



GLOBE Information Security Policy

I. PURPOSE

Globe Telecom, Inc. (“GLOBE”) recognizes that as a leading telecommunications provider, we are entrusted with the confidentiality, integrity, and availability of customer and employee information, communications, and critical business systems. This includes our business processes, network operations, information technology environments, and data centers. At the core of this Information Security Policy is an Information Security Management System (ISMS) that fosters a culture of information security as part of our corporate governance responsibilities.

We are committed to protecting information assets against all threats, whether internal or external, deliberate or accidental, to ensure uninterrupted service to our customers, partners, regulators, and stakeholders. This Information Security Policy establishes the framework for managing information security across GLOBE for the protection of the confidentiality, integrity, and availability of its information assets and in alignment with ISO/IEC 27001: Information Security Management Systems (ISMS).

The resulting Information Security Management System (ISMS) enables Globe to maintain its position as the network of choice by ensuring the secure and resilient delivery of critical products and services.

II. SCOPE OF APPLICATION

This policy applies to all GLOBE Board of Directors, key officers, employees, and all third parties representing and transacting with GLOBE, and functions as a guide for our subsidiaries and affiliates within the Globe Group of Companies.

Similarly, GLOBE ensures that third parties that represent and transact with us have in place, and/or are able to develop and build, their own information security policies and programs consistent with the standards and principles espoused herein.

III. STATEMENT OF COMMITMENT

As a telecommunications company, the protection and security of our information assets is our highest priority.

GLOBE commits to the following:

Governance and Continuous Improvement

- Aligning with international frameworks and best practices on information security, such as but not limited to ISO 27001, PCI-DSS, NIST, and SWIFT.
- Regularly reviewing and continually improving the ISMS through audits, monitoring,



testing, and management reviews to address emerging threats, vulnerabilities, and business needs;

- Reporting the performance of our ISMS to the Board, detailing the governance processes for critical security issues—such as cyber threats, data privacy, regulatory compliance, and incident management—to ensure all key risks are identified, managed, and continually improved;
- Providing the resources required to develop, implement, and continually improve our information security management framework;
- Compliance with all applicable ethical, legal, regulatory, and contractual requirements for information security, privacy, and core data center operations;

Risk Management

- Protecting the Confidentiality, Integrity, and Availability (CIA) of our customer, employee, and corporate information assets across all platforms, including our telecommunications networks, IT systems, and data centers;
- Identifying, assessing, and managing information security risks using a structured ISMS framework, ensuring that risks are treated within acceptable levels;
- Aligning with our Corporate Business Continuity Management System (BCMS) by ensuring information security controls support resilience against cyber threats, system disruptions, and data breaches;
- Detecting, reporting, and responding promptly to information security incidents to minimize business disruption and customer impact, including notifying affected data subjects and relevant legal and regulatory authorities when required;

Environmental Sustainability

- Prioritizing the procurement of energy-efficient hardware
- Ensuring the responsible disposal or recycling of equipment

Culture Building

- Ensuring our third parties, including vendors, suppliers, and partners, adhere to Globe's information security standards and practices;
- Promoting effective security awareness, education, and training to ensure that all employees and third parties understand their roles in safeguarding information and embrace a culture of information security and data protection.

IV. COMMUNICATION, TRAINING, AND AWARENESS

Policies related to GLOBE's Information Security Management Systems are made readily and easily available to all Board of Directors, key officers, employees, and third-party users. This policy and any amendments thereto will be posted through the internal communication channels and the corporate website of Globe. All covered persons are responsible for reading and implementing this policy at all times.



V. POLICY COMPLIANCE

All employees, including third parties and other covered persons, are required to comply with this Information Security Policy, the Information Security Manual, and all other relevant information security standards, procedures, and advisories issued by the company.

The Information Security Policy will be reviewed annually and whenever significant changes to internal or external factors occur.

VI. RELEVANT POLICIES AND DOCUMENTS

GLOBE's Information Security Management System is defined by its Information Security Policy framework, which comprises the following documents:

Internal

- Information Security Manual
- Information Security Program
- Employee Privacy Policy
- Acceptable Use Policy
- Integrated Management System Manual
- Energy Management Policy
- Social Media Policy

Public

- Globe Privacy Policy
- Manual of Corporate Governance
- Code of Conduct
- Business Continuity Management Policy
- Environmental Sustainability Policy
- Health and Safety Policy

Approved by:

Anton Reynaldo Bonifacio
Chief Information Security Officer and Chief Artificial Intelligence Officer
February 2026