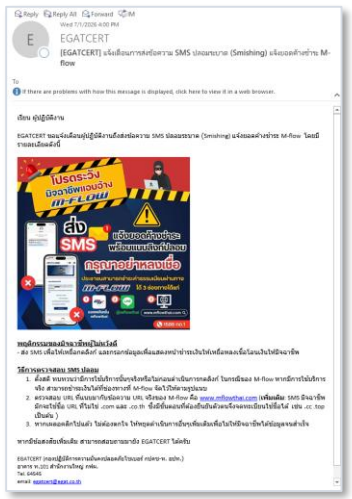


กฟผ. มีมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น มีขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response) และช่องทางสำหรับผู้ปฏิบัติงานใช้แจ้งเหตุ

<u>ช่องทางการแจ้งเหตุภัยคุกคามทางไซเบอร์</u> :

EGATCERT (กองปฏิบัติการความมั่นคงปลอดภัยไซเบอร์)
อาคาร ท.101 สำนักงานใหญ่ กฟผ.
Tel. 024364545
email: egatcert@egat.co.th

Total number of breaches

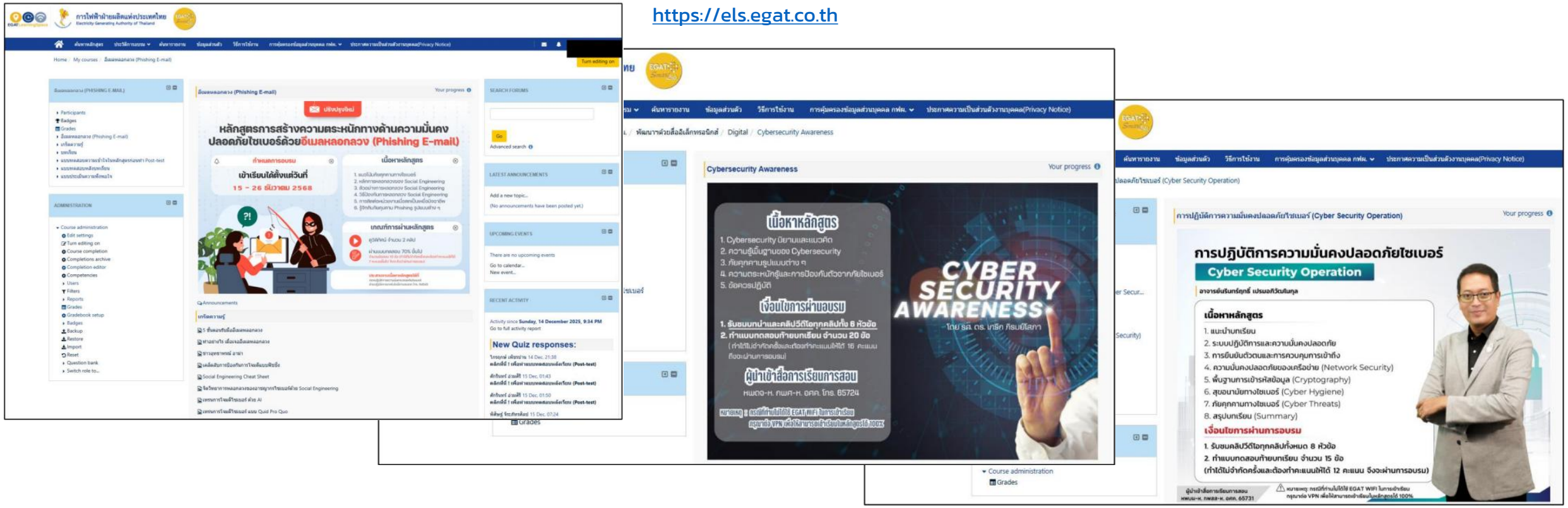


	2023	2024	2025
Total number of information security breaches or other cybersecurity incidents	0	0	0

จำนวนเหตุการณ์ภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบ
- ทำให้เกิดความสูญเสียทางการเงิน
- ทำให้การดำเนินงานตามพันธกิจหลักหยุดชะงัก
- ทำให้เกิดความเสียหายต่อภาพลักษณ์ขององค์กร

Information Security Awareness Training

EGAT for ALL



https://els.egat.co.th

ระบบการเรียนรู้ออนไลน์ กฟผ. (EGAT Learning Space) มีการจัดทำหลักสูตรความรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับผู้ปฏิบัติงาน เช่น

- อีเมลหลอกลวง (Phishing E-mail)
- หลักสูตรการปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operation)
- หลักสูตร Cyber Security for Operation Technology (OT)
- หลักสูตร Digital Literacy เป็นต้น

EGATCERT จัดกิจกรรมถ่ายทอดความรู้ในหัวข้อ ความตระหนักทางด้านความมั่นคงปลอดภัยไซเบอร์ในชีวิตประจำวัน ประจำปี 2568 ผ่านช่องทางออนไลน์ live.egat.co.th

Internal and External Audit

Internal Audit

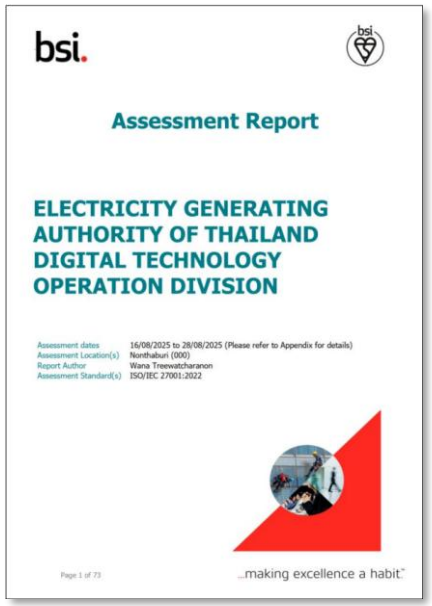
หน่วยงานผู้ช่วยผู้ว่าการสำนักงานตรวจสอบภายใน (ชกตน.) ได้ดำเนินการตรวจสอบกิจกรรม Cyber and Network Security – Information Security (IT) ตามแผนการตรวจสอบประจำปี 2568 ระหว่างวันที่ 24 กุมภาพันธ์ - 8 พฤษภาคม 2568 วัตถุประสงค์ของการตรวจสอบ เพื่อให้มั่นใจว่า กฟผ. มีการบริหารจัดการความมั่นคงปลอดภัยด้านไซเบอร์อย่างเหมาะสม

ผลการตรวจสอบ พบว่า ภายใต้ขอบเขตการตรวจสอบ หน่วยรับตรวจมีการดำเนินงานสอดคล้องและเป็นไปตามวัตถุประสงค์ของการตรวจสอบ การดำเนินงานโดยทั่วไปอยู่ในเกณฑ์ที่ดี ไม่พบประเด็นที่จะนำไปสู่ความเสี่ยงที่มีระดับนัยสำคัญสูง-สูงมาก

External Audit

กฟผ. จัดให้มีการตรวจประเมินระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อต่ออายุใบรับรอง (Re-Certification Audit) ปี 2568 ตามมาตฐาน ISO/IEC 27001 :2022 ขอบเขต "ศูนย์คอมพิวเตอร์ กฟผ."โดยขอบเขตครอบคลุมการให้บริการ

- Data Center & Infrastructure
- Intranet & Internet
- Application เช่น Microsoft 365, Database as a Service, Endpoint Management เป็นต้น


bsi.

Assessment Report

ELECTRICITY GENERATING AUTHORITY OF THAILAND DIGITAL TECHNOLOGY OPERATION DIVISION

Assessment dates 16/08/2025 to 28/08/2025 (Please refer to Appendix for details)
Assessment Location(s) Nonthaburi (000)
Report Author Wana Treewatcharanon
Assessment Standard(s) ISO/IEC 27001:2022

...making excellence a habit.


bsi.

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2022

This is to certify that:

ELECTRICITY GENERATING AUTHORITY OF THAILAND DIGITAL TECHNOLOGY OPERATION DIVISION
53 Moo 2, Charansanitwong Road,
Bang Kruai,
Nonthaburi
11130
Thailand

EGAT

Holds Certificate Number: IS 778852

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2022 for the following scope:

Provision of Data Center Services, Network Infrastructure Support, IT Services, EGAT Cloud and supporting use of public cloud, including the management of enterprise applications and customer services. The scope covers operations at EGAT's Head Office and the off-site Disaster Recovery center

This is in accordance with Statement of Applicability SP-DTO-ISC-003 Version 1/2568 Approved date 14/07/2025

For and on behalf of BSI:

Michael Lam, Senior Vice President, APAC Assurance

Original Registration Date: 2014-02-26
Latest Revision Date: 2025-09-19
Effective Date: 2026-02-26
Expiry Date: 2029-02-25

Page: 1 of 2

...making excellence a habit.