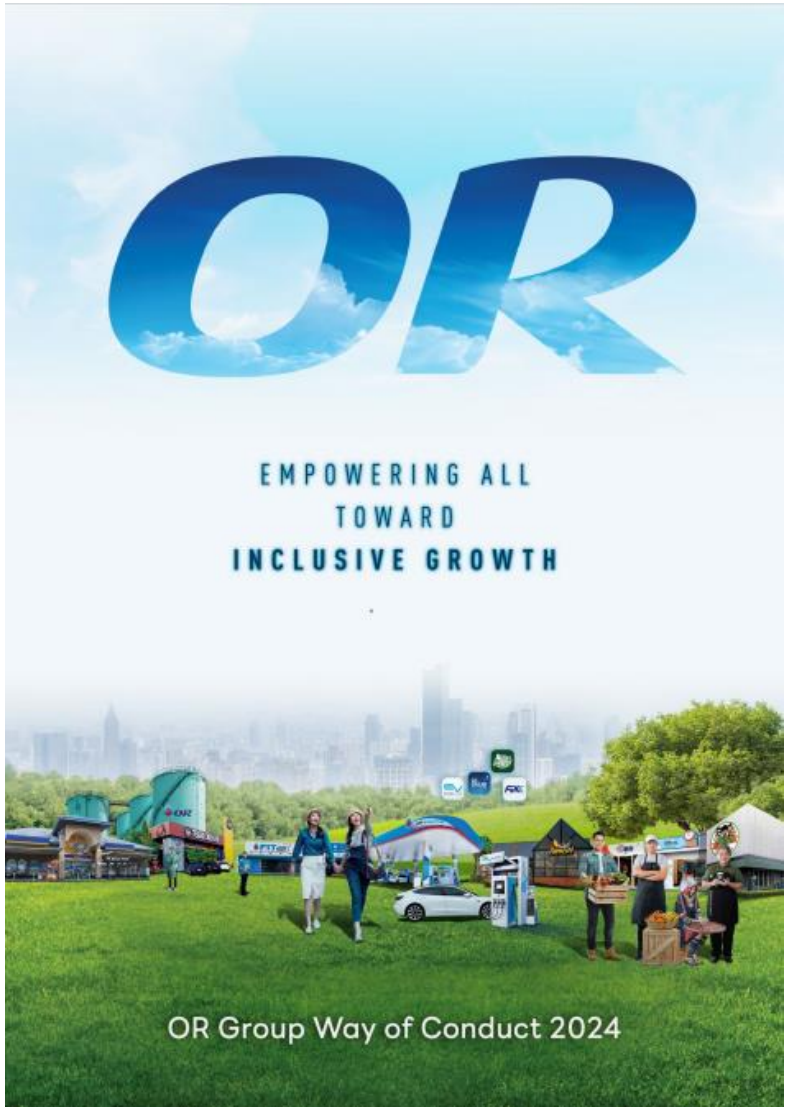
EMPOWERING ALL TOWARD
INCLUSIVE GROWTH

OR Information Security Management

2025

Information Security Management Policy

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

75

Digital Policy

8. 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

Digital Innovation for Business Department Tel. 089-8555369

76

OR's Information Security/Cybersecurity Policy is part of OR Group Way of Conduct 2024 available at : https://www.pttor.com/wp-content/uploads/2024/10/20240607_162817_0090.pdf, PDF Page 79-80

Information Security/Cybersecurity Policy - Overview

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

Information Security/Cybersecurity Awareness Training and Escalation Process

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 trainning and organized 2 times in 2024.

- OR employee pass an exam 99%
- Contractor pass an exam 100%

Key Performance: OR & Contractor employee pass the Phishing Drill Test exercise by resiliency rate 8.76%

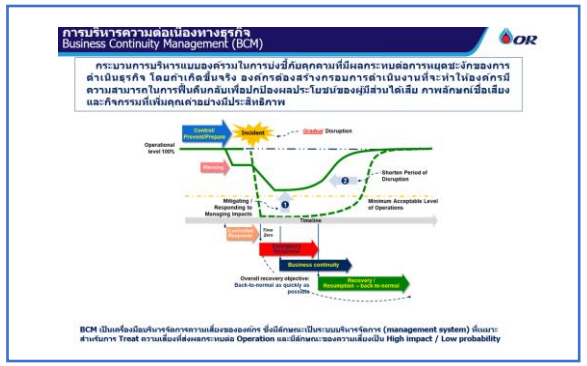
Source: OR's Data Privacy and Security Website:
https://www.pttor.com/en/sustainability/governance-and-economic-dimension/data-security-and-privacy

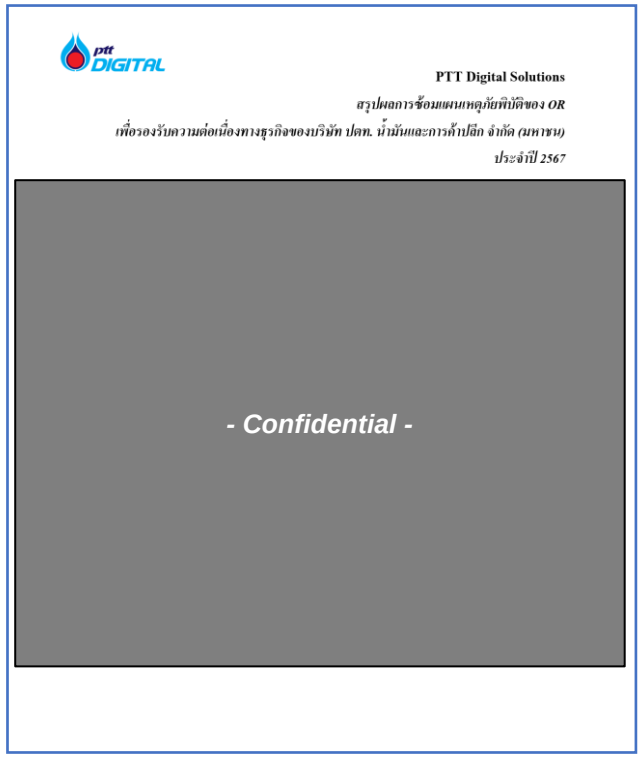
Escalation process for reporting IT/cyber incident or event

A clear escalation process is outlined in the OR Cyber Security Incident Response document, which provides detailed procedures and guidelines for responding to cyberattacks. This document serves as a comprehensive guideline for OR's cybersecurity team, with the primary objective of resolving incidents and restoring IT systems to normal operations as quickly as possible.

Employees are provided with a straightforward reporting process to follow when they observe suspicious activities by notify to PTT Digital Service Desk via Email or Phone. Additionally, employees can report suspected phishing emails by clicking the "Report Phishing" button, after which the IT Security Team will verify and handle the incidents before providing feedback to the reporting employees.

Information security-related business continuity plans and Incident Response Procedure





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

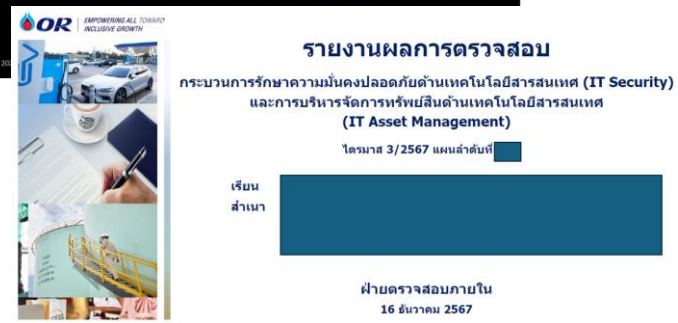
Each designated individual is responsible for promptly notifying relevant parties, including the executive team and other key stakeholders.

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 2024
- Cyber Drill Tabletop Exercises was tested 1 times in 2024
- System Preventive Maintenance was tested 2 times in 2024

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



Information Security Vulnerability Analysis with both internal and external audit

Our IT infrastructure and information security management systems have been audited both internally and externally. Vulnerability analysis was conducted by certified third party.

- OR has strong Compliance for Information Security Management.
- This has been audited by external audits such as PwC, EY, PTT PLC. and MASCI.
- OR with certified third party conduct comprehensive annual security assessments, including simulated cyberattacks, Red Team exercises, penetration testing, and vulnerability assessments. All identified vulnerabilities are properly mitigated and permanent fixes implemented on an ongoing basis.
- Also, OR has OR CAB (Change Advisory Board) to steer System Change to reduce risk and impact.

Key Performance: In 2024, the internal audit was conducted 1 times and external audit was conducted 1 times.

ISO27001 Certification

OR's IT infrastructure and information security management systems adhere to ISO 27001 standards through the utilization of third-party services :

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

Total number of breaches

	2021	2022	2023	2024
Total number of information security breaches or other cybersecurity incidents	0	0	0	0
Total number of data breaches	0	0	0	0
Total number of clients, customers and employees affected by the breaches	0	0	0	0
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://www.pttor.com/wp-content/uploads/2025/04/PTTOR-Assurance-Report_EN-FY2024.pdf

Moving forward with strong determination and leaving no one behind

6 groups of OR stakeholders

***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