



INFORMATION SECURITY POLICY

GUIDELINES

Revision 00

<u>Tanggal Terbit</u> <i>Issuance Date</i>	September 1 st , 2024
<u>Berlaku Efektif</u> <i>Effective Date</i>	October 1 st , 2024
<u>Departemen Penanggung Jawab</u> Responsible Department	Information Technology Department

Approved by	Reviewed by,	Acknowledge by,	Prepared by,
			
Atsushi Aoki President Director	Takuro Shinoda GM FA IT Manager	Widy Indrayanto Deputy GM FA IT	Dolly Indra IT Manager

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) POLICY

1. PURPOSE

The purpose of this Information Security Management System (ISMS) Policy is to establish a structured framework for managing the security of information assets within PT Niterra Mobility Indonesia.

The policy aims to safeguard the confidentiality, integrity, and availability of information, ensuring compliance with legal, regulatory, and contractual obligations while supporting the company's strategic objectives.

The Information Security Policy serves multiple purposes, there are:

- To set out the managing information security as part of effective corporate activities.
- To provide guidance to users, administrators and developers of information systems on appropriate behaviors and controls required to maintain the integrity of information
- To provide a comprehensive approach to information security across the employees.
- To set out how information policies are scrutinized, approved, revised, communicated and monitored.

2. SCOPE

This policy applies to all employees, contractors, third-party service providers, and any individual or entity with access to PT Niterra Mobility Indonesia's information assets.

It covers all information systems, networks, data storage, communication systems, and facilities used for processing, storing, and transmitting information.

3. OBJECTIVES

The objectives of PT Niterra Mobility Indonesia's ISMS are:

- To maintain confidentiality, integrity, and availability of information.
- To mitigate information security risks to acceptable levels.
- To comply with applicable laws, regulations, and contractual requirements.
- To ensure the secure handling of customer and partner information.
- To foster a culture of continuous improvement in information security management.

4. DEFINITIONS

- **Operations:**

Activities to set out how information systems are operated to protect information security.

Includes standard procedures for operation of key systems and responsibilities of operators in normal conditions as well as fault and incident reporting and review.

Process for assignment of duties to staff should include consideration of whether segregation of duties is necessary. Also includes capacity management of information systems.

- **Information Handling:**

Information handled by the organization and the requirements on the labelling, storage, transmission, processing and disposal of each.

Requirements may include confidentiality (in handling, storage and transmission), integrity (e.g. validation processes) and availability (e.g. backups).

- **User Management**

Information of user accounts and privileges are created, managed and deleted. Includes how new users are authorized and granted appropriate privileges as well as how these are reviewed and revoked when necessary, and appropriate controls to prevent users obtaining unauthorized privileges or access.

Also includes recording of user activity on information systems and networks.

- **System Management**

Document setting out the responsibilities and required behavior of those managing computer systems.

Includes requirements on the maintenance and management of information systems and the software and services they run.

Also required security software (e.g. antivirus) and configurations, as well as appropriate logging and monitoring of system activity, and expected behavior when faults or incidents are detected.

- **Network Management**

Document setting out how networks are designed, and systems connected to them.

Includes continuing risk assessment and appropriate technical and procedural controls to reduce risk and to meet the requirements of the information handling policy, as well as emergency measures to deal with faults and incidents.

- **Software Management**

Document setting out how software runs on information systems is managed. Includes controls on the installation and use of software, the features provided and granting of access to software packages. Also includes maintenance of software with appropriate procedures for upgrades to minimize the risk to information.

5. LEADERSHIP & COMMITMENT

Top management at PT Niterra Mobility Indonesia is committed to the establishment, implementation, and continual improvement of the ISMS.

The leadership will ensure:

- Information security policies are integrated with the company's strategic objectives.
- Resources necessary for ISMS implementation, including human, technical, and financial resources, are allocated.
- Ongoing training and awareness programs are conducted to foster a security-conscious culture.
- Regular reviews of the ISMS to address any changes in risks or the external environment.

6. ROLES & RESPONSIBILITIES

A. Executive Management

1. Evaluating and accepting risk on behalf of the company
2. Identifying information security responsibilities and goals and integrating them into relevant processes
3. Supporting the consistent implementation of information security policies and standards
4. Supporting security through clear direction and demonstrated commitment of appropriate resources
5. Determining who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data

B. Information Security Management System

1. Supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network(s) which support the information owners

2. Providing resources needed to maintain a level of information security control consistent with this policy
3. Identifying and implementing all processes, policies and controls relative to security requirements defined by the business and this policy
4. Implementing the proper controls for information owned based on the classification designations
5. Providing training to appropriate technical staff on secure operations
6. Fostering the participation of information security and technical staff in protecting information assets, and in identifying, selecting and implementing appropriate and cost-effective security controls and procedures
7. Implementing business continuity and disaster recovery plans.

C. Employees

1. Understanding & commit the baseline information security controls necessary to protect the confidentiality, integrity and availability of information entrusted
2. Protecting information and resources from unauthorized use or disclosure
3. Protecting personal, private, sensitive information from unauthorized use or disclosure
4. Abiding by Acceptable Use of Information Technology Policy
5. Reporting suspected information security incidents or weaknesses to the appropriate manager and IT representative.
6. Understand the requirements arising from business strategies, rules, laws and contracts.
7. Understand the risk of information security threats now or in the future.

D. Third-Party Vendors

Must comply with the company's security policies when accessing PT Niterra Mobility Indonesia's information systems.

7. INFORMATION CLASSIFICATION

Information classification is a process used to categorize data based on the level of sensitivity and the impact that disclosure, modification, or destruction of the data.

The purpose is to ensure that information is appropriately protected according to its value and sensitivity.

Information Classification Categories:

1. PUBLIC

- *Description:* Information that is intended for public dissemination. There are no restrictions on access and can be freely shared with anyone without causing harm to the organization.
- *Examples:* Social media, Marketing materials, press releases, publicly available financial reports, and information published on the organization's website.
- *Protection Measures:* Minimal security controls, ensuring that the information remains accessible and accurate.

2. INTERNAL

- *Description:* Information that is not intended for public distribution but can be shared within the organization without special permissions. Access to this information is restricted to employees or authorized personnel.
- *Examples:* Internal memos, internal emails, company policies, and internal project documents.
- *Protection Measures:* Standard security controls such as user authentication, access controls, and regular backups.

3. CONFIDENTIAL

- *Description:* Sensitive information that requires protection because unauthorized disclosure, modification, or destruction could cause significant harm to the organization. Access to this information is limited to individuals who need it to perform their job duties.
- *Examples:* Employee records, internal financial statements, business plans, and customer information.
- *Protection Measures:* Enhanced security controls including stricter access controls, regular audits, and employee training on handling sensitive information.

4. RESTRICTED

- *Description:* Highly sensitive information that, if disclosed, could cause severe damage to the organization. Access is strictly controlled and limited to a small number of authorized individuals.

8. SECURITY CONTROLS

The ISMS is based on the following core security controls in compliance with ISO 27001:

- **Access Control:** Ensure that access to information and systems is restricted to authorized personnel based on the principle of least privilege.
- **Asset Management:** Maintain an inventory of information assets and classify them based on their importance and sensitivity.
- **Cryptography:** Implement encryption for sensitive data in transit and at rest.
- **Physical Security:** Secure facilities and equipment to prevent unauthorized physical access, damage, and interference.
- **Operations Security:** Establish secure operational procedures, including malware protection, backup management, and system monitoring.
- **Communications Security:** Ensure the secure exchange of information over networks, preventing unauthorized access, loss, or tampering.
- **Incident Management:** Develop a process to identify, report, and manage security incidents, including appropriate escalation and response mechanisms.
- **Business Continuity:** Ensure business continuity through disaster recovery planning and regular testing of critical systems.

9. INCIDENT RESPONSE AND BUSINESS CONTINUITY

PT Niterra Mobility Indonesia will:

- Maintain and regularly test an incident response plan to handle information security incidents.
- Ensure that all incidents are reported, logged, investigated, and resolved
- Maintain a business continuity plan (BCP) with GHQ to ensure the availability of critical business functions in the event of a security incident or disruption.

10. TRAINING AND AWARENESS

All employees and contractors are required to have regular information security training that covers:

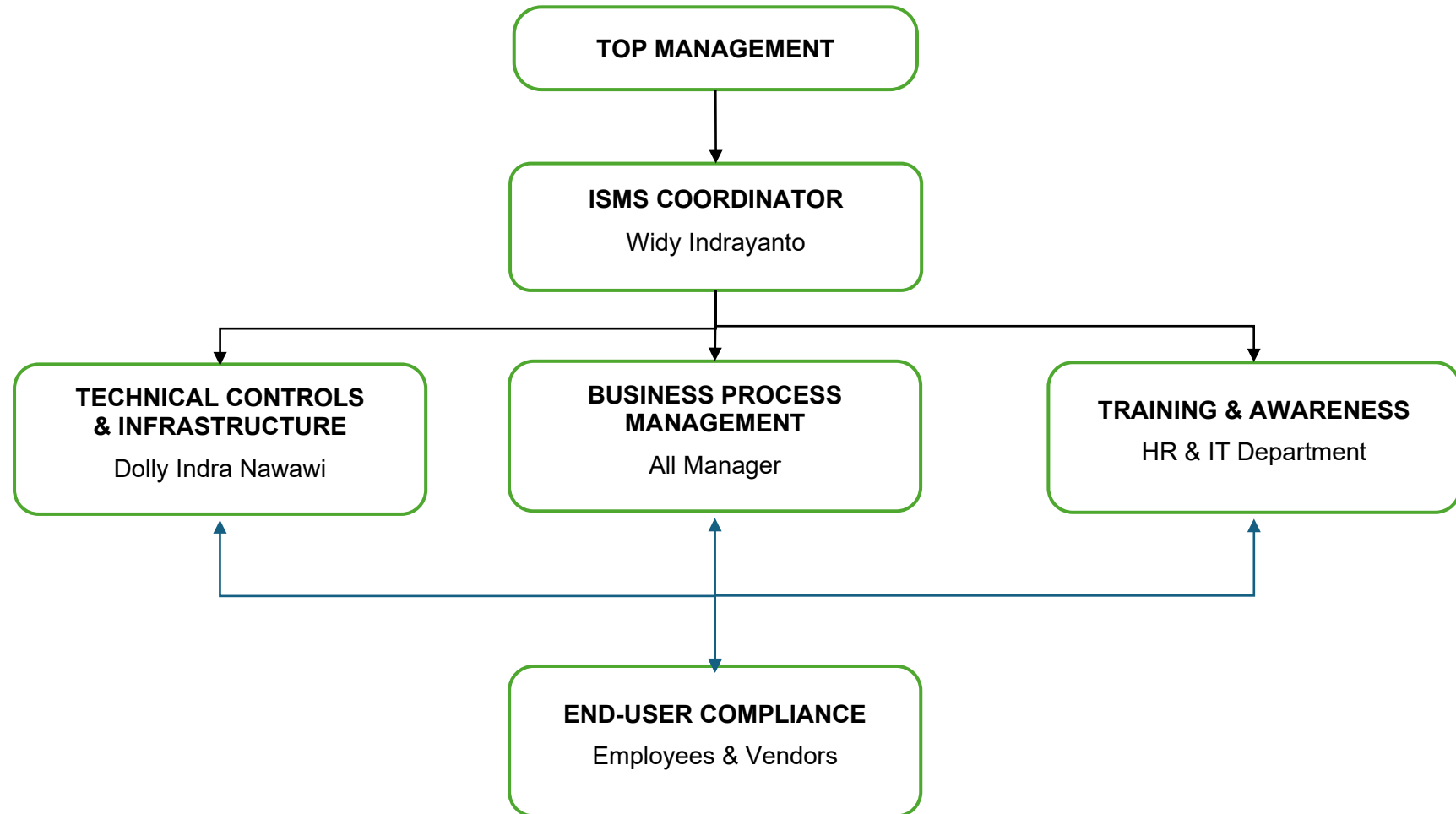
- The importance of information security.
- How to identify potential security threats (e.g., phishing).
- Procedures for reporting security incidents or breaches.

11. REVIEW & MONITORING

- The IT department will review all material information periodically (yearly) and revised based on new/ updated information.
- The IT department will also publish new revision to all stakeholders.
- IT department will review and monitoring by periodically usage of the software that existed.
- IT personnel also have the right to delete any files or data that are in the system that is categorized as a threat. Including all information contrary to the IT Security Policy.

APPENDIX PAGE

I. Information Security Management Chart



REVISION HISTORY				
No.	Date Revision	Rev	Pages / Points	Revision Material
01	September 2024	0	All	Create ISMS Policy
				Create ISMS Chart