

GPSC

Information Security Management Program 2025



Content

No.	Content	Page
1.	Introduction	3
2.	Information security-related business continuity plans	4-6
3.	Information security vulnerability analysis	7-11
4.	Internal audits of the IT infrastructure and/or information security management systems	12-18
5.	Independent external audit of the IT infrastructure and/or information security management systems	19-20
6.	Escalation process for employees to report incidents, vulnerabilities or suspicious activities	21-24
7.	Information security awareness training	25-28



Introduction

In today's fast-evolving digital landscape, the protection of information assets is essential to maintaining business continuity, operational efficiency, and stakeholder trust. Recognizing the increasing complexity of cyber threats and the critical importance of safeguarding data, the company has established a comprehensive Information Security Management Program to guide its approach to information protection, risk mitigation, and regulatory compliance. The Information security management program provides a structured framework for identifying, assessing, and managing information security risks across all business units and functions. It aligns with international standards and best practices, promoting a consistent and proactive security culture throughout the organization. The program emphasizes not only technical controls but also governance, policies, awareness, and the continuous improvement of systems and processes. Through this program, the company aims to ensure the confidentiality, integrity, and availability of its information assets while supporting secure business operations, protecting stakeholder interests, and enabling sustainable digital growth.

Information security-related business continuity plans

Information security-related business continuity plans

GPSC has the business continuity plan (BCP) as practical approach in recovery the main operation of GPSC (Announced on 1 Feb 2025). The plan has included the incident response related to business continuity plan (BCP) of GPSC that covers IT System/Network Failure and cyber attack, the structure of management team associated with the incident, role and relevant department, the process of implementation, and the recovery plan from the incidents.

Objective

- Define the framework for the organization’s business continuity management during a crisis situation.
- Establish the structure of crisis management teams and related working groups, including clearly defined roles and responsibilities for each group.
- Outline the procedures to be followed in response to a crisis event. Specify the actions to be taken when the Business Continuity Plan (BCP) is activated.
- Provide definitions and terminology to ensure a shared and accurate understanding

Scope

This plan has been established for GPSC to serve as a guideline for action in the event that the BCP is triggered to activate. All personnel within the business unit are expected to adhere to the procedures outlined in this plan, as well as those detailed in the unit-specific BCP. Employees who have been assigned designated roles, whether in the Primary Response Team or the Backup Response Team, are responsible for performing the tasks associated with their roles, as specified in both this plan and the relevant unit’s continuity plan. The scenarios that are the key disaster for plan activation constitute production interruption, delivery interruption, office deny, and IT System/ Network failure.

Business continuity plan (BCP)

GPSC Group
Work Instruction
ชื่อเอกสาร: แผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan)
หมายเลขเอกสาร: PDV-WI-0030

หน้า 1 of 13
ครั้งที่แก้ไข 02
วันที่ประกาศ 1 กุมภาพันธ์ 2568


Global Power Synergy Public Company Limited

วิธีปฏิบัติงาน
Work Instruction

ข้อมูลเอกสารฉบับล่าสุด

หมายเลขเอกสาร	PDV-WI-0030	Business Unit (Function)	PSE	Dep/Div.	PDV
ชื่อเอกสาร	แผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan)			สถานะ	ประกาศใช้
Revision	02	วันที่ประกาศใช้	1 กุมภาพันธ์ 2568	จำนวนหน้า	13
ตำแหน่งที่จัดเก็บไฟล์เอกสาร	GPSC Corporate Document Management System (CDMS) / PDV / Work Instruction				

ระบบมาตรฐานที่อ้างอิง / มาตรฐานและข้อกำหนดที่เกี่ยวข้อง

ที่	ระบบ / มาตรฐาน	ข้อกำหนด
1	ISO 22301 ระบบบริหารความต่อเนื่องทางธุรกิจ	ทุกข้อกำหนด



Information security-related business continuity plans

As part of GPSC's Business Continuity Plan, the information security component includes scenario-based planning to address critical threats such as IT system or network failures and cyberattacks. These events are identified as key triggers for activating the continuity plan. In response, the plan outlines detailed, step-by-step procedures to guide the recovery process, ensuring that business operations can be restored efficiently and effectively in the event of a disruption. This approach enhances organizational resilience and preparedness against information security incidents.

สถานการณ์หลัก (Key Scenarios)	สถานการณ์ย่อย (Sub Scenarios)
1. การหยุดชะงักของกระบวนการผลิต (Production interruption)	Confidential
2. การหยุดชะงักของการส่งมอบผลิตภัณฑ์ (Delivery interruption)	
3. ไม่สามารถเข้าปฏิบัติงานในสถานที่ (Office Deny)	
4. ระบบเทคโนโลยีสารสนเทศไม่สามารถใช้งาน (IT System/Network Failure)	4.1 โจมตีทางไซเบอร์ (Cyber Attack)

ลำดับ	แผนปฏิบัติงาน	ผู้รับผิดชอบ
1.	เตรียมความพร้อมคอมพิวเตอร์ - จัดหาเครื่องคอมพิวเตอร์สำหรับพนักงาน และ ติดตั้งระบบ Remote Support และ ระบบ Conference ในคอมพิวเตอร์พนักงาน	Confidential
2.	เตรียมความพร้อมสำหรับการทำงานระยะไกล - ติดตั้งระบบ VPN ในคอมพิวเตอร์พนักงาน	
3.	เฝ้าระวังการโจมตีทางไซเบอร์ผ่านระบบ CSOC โดยผู้ให้บริการ PTT Digital	
4.	เตรียมความพร้อมแก้ไขระบบ Network ด้วยกระบวนการ Incident Management	
5.	เตรียมความพร้อมของ DR-Site และมี DR-Drill ของระบบต่าง ๆ ประจำปี	
6.	เตรียมความพร้อมแผนรับมือการโจมตีทางไซเบอร์ของระบบ IT โดยการทำให้ Cyber Drill ประจำปี	
7.	เตรียมความพร้อมแผนรับมือการโจมตีทางไซเบอร์ของระบบ OT โดยการทำให้ Cyber Drill ประจำปี ร่วมกับตัวแทนของโรงงาน	

Information security vulnerability analysis

In 2024, GPSC carried out an external audit, including a comprehensive vulnerability assessment and penetration testing, to identify and address potential weaknesses in its digital systems. The evaluation was conducted by specialized cybersecurity firm (DA Digital Associates Co., Ltd.) to ensure the integrity, resilience, and security of GPSC's IT infrastructure.

Date: 06 Nov 24 to 18 Dec 24

The assessment resulted in two different level of status, including critical and high levels of vulnerability through testing.

Old IP found from records

Information security vulnerability analysis (2/4)

GPSC carried out an external audit for vulnerability assessment to identify and address potential weaknesses in its digital systems. The evaluation was conducted by specialized cybersecurity firm (Tenable, Inc.) to ensure the integrity, resilience, and security of GPSC's IT infrastructure.

Assessor: Tenable, Inc.

Date: 06 Nov 24 to 18 Dec 24

Result:

The assessment resulted in five different level of status, including critical, high, medium, low, and info levels of vulnerability through testing.



Information security vulnerability analysis (3/4)

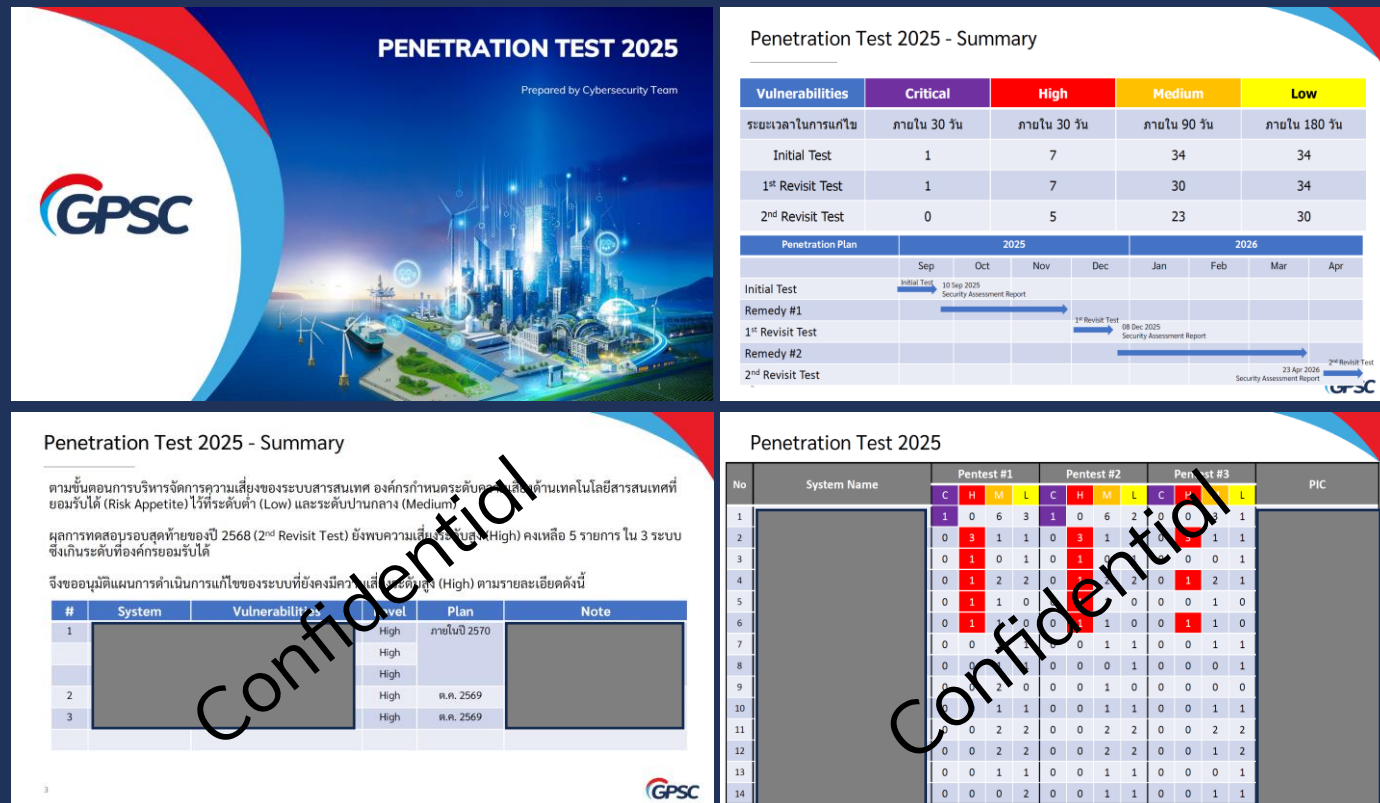
In 2025, GPSC applies a defined risk appetite (accepting only Low and Medium residual risk) and manages identified vulnerabilities through a closed-loop remediation process. Each finding is assigned an owner and a severity-based remediation timeline, and is re-tested in subsequent review rounds to verify that fixes are effective.

Classification : Critical / High / Medium / Low (per CVSS v3.1)

Review cycle: Initial >> 1st Revisit >> 2nd Revisit (3 rounds)

Result:

The majority of previously reported issues were remeasured across the revisit rounds; residual high-risk items are placed under a time-bound remediation plan with assigned owners.



Information security vulnerability analysis (4/4)

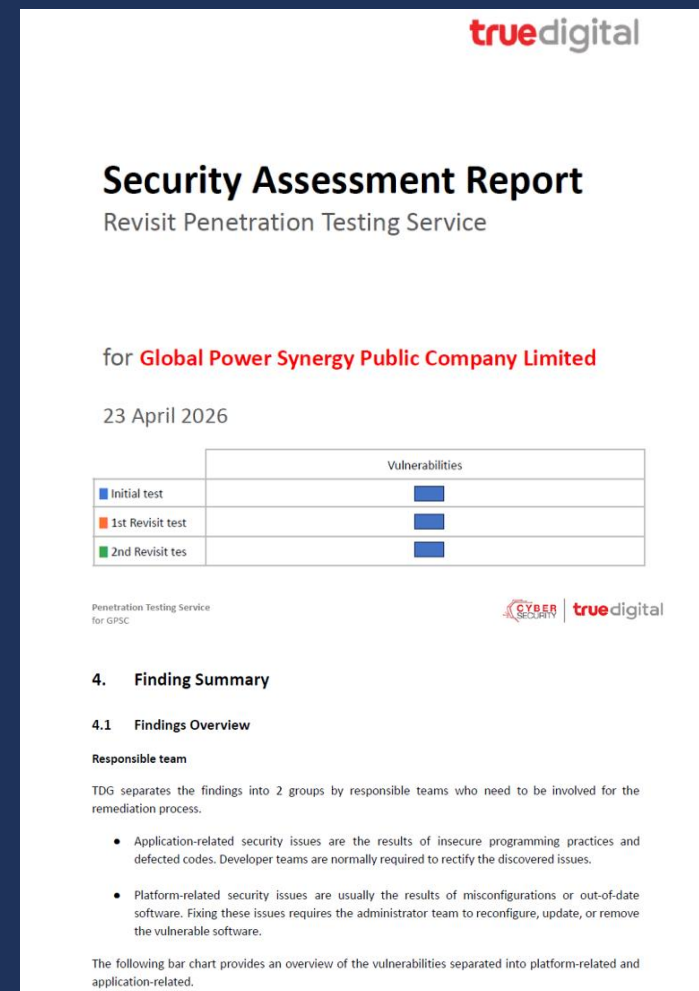
In 2025, GPSC carried out an external audit, including a comprehensive vulnerability assessment and penetration testing, to identify, classify and prioritize potential weaknesses in its network, application and cloud (SaaS) infrastructure. The assessment was conducted by an independent cybersecurity specialist to ensure the integrity, resilience and security of GPSC's IT infrastructure.

Assessor: TDG (independent cybersecurity specialist)

Period: 10 Sep 2025 - 23 Apr 2026 (Initial test + 2 revisit rounds)

Result:

The revisit assessment identified remaining vulnerabilities. The three high-risk findings relate to file-upload handling, broken authorization (IDOR) and unprotected web pages/APIs.



Internal audits of the IT infrastructure and/or information security management systems

Internal audits of the IT infrastructure and/or information security management systems (1/6)

In 2024, GPSC conducted comprehensive internal audits to evaluate and enhance the integrity, resilience, and security of its IT infrastructure and information security management systems. These audits aimed to ensure preparedness against potential disruptions and cyber threats across the organization. Key activities included a:

- Disaster Recovery (DR) and emergency drill for the SAP S/4 HANA system to test business continuity capabilities,
- Tabletop cyber drills focused on both operational technology (OT) and information technology (IT) systems to simulate and respond to cybersecurity incidents.
- Additionally, GPSC tested its DR plan for Cloud Infrastructure as a Service (IaaS) to validate cloud recovery protocols, and
- Carried out a phishing email simulation to assess employee awareness and response to social engineering threats.

These proactive measures reflect GPSC's commitment to maintaining a secure and resilient digital environment.

Internal audits of the IT infrastructure and/or information security management systems (2/6)

In 2024, GPSC carried out its annual Disaster Recovery (DR) and Emergency Drill for the SAP system, aiming to ensure organizational readiness in the event of an unexpected incident. The drill was designed to test the effectiveness of incident management procedures, confirm the clarity of roles and responsibilities among employees, and assess their ability to respond promptly and accurately during disruptions. In addition to evaluating the SAP S/4 HANA system, the exercise also involved critical components of GPSC's broader IT infrastructure, including servers, network configurations, storage systems, and backup environments, to ensure system interoperability and infrastructure resilience. The drill assessed the organization's Recovery Point Objective (RPO) and Recovery Time Objective (RTO) in accordance with the defined Service Level Agreement (SLA). This proactive initiative not only strengthens GPSC's operational resilience but also supports continuous improvement in business continuity and IT system recovery capabilities.

Date of internal audit: 21 Sep 2024

Annual disaster recovery and emergency drill (DR drill) for SAP S/4 HANA

Sep 21, 2024

DR process prepared by Sivapong T. & Ratcharin U.



Test State

วันเสาร์ที่ 21 กันยายน 2024 เวลา 08.00-22.45 **ระยะเวลาในการซ้อม 12 ชั่วโมง**

DR Drill Step	Activities	Responsible	Duration	
State 1		GPSC DR Team	8.00 – 9.00 น. 1 ชั่วโมง	
State 2		GPSC IT / SAP ECS	9.00 – 16.15 น. 7 ชั่วโมง 15 นาที	
		GPSC End Users / GPSC IT Functional (Partial support by AMS)	16.15 – 18.15 น. 2 ชั่วโมง	
State 3		GPSC IT / SAP ECS	18.15 – 20.10 น. 1 ชั่วโมง 55 นาที	
		GPSC End Users / GPSC IT Functional (Partial support by AMS)	20.10 – 22.10 น. 2 ชั่วโมง	
		GPSC IT	22.10 – 22.45 น. 35 นาที	

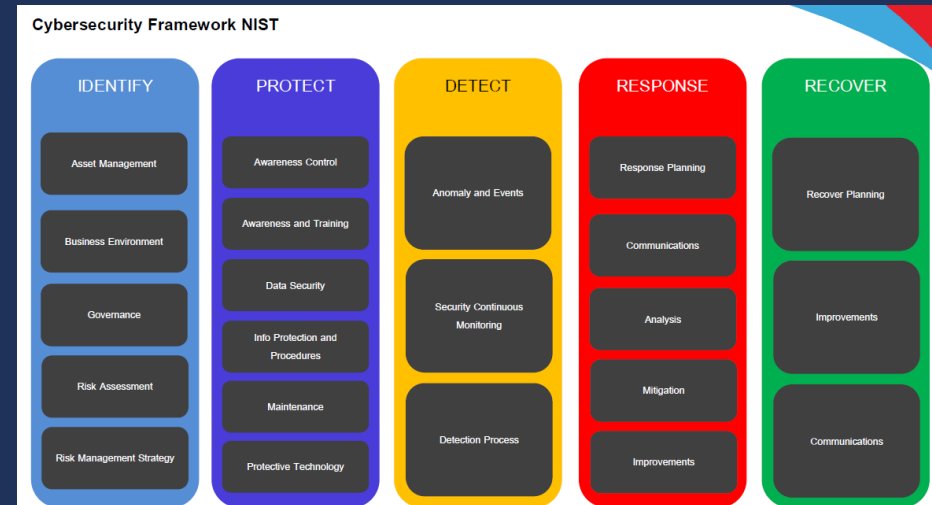


Internal audits of the IT infrastructure and/or information security management systems (3/6)

GPSC conducted cyber drill tabletop activities for operation technology and information technology in 2024 to prepare the readiness for quick incident response to recover the business operation, establish the comprehensive understanding the process for incident management for employees, and ensure role and responsibility of all employees for cyber security.

The scope of test involved a tabletop exercise combined with the activation of a command center to oversee the response. The simulation focused on handling a cybersecurity threat scenario, specifically a Zero-Day Malware Attack. Key participants in the drill included the Cyber Warfare Team (CWT), Information Security Management System (ISMS) team, Enterprise Technology Management (ETM), Plant Operation (C&I), and external service providers. The simulated attack was designed to impact critical systems such as the PI Server, PI Interface, and OPC, which in turn affected operations at CUP1, CUP4, GIPP, and Phase 5 plants. Notably, the production systems were not shut down, as the exercise was purely procedural. The entire drill was conducted online with the command center operating virtually via Microsoft Teams.

Date of internal audit: 21 Oct 2024 to 11 Dec 2024



Internal audits of the IT infrastructure and/or information security management systems (4/6)

The test focused on evaluating the organization’s response to a critical incident affecting core IT infrastructure. It aimed to assess the effectiveness of emergency communication, decision-making, and coordination between internal teams and service providers. An internal audit tested the continuity of key systems and services, such as user authentication and file access, and involved declaring an emergency to ensure appropriate escalation and recovery actions were taken within the defined timeframe.

Date of internal audit: 22 Nov 2024



Test State

จัดซ้อมในวันที่ 22 พฤศจิกายน 2567 รายละเอียดดังนี้

DR Drill Step	Activities	Responsible	Duration
State 1		GPSC DR Team	13.00 – 13.15 น. 15 นาที
		GPSC DR Team	13.15 – 14.45 น. 1 ชั่วโมง 30 นาที
State 2		GPSC IT / Dailitech / PTT Digital	14.45 – 17.35 น. 2 ชั่วโมง 50 นาที
State 3		GPSC IT / Dailitech / PTT Digital	17.35 – 23.55 น. 6 ชั่วโมง 20 นาที

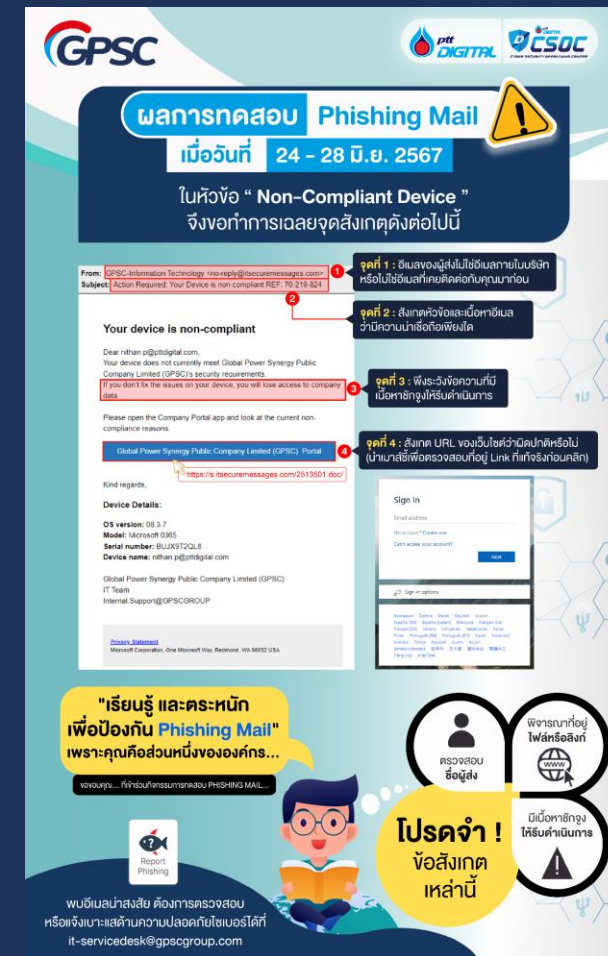
== Internal Use Only ==

Internal audits of the IT infrastructure and/or information security management systems (5/6)

Phishing email simulation is one of the key internal audit programs implemented by GPSC across the organization. Conducted annually, this program serves as a practical assessment of employees' ability to recognize and respond to phishing attempts, following their participation in cybersecurity awareness training. The simulation helps evaluate the effectiveness of the training program by measuring real-time responses to potential threats, identifying areas where additional support or education may be needed, and reinforcing a culture of vigilance. This proactive approach plays a crucial role in strengthening the organization's overall cybersecurity posture and minimizing the risk of social engineering attacks.

Date of internal audit:

- 24 Jun 2024 to 28 Jun 2024
- 26 Aug 2024 to 30 Aug 2024



Internal audits of the IT infrastructure and/or information security management systems (6/6)

In 2025, GPSC conducts internal audits of its Information Security Management System (ISMS) against the ISO/IEC 27001:2022 standard. The most recent internal audit was carried out on 15–16 July 2025 by formally appointed independent auditors.

The audit assessed the full management-system requirements. Areas verified included information security policy and roles, technical vulnerability management, business continuity and IT disaster recovery, incident management, access control, change management, and information security awareness. Audit results are recorded against a conform / non-conformity / observation status, escalated through corrective and preventive action (CAR/PAR) tracking, and fed into management review for continual improvement.

Supporting practices confirmed during the audit include a technical vulnerability management program combining regular vulnerability scanning and annual penetration testing, with defined remediation timeframes based on severity; a documented business continuity plan supported by an ISO 22301 certification and a disaster-recovery site hosted across three availability zones; a structured information security incident management process with defined severity classifications and escalation channels; and recurring security awareness training delivered through the company's e-learning platform and new-employee onboarding.

Audit Check List
(รายการคำถามตรวจสอบประเมินภายใน ISO/IEC 27001:2022)

วัตถุประสงค์การตรวจ ตรวจสอบข้อกำหนดมาตรฐาน ISO/IEC 27001:2022 ในขอบเขตของ ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศใช้กับ ศูนย์ข้อมูลหลัก (Data Center) และระบบคลาวด์ (Cloud management for IaaS) รวมถึงโครงสร้างพื้นฐานเครือข่ายและถึงอำนวยความสะดวกที่รองรับ ซึ่งดำเนินการโดย บริษัท โกลบอล เพาเวอร์ ซินเนอร์ยี่ จำกัด (มหาชน) เป็นไปตาม Statement of Applicability (SoA)

เกณฑ์การตรวจ

- มาตรฐาน ISO/IEC 27001:2022

ขอบข่ายของการตรวจ หน่วยงาน GPSC Group Digital Platforms (PDV) & Digitalization Strategy (SDM) **วันที่ตรวจสอบประเมิน** : 15-16 กรกฎาคม 2568

ผู้ตรวจประเมิน	1.	(Lead Auditor)		(Auditor)
	3.		4.	
	5.		6.	
	7.		8.	

Internal ISMS Audit Checklist_v.1.0

Independent external audit of the IT infrastructure and/or information security management systems

External audit of the IT infrastructure and/or information security management systems

In 2024, GPSC underwent an external audit of its IT infrastructure and information security management systems, conducted by BSI Group. As part of this process, GPSC upgraded its certification from ISO/IEC 27001:2013 to **ISO/IEC 27001:2022**. The transition reflects the organization's commitment to maintaining a robust and up-to-date information security framework. The updated 2022 version of the standard introduces a more structured approach to risk management, enhanced alignment with modern cybersecurity practices, and greater emphasis on continual improvement and stakeholder expectations. This upgrade ensures that GPSC's information security management system remains resilient, relevant, and aligned with evolving global security challenges and regulatory requirements.

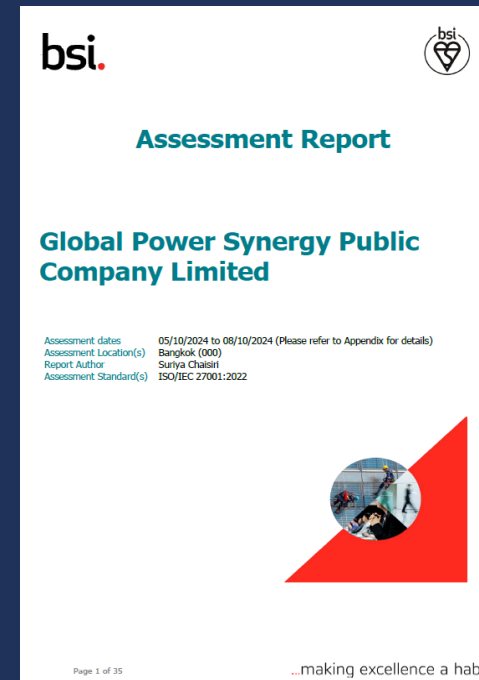
Assessor: BSI Group

Assessment date: 05 Oct 2024 to 08 Oct 2024

Certificate date: 15 Nov 2024 to 14 Nov 2027

Result:

The organization has demonstrated a strong commitment to enhancing the effectiveness of its management system. Evidence shows that the system has been properly implemented and operated to achieve its intended outcomes. The management team has actively ensured compliance with internal policies, customer expectations, legal obligations, and other relevant requirements, while also fostering a culture of continual improvement. Furthermore, the organization has successfully completed the transition from ISO/IEC 27001:2013 to ISO/IEC 27001:2022, reflecting its proactive approach to aligning with updated international standards.

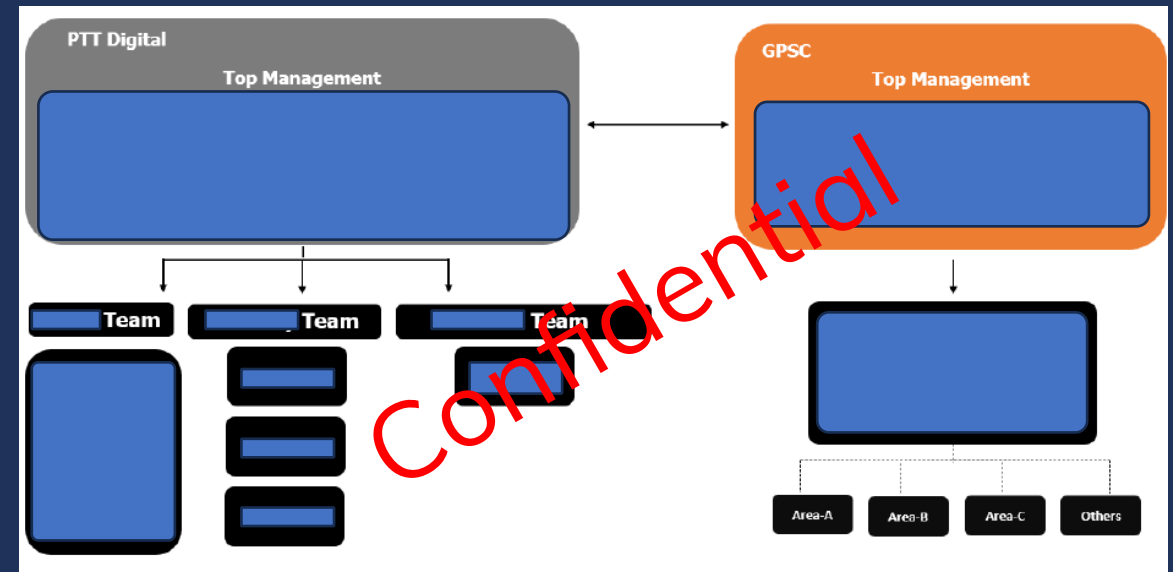
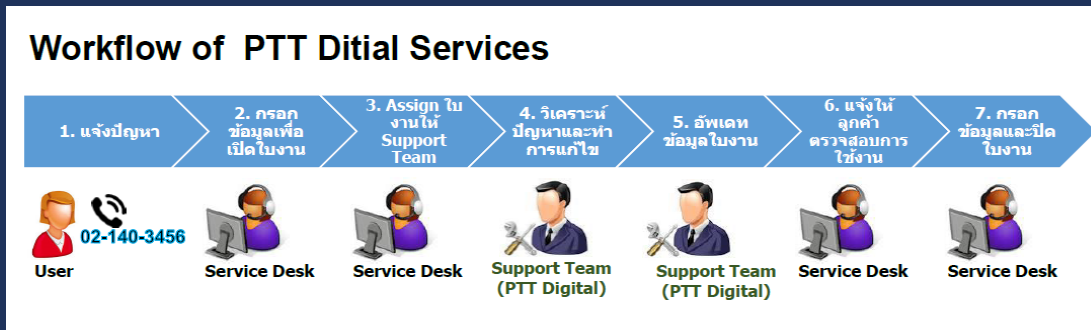
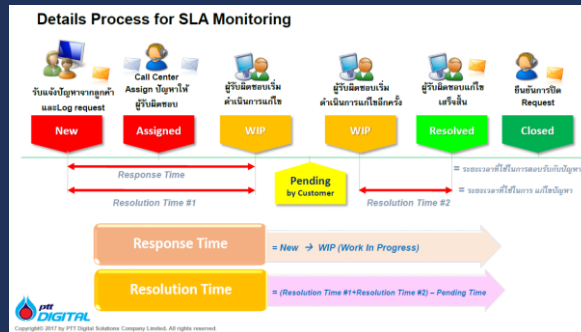


Escalation process for employees to report incidents, vulnerabilities or suspicious activities

Escalation process for employees to report incidents, vulnerabilities or suspicious activities (1/3)

GPSC, as a PTT flagship company, uses the process of service level agreement (SLA) monitoring and workflow as a clear escalation process of manage information and cybersecurity event/ incident of PTT digital services as well as PTT Digital Service Request Channel for resolving the customers' IT Problems. The workflow is managed by PTT Digital who is the operator of GPSC major IT infrastructure. The process enables GPSC Group's employees can follow on suspicious activities through hotline or service desk.

In addition to escalation process from PTT digital, GPSC has the work instruction of both Operation Technology (OT) and Information Technology (IT) in place for all employees in the organization. The instructions encompass role, responsibility, and workflow between GPSC and PTT Digital team.



Escalation process for employees to report incidents, vulnerabilities or suspicious activities (2/3)

Specifically, regarding the employee escalation process, GPSC has implemented an internal Incident Management Procedure applicable organization-wide. This procedure is designed to establish a documented structure that defines the rules and standards for managing incidents effectively. It clarifies the roles and responsibilities of employees involved in incident response, promoting transparency and accountability throughout the process. The procedure outlines the methods and best practices to ensure incidents are addressed efficiently and in line with organizational policies. It also incorporates robust internal controls and approval mechanisms throughout the incident management cycle.

Incident management procedure as part of escalation process for employees



Global Power Synergy Public Company Limited

ระเบียบปฏิบัติ

Procedure

ข้อมูลเอกสารฉบับล่าสุด

หมายเลขเอกสาร	PDV-P-0020	สายงาน	PSE	ฝ่าย/ส่วน	PDV
ชื่อเอกสาร	ขั้นตอนการบริหารจัดการเหตุการณ์ระบบสารสนเทศ (Incident management procedure)			สถานะ	
การแก้ไข	02	วันที่ประกาศใช้	15 ต.ค. 2567	จำนวนหน้า	16

Escalation process for employees to report incidents, vulnerabilities or suspicious activities (3/3)

Additionally, the escalation process use the priority level table to identifies the relative importance of an Incident. Incident priority is based on the combined Impact and Urgency assignments, and is used to identify the required action times. Leading to action to be activated that complies with the stepwise instruction to guide employees in executing the process correctly. Overall, this procedure ensures that incident management efforts align with business objectives and serve the best interests of the organization.

Example of priority level table

Incident Priority		4 - Urgent	3- High	2 - Medium	1 - Low
Incident Priority		Impact			
		Low (1)	Medium (2)	High (3)	
Urgency	High (3)	Medium	High	Urgent	
	Medium (2)	Low	Medium	High	
	Low (1)	Low	Low	High	

Example of Escalation process for employees to report incidents, vulnerabilities or suspicious activities

6.3 [P1] Incident Management Process

Procedure Description. In this section, the above process workflow is detailed in a more explanatory procedure description table format.

Reporter	Inform/Notify Event/System Alarm/Complaint	Inform or notify events, system alarms, or complaints to IT Service Desk through various means, i.e., phone, email, Microsoft Teams, or Service Desk Platform. Some events or system alarms are early detected by Digital Platform Analyst themselves.
----------	--	--

Information security awareness training

Information security awareness training (1/3)

GPSC has organized training courses on information security and cybersecurity awareness, including compliance with the company's Information and Communication Technology Policy Standard Practice, covering areas such as computer and software usage, internet access, email communication, and computer virus protection. These trainings are provided to employees at all levels, including new hires, through online platforms such as e-Learning and orientation sessions. The objective is to raise awareness of cyber threats and ensure understanding of the policies and regulations governing the use of information technology systems, which all employees must strictly follow as part of their performance evaluation. In addition to the existing curriculum, the training has been enhanced with new modules covering emerging cybersecurity topics such as ransomware attacks, the rise of cybersecurity AI, potential cybersecurity incidents projected for 2030, AI-based predictive social engineering, zero trust architecture, the role and function of Computer Emergency Response Teams (CERT), and cybersecurity incident preparedness. These additions aim to equip employees with up-to-date knowledge and readiness to respond to evolving cyber threats.

Information security awareness training (2/3)

AI Data Security Awareness

ระวังภัย! AI สรุปลงานฟรี... หรือกับดักลวงความลับ?

**รูปแบบลวดลายและจุดสังเกต
(The Trap & Red Flags)**

รูปแบบการล่อลวงเบื้องต้น



ต้องระวังการสรุปเอกสารฟรีเพื่อแลกกับข้อมูลส่วนตัวขององค์กรหรือข้อมูลส่วนตัว

**สัญญาณอันตราย
(Red Flags)**



ขอสิทธิ์เข้าถึงข้อมูล
ที่เกินความจำเป็น



ขอข้อมูล
ที่ไม่เกี่ยวข้อง



**แนวทางปฏิบัติเพื่อความปลอดภัย
(Call to Action)**

สิ่งที่ต้องถามเมื่อเจอรอย



หยุดการให้
ข้อมูลทันที



ตรวจสอบ
ความน่าเชื่อถือ
ของเว็บไซต์



แจ้ง
หน่วยงาน
ที่เกี่ยวข้อง

ป้องกันข้อมูลรั่วไหล



หลีกเลี่ยงการให้ข้อมูลแก่ผู้ขอข้อมูลความลับ
บริษัทโดยไม่คำนึงถึง AI ที่ไม่ผ่านการรับรอง

Security Patch Management Communication

WINDOWS SECURITY

UPDATE!

ประกาศเตือน

กุกาพาร์ 2568

สื่อความหมาย Update Security Patch

ให้กับเครื่องคอมพิวเตอร์ในองค์กร

เพื่อเพิ่มประสิทธิภาพของระบบ และความปลอดภัยมากขึ้น

เพื่อความปลอดภัยในการใช้งานคอมพิวเตอร์ จากภัยคุกคามทางไซเบอร์ (Cybersecurity) คณะกรรมการผู้จัดซื้อสื่ออิเล็กทรอนิกส์ (PDA) จัดให้มีการปรับปรุงความปลอดภัยของเครื่องคอมพิวเตอร์ของวิทยาลัยอาชีวศึกษา ในวันพฤหัสบดีที่ 6 กุมภาพันธ์ 2568 ตั้งแต่เวลา 19:00 น. เป็นต้นไป ซึ่งจะออก Update

ปรับปรุงระบบให้ดีขึ้น

เพื่อป้องกันไวรัส
และภัยคุกคาม
ภายนอก

สิ่งที่เกิดขึ้นเมื่อเครื่องได้รับ Windows Security Update

1. เมื่อได้รับแจ้งเตือนว่าเครื่องมีอัปเดตที่จะถูกดาวน์โหลดและติดตั้ง ให้คลิกที่ปุ่ม Menu Windows -> Power แล้วเลือก update และ shutdown หรือ update and restart เพื่อให้ระบบดำเนินการติดตั้งอัปเดต
2. เมื่อ Update สำเร็จแล้ว สามารถ Update 100% หรืออาจมีการแจ้งเตือนว่าอัปเดตไม่สำเร็จ

***ห้ามดับเครื่องขณะที่กำลัง update ไม่สำเร็จ

Working on updates 30% complete

Don't turn off your PC. This will take a while.

ตอนจบมีข้อมูลเพิ่มเติมที่ PTT Digital Contact Center 3456 หรือ 02-140-3456

Industry Technology Awareness




การประยุกต์ใช้ **IoT** (อินเทอร์เน็ตของสรรพสิ่ง) ในอุตสาหกรรมพลังงาน

(Internet of Things: IoT) คือ เครือข่ายของอุปกรณ์เชื่อมต่อที่สามารถสื่อสารกันเอง และเก็บรวบรวมข้อมูล อุปกรณ์ที่เชื่อมต่อด้วยอินเทอร์เน็ตสามารถรับส่งและประมวลผลข้อมูลจากอุปกรณ์ร่วมกันและสามารถเพิ่มประสิทธิภาพได้

ข้อดีของ IoT สำหรับอุตสาหกรรมพลังงาน

UPGRADE

↑

ประสิทธิภาพมากขึ้น
ช่วยเพิ่มประสิทธิภาพ
การการผลิตมากขึ้น
ในอุตสาหกรรมพลังงาน

✓

ปลอดภัยมากขึ้น
ลดข้อผิดพลาด
ของมนุษย์ทำให้
มีความปลอดภัยมากขึ้น

⚡

ใช้พลังงานน้อยลง
มีการวางแผนการผลิต
ได้แม่นยำมากขึ้น
ลดการสิ้นเปลืองพลังงาน

🛡️

ค่าใช้จ่ายน้อยลง
ลดแรงจูงใจมนุษย์ได้
เนื่องจากเครื่องจักร
มีประสิทธิภาพมากขึ้น



6 วิธีการนำ IoT มาใช้ในอุตสาหกรรมพลังงาน



- 1

Smart asset monitoring improves grid reliability:
เทคโนโลยี IoT สามารถตรวจสอบสถานะของระบบได้อย่างมีประสิทธิภาพทุกอุปกรณ์
ตรวจสอบและแจ้งเตือนล่วงหน้าถึงระบบที่ผิดปกติได้ทันที
- 2

Helps prevent breaches
ระบบ IoT ช่วยตรวจสอบการตรวจพบปัญหาต่างๆที่อาจเกิดขึ้นก่อนเกิดเหตุได้จริง
ดังนั้นจึงสามารถดำเนินการป้องกันก่อนที่จะถึงจุดที่การโจมตีอาจสร้างความเสียหายต่อข้อมูล
- 3

Facilitates regulatory compliance:
การตรวจสอบ IoT รวมการแจ้งเตือนล่วงหน้าเพื่อช่วยในการตรวจสอบ * ปฏิบัติตามกฎระเบียบ
ด้านสิ่งแวดล้อมและประสิทธิภาพได้ดียิ่งขึ้น ด้วยการแจ้งเตือนล่วงหน้าให้สามารถควบคุม
สิ่งต่าง ๆ ตามความจำเป็นเฉพาะกิจ
- 4

Enables advanced energy management:
เมื่อทำงานร่วมกับ AI like: Machine Learning ระบบ IoT สามารถตรวจสอบ
การวางแผนใช้พลังงานรวมกับข้อมูลการดำเนินงานเพื่อการตัดสินใจ
- 5

Automation to the next level
ด้วยระบบ IoT บริษัทสามารถยกระดับระบบ Automation ได้ดียิ่งขึ้น
- 6

Clean energy economics:
นำเทคโนโลยีมาประยุกต์ใช้ในโรงไฟฟ้าใช้พลังงานทดแทน การแปลงพลังงานแสงอาทิตย์
ระหว่างเครื่องใช้เพื่อการผลิตพลังงานแบบ Micro-grid ผลักดันการนำ IoT like Blockchain
เพื่อเปิดตลาดซื้อขายพลังงานแบบ peer-to-peer

ที่มา : Maelgoging, Duke Energy, Chevron



Shell สามารถลดต้นทุนด้านการดำเนินงานแบบบูรณาการ ในปี 2017 จากกรณี IoT มาใช้ในโรงงานของ
แท่นผลิตปิโตรเลียมที่ดำเนินการผลิตปิโตรเลียมและปิโตรเคมีที่สามารถปรับปรุงกระบวนการผลิตปิโตรเลียมและปิโตรเคมี

PdV-Cybersecurity ฉบับ 003-068

หน่วยงานที่จัดทำ/แก้ไข/เผยแพร่เอกสารฉบับนี้

Data Classification Awareness

[illegible]

Cybersecurity Trend Awareness




GPSC

ACT*SPIRIT

The energy we create together

แนวโน้มเทคโนโลยีสำคัญ ในอุตสาหกรรมพลังงาน 2025

อุตสาหกรรมพลังงานกำลังเผชิญการเปลี่ยนแปลงจากนโยบายความยั่งยืนทั่วโลก ทำให้อุตสาหกรรมต้องปรับตัวเพื่อรับมือกับการจัดการข้อมูลสื่งเพิ่มขึ้นอย่างมหาศาล รวมถึงรักษาความปลอดภัยของโครงสร้างพื้นฐานสำคัญจากภัยคุกคามทางไซเบอร์ ที่คาดว่าจะทวีความรุนแรงในปี 2025.



5 แนวโน้มหลักของเทคโนโลยีในอุตสาหกรรมพลังงานปี 2025

- 1

AI and Machine Learning for Safety

 - ใช้งาน AI และ Machine Learning ในการเพิ่มประสิทธิภาพด้านความปลอดภัยที่ประสิทธิภาพ
- 2

Digital Twins for Asset Uptime

 - ขยายการใช้งาน Digital Twins ในทุกขั้นตอนการดำเนินงาน
 - เชื่อมโยงข้อมูลดิจิทัลและแบบจำลองเสมือน เพื่อเพิ่มความน่าเชื่อถือ
- 3

Predictive Maintenance and Supply Chains

 - สนับสนุนการแลกเปลี่ยนข้อมูล IoT ระหว่างผู้ให้บริการและบริษัทพลังงาน
 - ขับเคลื่อนห่วงโซ่อุปทานด้วยระบบแบบดิจิทัลที่เชื่อมโยงกัน
- 4

Improved Customer Experiences

 - เพิ่มประสบการณ์ของผู้บริโภคที่ลงทุน ในบริการสาธารณะทุกด้านพลังงานที่หลากหลายภายใต้การบูรณาการดิจิทัลที่ดียิ่งขึ้น
- 5

Strengthened Cybersecurity

 - ลดความเสี่ยงด้านความปลอดภัยไซเบอร์แบบโครงสร้างพื้นฐานพลังงาน
 - AI จะมีส่วนในการป้องกันความเสี่ยงจากการโจมตีทางไซเบอร์มากขึ้นในอนาคต

ตัวอย่างการดำเนินงานที่สำคัญในอุตสาหกรรมพลังงาน





บริษัทพลังงานสเปนได้ดำเนินการได้กำหนดแผนธุรกิจปี 2024 – 2026 ในการลงทุนด้าน AI โดยได้ขยายระบบโครงสร้างพื้นฐานด้านไอทีไปยังตลาดอย่างสมบูรณ์ ในปีนี้ 2024 ได้ดำเนินการจัดทำโปรแกรม Copilot ด้วย AI ช่วยในการส่งตรวจวิเคราะห์และเอกสารเชิงตัวเลขที่จองกรัง

Siemens ได้สร้างผลิตภัณฑ์ใหม่ทาง AI สำหรับระบบควบคุมแบบกระจายพลังงานไฮโดรเจน Simatic PCS neo: SFC Generation โดยในอุตสาหกรรมก๊าซ AI เชิงสร้างสรรค์ ซึ่งคาดว่าจะวางจำหน่ายบริการดังกล่าวในปี 2025

ที่มา : openText, Enel, Siemens

PDV-Cybersecurity ฉบับ 01/68

รับชมได้ที่เว็บไซต์และแพลตฟอร์ม

Information security awareness training (3/3)

Phishing Simulation Debrief

Phishing Prevention Guideline

ผลการทดสอบ Phishing Mail
เมื่อวันที่ 25 - 29 พ.ค. 2569

ในหัวข้อ "Gemini Free Month"
จึงขอทำการเฉลยจุดสังเกตต่อไปนี้

จุดที่ 1 ตรวจสอบผู้ส่งที่ใช้ในอีเมลในองค์กรหรือไม่
หรือใช้ชื่อที่คล้ายคลึงกับองค์กรของคุณ

จุดที่ 2 คุณได้รับข้อความที่ผิดปกติหรือไม่
หรือการกระทำที่ไม่น่าเชื่อถือหรือไม่

จุดที่ 3 สันดา URL ของเว็บไซต์ที่คุณคลิกหรือไม่
เป็นเว็บไซต์ที่เชื่อถือได้หรือไม่

จุดที่ 4 "เรียนรู้ และตระหนัก เพื่อป้องกัน Phishing Mail"
เพราะคุณคือส่วนหนึ่งขององค์กร...

โปรดจำ! ข้อสังเกตเหล่านี้

- ตรวจสอบผู้ส่ง
- พิจารณาที่อยู่ไฟล์หรือลิงก์
- มีเนื้อหาที่ดูน่าสงสัยหรือไม่

พร้อมกันนี้ ทีมงานจะขอแจ้งให้ทราบถึงผลการทดสอบ Phishing Mail
Email: servicedesk@pttdigital.com | โทร: 02-140-3456

ผลการทดสอบ Phishing Mail
เมื่อวันที่ 30 มิ.ย. 4 ก.ค. 2568

ในหัวข้อ "สิทธิพิเศษสำหรับพนักงาน GPSC"
จึงขอทำการเฉลยจุดสังเกตต่อไปนี้

จุดที่ 1 ตรวจสอบผู้ส่งที่ใช้ในอีเมลในองค์กรหรือไม่
หรือใช้ชื่อที่คล้ายคลึงกับองค์กรของคุณ

จุดที่ 2 คุณได้รับข้อความที่ผิดปกติหรือไม่
หรือการกระทำที่ไม่น่าเชื่อถือหรือไม่

จุดที่ 3 สันดา URL ของเว็บไซต์ที่คุณคลิกหรือไม่
เป็นเว็บไซต์ที่เชื่อถือได้หรือไม่

จุดที่ 4 "เรียนรู้ และตระหนัก เพื่อป้องกัน Phishing Mail"
เพราะคุณคือส่วนหนึ่งขององค์กร...

โปรดจำ! ข้อสังเกตเหล่านี้

- ตรวจสอบผู้ส่ง
- พิจารณาที่อยู่ไฟล์หรือลิงก์
- มีเนื้อหาที่ดูน่าสงสัยหรือไม่

พร้อมกันนี้ ทีมงานจะขอแจ้งให้ทราบถึงผลการทดสอบ Phishing Mail
Email: servicedesk@pttdigital.com | โทร: 02-140-3456

ผลการทดสอบ Phishing Mail
เมื่อวันที่ 13 - 16 พ.ย. 2568

ในหัวข้อ "COMPLETED: PDF DOCUMENT RECEIVED"
จึงขอทำการเฉลยจุดสังเกตต่อไปนี้

จุดที่ 1 ตรวจสอบผู้ส่งที่ใช้ในอีเมลในองค์กรหรือไม่
หรือใช้ชื่อที่คล้ายคลึงกับองค์กรของคุณ

จุดที่ 2 คุณได้รับข้อความที่ผิดปกติหรือไม่
หรือการกระทำที่ไม่น่าเชื่อถือหรือไม่

จุดที่ 3 สันดา URL ของเว็บไซต์ที่คุณคลิกหรือไม่
เป็นเว็บไซต์ที่เชื่อถือได้หรือไม่

จุดที่ 4 "เรียนรู้ และตระหนัก เพื่อป้องกัน Phishing Mail"
เพราะคุณคือส่วนหนึ่งขององค์กร...

โปรดจำ! ข้อสังเกตเหล่านี้

- ตรวจสอบผู้ส่ง
- พิจารณาที่อยู่ไฟล์หรือลิงก์
- มีเนื้อหาที่ดูน่าสงสัยหรือไม่

พร้อมกันนี้ ทีมงานจะขอแจ้งให้ทราบถึงผลการทดสอบ Phishing Mail
Email: servicedesk@pttdigital.com | โทร: 02-140-3456

แนวทางป้องกัน Phishing Email

การป้องกัน Phishing Email เป็นการตรวจสอบผู้ส่งและลิงก์ที่แนบมา
อย่าเปิดไฟล์แนบหรือคลิกลิงก์ที่ไม่แน่ใจ เพราะมันอาจเป็นอันตราย
พร้อมเปิดใช้งานยืนยันตัวตนสองขั้นตอน (2FA)

แนวทางการป้องกัน Phishing Email

1. ผู้รับก่อนตอบเป็นเหตุ
- ตรวจสอบผู้ส่งที่ใช้ในอีเมลในองค์กรหรือไม่
- ตรวจสอบผู้ส่งที่ใช้ในอีเมลในองค์กรหรือไม่
- ตรวจสอบผู้ส่งที่ใช้ในอีเมลในองค์กรหรือไม่
2. อย่าคลิกลิงก์หรือไฟล์แนบโดยไม่ตรวจสอบ
- ตรวจสอบผู้ส่งที่ใช้ในอีเมลในองค์กรหรือไม่
- ตรวจสอบผู้ส่งที่ใช้ในอีเมลในองค์กรหรือไม่
3. เปิดใช้การยืนยันตัวตนแบบ 2 ขั้นตอน (2FA/MFA)
- ตรวจสอบผู้ส่งที่ใช้ในอีเมลในองค์กรหรือไม่
- ตรวจสอบผู้ส่งที่ใช้ในอีเมลในองค์กรหรือไม่
4. ใช้ระบบกรองอีเมลและซอฟต์แวร์รักษาความปลอดภัย
- ตรวจสอบผู้ส่งที่ใช้ในอีเมลในองค์กรหรือไม่
- ตรวจสอบผู้ส่งที่ใช้ในอีเมลในองค์กรหรือไม่
5. อบรมพนักงานให้รู้เท่าทัน
- ตรวจสอบผู้ส่งที่ใช้ในอีเมลในองค์กรหรือไม่
- ตรวจสอบผู้ส่งที่ใช้ในอีเมลในองค์กรหรือไม่
6. มีแผนรับมือเมื่อเกิดเหตุ
- ตรวจสอบผู้ส่งที่ใช้ในอีเมลในองค์กรหรือไม่
- ตรวจสอบผู้ส่งที่ใช้ในอีเมลในองค์กรหรือไม่

จำไว้เสมอ: Phishing ไม่ได้นับที่แค่เมล - แต่อาจเป็นจุดเริ่มต้นของภัยคุกคามทั้งหมด

Report Phishing

การแก้ปัญหาเมื่อโดน Phishing Email โจมตี

การแก้ปัญหาเมื่อโดน Phishing Email โจมตี

- STEP 1: หยุดทันที
- หยุดการคลิกหรือดาวน์โหลดไฟล์แนบ
- ดึงการเชื่อมต่ออินเทอร์เน็ต
- STEP 2: เปลี่ยนรหัสผ่านทุกบัญชี
- เปลี่ยนรหัสผ่าน
- เปลี่ยนรหัสผ่าน
- STEP 3: เปิดใช้ 2FA / MFA
- เปิดใช้งานการยืนยันตัวตนด้วย OTP / Authenticator
- ติดตั้งแอปพลิเคชัน
- STEP 4: แจ้งฝ่าย IT / ผู้ดูแลระบบ
- แจ้งฝ่าย IT / ผู้ดูแลระบบ
- แจ้งฝ่าย IT / ผู้ดูแลระบบ
- STEP 5: รายงานเหตุการณ์
- รายงานเหตุการณ์
- รายงานเหตุการณ์
- STEP 6: ตรวจสอบข้อมูลอุปกรณ์
- ตรวจสอบข้อมูลอุปกรณ์
- ตรวจสอบข้อมูลอุปกรณ์
- STEP 7: แจ้งเตือนเพื่อนร่วมงาน
- แจ้งเตือนเพื่อนร่วมงาน
- แจ้งเตือนเพื่อนร่วมงาน
- STEP 8: ปรับปรุงระบบความปลอดภัย
- ปรับปรุงระบบความปลอดภัย
- ปรับปรุงระบบความปลอดภัย

การรู้ทันและตอบสนองต่อภัยคุกคาม

Report Phishing

Thank You

