



EMPOWERING ALL TOWARD
INCLUSIVE GROWTH

OR Information Security Management

2026



Information Security Management Policy



Digital Policy

Digital is powered to operate the OR Group's business in order to improve both the efficiency and the value of business operation significantly which generates mobility, transparency and safety. Moreover, OR concerns with the excellent potential and cooperation in OR Group and supports the sustainable operation of energy business and chemical petroleum entirely in order to increase the opportunity and develop technology innovation which encounter with global challenge dramatically and keep up with globalization.

OR Group's Information Technology Policy

1. Every departments shall follow the Digital Law including company's rules and regulations, digital industry standards and cyber security as the basic.
2. Develop and concentrate on making the highest benefit in business with digital in order to reinforce the competitiveness. Also, search for New S-Curve to produce sustainable growth and response the customer requirements and customer experiences.
3. Develop the efficiency of annual budgeting expense in order to provide satisfied and valuable products and services to consumer, and support business operation continuously as service level agreement (SLA) and standard agreement.
4. Support business operation by digital sustainability management, provide information security and risk management in order to prevent possible damage and loss to company stakeholders. To concern digital threats, control measure and preventive measure shall be determined strictly, and digital emergency backup plan shall be provided also.
5. Support development and procurement of products and services in order to generate digital innovation with quality, safety and digital green.
6. Support digital competency development of employees both digital knowledge and skills which are involved with OR Group's operations.

Digital Policy

7. Encourage the digital synergy of OR Group to modernize with innovation and technology which supported digital transformation by PTT Digital within OR operations.

This policy is applied for every departments in supply chain of OR Group. Chief Executive shall manage direction of the result as close as the goal. Management shall be exemplary by following OR corporate governance, supporting and encouraging the performance seriously. Employee shall understand and follow this policy sequentially.

Policy Owner

Senior Executive Vice President, Digital Business and Solutions Tel. 061-195-1689

OR Group's Digital Policy is designed to leverage technology for improved business operations, focusing on efficiency, value, transparency, mobility, and safety.

Key aspects of their approach include strict adherence to digital laws and cybersecurity, utilizing digital tools for maximum business benefit and competitive advantage, and continuously seeking new avenues for sustainable growth while prioritizing customer needs. They also emphasize efficient budget management for quality products and services, robust information security, risk management, and emergency preparedness to prevent losses.

The policy supports business operations by promoting digital sustainability management, risk management, and information security to prevent damage and loss to company stakeholders, ensuring the integrity and protection of data. Strict controls, preventive measures, and digital emergency backup plans with monitoring and continuous improvement are mandatory to address digital threats.

Furthermore, the policies encourage the improvement and procurement of high-quality, safe, and environmentally friendly digital innovations, alongside enhancing employees' digital knowledge and skills.

This comprehensive strategy promotes digital synergy across the OR Group, driving modernization through technology and innovation with the support of **PTT Digital**, and **applies to all departments within the supply chain to ensure the establishment of information security requirements for all parties related to OR operations, including suppliers. The Chief Executive is responsible for overseeing progress toward goals of protecting information security**, management must lead by example in compliance with OR corporate governance, and all employees are required to understand and follow this policy consistently.

Information Security Management Programs

Remind! กับการสอบ

Cyber Security Awareness

สำหรับพนักงาน OR ประจำปี 2568 และรายงานสถานะจำนวนผู้สอบผ่านแยกตามสายงาน

วัตถุประสงค์ :

เพื่อให้พนักงาน OR มีความตระหนักและรู้เท่าทันภัยคุกคามทาง Cyber Security รวมทั้งสามารถใช้งานสารสนเทศได้อย่างถูกต้อง

กลุ่มเป้าหมาย :

พนักงาน OR ทุกคน

ระยะเวลาการสอบ :

3 เดือน
(1 กรกฎาคม - 30 กันยายน 2568)

หลักเกณฑ์การสอบ :

- เนื้อหาผ่าน Cyber Security เช่น Mobile Using, Phishing E-mail, Password Security, Multi Factor Authentication (MFA) เป็นต้น
- แบบทดสอบ 4 ตัวเลือก ไม่จำกัดเวลาในการทดสอบ
- เกณฑ์การผ่านต้องตอบถูก 15 ข้อ (100%) ไม่จำกัดครั้งในการทดสอบ

หมายเหตุ: จำนวนที่ผ่านเกณฑ์ในแต่ละสายงาน ไม่ได้อัดรวมกันเป็นผลรวมทั้งหมดของพนักงาน

จึงขอความร่วมมือให้พนักงาน OR ทุกท่านเข้าทำการทดสอบ Cyber Security Awareness ประจำปี 2568 นี้

โดยท่านสามารถเข้าสอบได้ที่

คลิกเพื่อเข้าสอบ

QR CODE

สแกนเพื่อเข้าสอบ

OR IMS PLATFORM (IMS.CORP.CO.TH)

กรุณาเข้าสู่ระบบด้วย Username และ Password ที่มอบให้

รายงานสถานะจำนวนผู้สอบผ่านแยกตามสายงาน

ความเสี่ยง จากจุดชาร์จไฟฟรีสาธารณะ

"Juice jacking"

เป็นวิธีการขโมยข้อมูลจากมือถือผ่านพอร์ตชาร์จ USB ในที่สาธารณะที่ผู้ใช้งานเชื่อมต่อและใช้มือถือเพื่อชาร์จแบตเตอรี่

วิธีการป้องกัน Juice jacking

- ผู้ถือมือถือต้องพกพอร์ตชาร์จ USB ที่จุดชาร์จไฟฟรี เช่น ห้างสรรพสินค้า โรงแรม หรือร้านอาหาร
- ผู้ถือมือถือ USB ต้องตรวจสอบอุปกรณ์
- ถ้าได้ปลั๊กชาร์จแล้วอุปกรณ์จะขึ้นหน้าจอแสดงข้อความว่า "เชื่อมต่อ" หรือ "เชื่อมต่อแล้ว" แสดงว่าปลอดภัย
- ห้ามเชื่อมต่ออุปกรณ์กับเครื่องที่ไม่รู้จัก
- ถ้าจำเป็นต้องเชื่อมต่อกับเครื่องที่ไม่รู้จัก ให้ใช้สายชาร์จที่เชื่อถือได้ หรือพกสายชาร์จสำรองไว้

คำแนะนำสำหรับผู้ใช้งานในที่สาธารณะให้ปลอดภัย

- สายชาร์จแบบหัวต่อแบบถอดออกได้
- พก Power Bank ส่วนตัว เพื่อชาร์จแบตเตอรี่ฉุกเฉิน
- ใช้ USB Data Blocker หรือสายสำหรับชาร์จไฟเท่านั้น โดยที่ไม่มีสายอื่นต่อ

ข้อมูลเผยแพร่โดย : ทีมงานด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ (สารสนเทศ) บริษัท ปตท. จำกัด (มหาชน) จัดทำ (เผยแพร่)

Digital Security Awareness Program | SecurityAwareness@pttdigital.com

Information Security/Cybersecurity Awareness Training

To raise awareness of personal data protection and data security and strengthen knowledge of cybersecurity within the company, OR has organized training programs for employees. These programs include courses on cybersecurity and personal data protection to ensure employees gain a thorough understanding of data protection and are adequately prepared to address cyber threats. These training programs aim to enable OR to transition effectively into a Digital-Driven Organization. Moreover, OR have conducted information/cyber security awareness refreshment program for employee who had previously undergone training and organized 2 times in 2025.

- OR employee pass an exam 98.5%
- Contractor pass an exam 100%

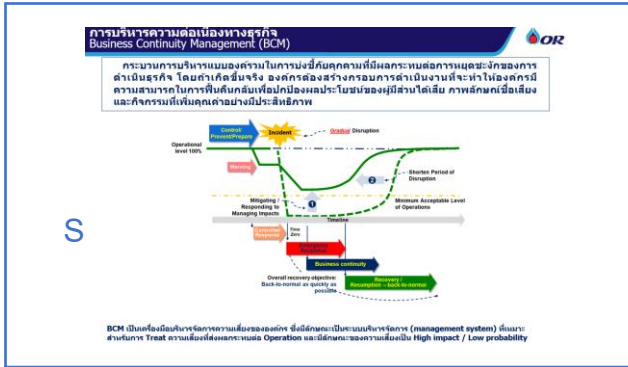
Key Performance: OR & Contractor employee pass the Phishing Drill Test exercise by resiliency rate 17.74%

Source: OR's Data Privacy and Security Website:

<https://www.pttor.com/en/sustainability/governance-and-economic-dimension/data-security-and-privacy>

Escalation process for reporting IT/cyber incident or event

A clear escalation process is outlined in the OR Cyber Security Incident and Response document, which provides detailed procedures and guidelines in the event of a cyberattack, enforcing by the OR's Digital Solutions Department of OR, with the goal of resolving and restoring the situation to normal as quickly as possible. Employees are also provided with a clear reporting process to follow if they notice any suspicious activity, which involves promptly notifying the department.



PTT Digital Solutions
ศูนย์จัดการความเสี่ยงทางดิจิทัลของ PTT
เพื่อรองรับความต่อเนื่องทางธุรกิจของ PTT จำกัด (มหาชน)
ประจำปี 2568

โครงสร้างศูนย์บริหารจัดการภาวะวิกฤติและความต่อเนื่องทางธุรกิจ
Crisis and Business Continuity Management Center (CMC&BCM)

- Confidential -

Information Security/Cyber Security business continuity/ contingency plans and incident response procedures

Business Continuity Management (BCM) is a critical framework that enables organizations to prepare for, respond to, and recover from disruptive incidents that could affect operations. OR has implemented proactive planning and preparedness measures to ensure the continuity or rapid resumption of critical business functions in the event of a disruption. This includes a comprehensive **Crisis and Business Continuity Management Plan, with a specific focus on network security and the protection of IT assets.**

The plan clearly defines the roles and responsibilities of all relevant departments and personnel. It includes detailed, scenario-specific procedures designed to address various incidents, such as:

- Cyber attack
- IT System Failure

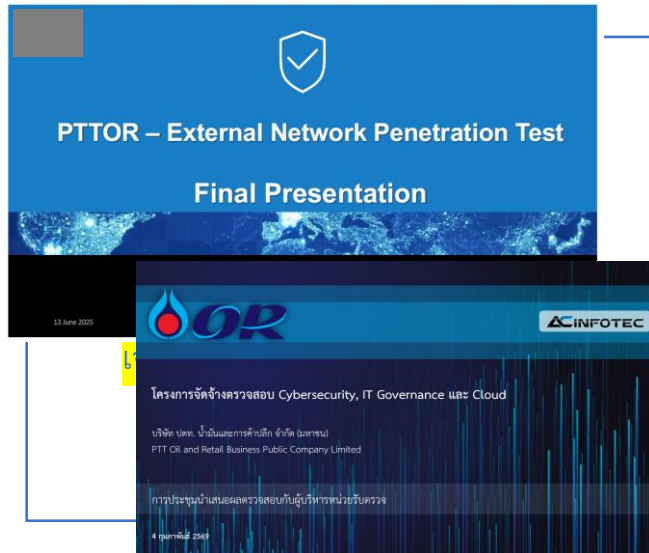
Each designated individual is responsible for promptly notifying relevant parties, including the executive team and other key stakeholders.

To validate and enhance preparedness, OR conducts incident response testing on a semi-annual basis.

Key programs include:

- Disaster Recovery (DR) Testing was tested 2 times in 2025
- Cyber Drill Tabletop Exercises was tested 1 times in 2025
- System Preventive Maintenance was tested 2 times in 2025

In addition, OR has conducted Black Swan event preparedness, focusing on scenarios such as Cyber Attacks failures in digital infrastructure in 2024.



Information Security Vulnerability Analysis with both internal and external audit

OR has a strong compliance for infrastructure and information security management systems, which are regularly audited both internally and externally. To internally mitigate risks and minimize potential impacts from system changes, OR has established a Change Advisory Board (OR CAB) to oversee and guide all system modifications. Additionally, vulnerability assessments are conducted and audited by certified third-party organizations such as PwC, EY, PTT PLC., MASCI, and ACinfotec Co. ensuring a high level of security and accountability.

The analysis included simulated hacker attacks.

- OR collaborated with partner to conduct a simulated hacker attack, Red Team exercise, penetration testing, and vulnerability assessment, with proper mitigation and permanent fixes for system vulnerabilities.

Key Performance: In 2025, the internal audit was conducted 1 times and external audit was conducted 1 times.



ISO27001 Certification

OR's IT infrastructure and information security management system is 100% certified to ISO 27001 by;

- PTT DIGITAL (Network-Infrastructure & Private Cloud)
- Awn (Advanced Wireless Network Company Limited) (Network-Infrastructure & Cloud Landing Zone)

	2022	2023	2024	2025
Total number of information security breaches or other cybersecurity incidents	0	0	0	1
Total amount of fines/ penalties paid in relation to information security breaches or other cybersecurity incident.	0	0	0	0

Data source: [OR Performance summary Economic](#), Topic IT Security/ Cybersecurity Breaches PDF p1.
Our data is verified by third-party, please see GRI 418-1 Substantiated complaints concerning breaches of customer privacy and losses of customer data (2016): <https://investor.pttor.com/en/document/viewer/187686/56-1-one-report-2025-publish-date-march-9-2026>



**EMPOWERING ALL TOWARD
INCLUSIVE GROWTH**

OR เติมเต็มโอกาส เพื่อทุกการเติบโต ร่วมกัน

*Harnessing OR
competencies to support,
fulfill, and elevate*

*Sustainable growth
with Living Community,
Healthy Environment, and
Economic Prosperity*

*Moving forward with
strong determination and
leaving no one behind*

*6 groups of
OR stakeholders*