Information Security Policy

The following is a summarized version of Terra Translations LLC's internal security policy. For further information regarding Terra's security policies and procedures, you can contact the Information Security Officer at cfo@terratranslations.com

1. OBJECTIVE

The purpose of this policy document is to define the direction, principles, and basic rules for information security management within Terra Translations LLC. This document describes the management's vision and commitment to effectively protect "confidentiality," maintain "integrity," and ensure the "availability" of its information assets and to respond and recover from information security incidents when they arise.

Information security is deemed to safeguard three main objectives:

- **Confidentiality** – Data and information assets must be confined to people authorized to access them and not be disclosed to others.
- **Integrity** – Keeping the data intact, complete, and accurate, and information systems operational.
- **Availability** – An objective indicating that information or system is at the disposal of authorized users when needed.

2. SCOPE

This policy is applicable to the following:

- All staff members working for Terra Translations LLC who have access to the organization's and client's information.
- All staff members, vendors, and third-party employees who have access to Terra Translations LLC's information processing systems and the data contained in them. This includes the data accessed by licensed third parties, which is, in turn, deployed to and used by their clients.
- All stakeholders and interested parties who are relevant to the operations of Terra Translations LLC.
- All digital and non-digital assets that play a role in the creation, storage, transmission, and disposal of information come under the purview of this policy.

3. POLICY STATEMENT

- Terra Translations LLC shall establish, implement, and maintain a holistic and robust Information Security Management System (ISMS). ISMS is defined as the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. The management system includes the information systems that support commercialization and provision of text translation and localization services based on the applicability statement.
- The ISMS shall have adequate and appropriate arrangements which shall enable it to effectively protect "confidentiality, maintain "integrity" and ensure "availability" of its information assets and to respond and recover from information security incidents when they arise.
- While planning the ISMS, Terra Translations LLC shall consider its internal and external issues along with the requirements of the interested parties and determine risks and opportunities which could affect the activities supporting the provision of its products and services. The top management shall provide the required resources and sufficiently contribute towards the ISMS, ensuring it achieves its intended outcome(s).

4. INFORMATION SECURITY REQUIREMENTS

- Information and supporting technology - including hardware and software systems, are critical business assets. Confidentiality, integrity, and availability of information are essential to maintaining a better competitive edge, profitability, legal compliance, and reputation.
- Organizations and their information systems and networks increasingly face security threats from a wide range of sources, including external hacking and intrusions, computer-assisted fraud, espionage, sabotage, vandalism, or damage from natural disasters. Due to the dependence on information systems and services, organizations are now more vulnerable to security threats.
- Designing security controls and implementing them requires careful planning and attention. Management policies and administrative controls are needed to supplement technical controls that are implemented to protect data. Information Security Management needs, at a minimum, participation from all employees in the organization. It may also require involvement from suppliers, vendors, service providers, customers, and external specialists.

5. INFORMATION SECURITY OBJECTIVES

The objectives of the Information Security Policy are:

- To create a coherent system for the management of information security that is aligned with

Terra Translations LLC's business strategy.

- To protect and safeguard the information that is important to Terra Translations LLC and its clients. To reduce risk related to the use of technology and technology outsourcing.
- To ensure that all Terra Translations LLC's information assets are accounted for and adequately protected from damage, alteration, loss, and unauthorized use or access.
- To ensure that information and information systems are available only to authorized users.
- To ensure that Terra Translations LLC provides its customers with the means to enable them to fulfill their obligation to facilitate the exercise of Personally Identifiable Information (PII) principals' right to access, correct, or erase PII pertaining to them, defined by the contract.
- To ensure that PII processed under a contract shall not be processed for any purpose independent of the instructions of Terra Translations LLC's customer.
- To be compliant with all information security-related regulatory and statutory requirements pertaining to information collection, storage, processing, transmission, and disclosure.
- To set aside resources to establish, implement, operate, monitor, review, and maintain information security safeguards.
- To create awareness of information security and to ensure that all employees understand their responsibilities for maintaining information security.
- To create detailed information security best practices and guideline documents and ensure compliance with such documents.
- To assess and update the information security policy objectives periodically as per the business need and ensure continuous improvement.

6. SEGREGATION OF DUTIES

- Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of an organization's assets.
- While assigning responsibilities, conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
- Care shall be taken that every individual may access, modify or use assets with proper authorization or detection. The possibility of collusion should be considered while designing the controls.

7. CONTACT WITH SPECIAL INTEREST GROUPS

Based on requirements and proper vendor validation, specialist advice shall be sought whenever required. This could be by having a Security Consultant on a contractual or per-call payable basis. The same could also be sought from non-profit agencies.

8. CONTACT WITH AUTHORITIES

Where required, the organization shall maintain appropriate contact with law enforcement authorities, regulatory bodies, fire departments, emergency services, telecommunication providers, and others. These contacts shall ensure help can be availed of and is accessible during a crisis.

9. INFORMATION SECURITY IN PROJECT MANAGEMENT

Information security should be integrated into the organization's project management method(s) to ensure that information security risks are identified and addressed as part of a project. This applies generally to any project regardless of its character. Examples: a project for a core business process, IT, facility management, and other supporting processes.

10. RESPONSIBILITIES

- The Information Security Officer has the ultimate authority over the Information Security Policy and approves and authorizes all changes to the Information Security Policy.
- The Information Security Officer has executive authority over information security and works with Executive Management to approve, authorize, and issue all documentation.
- The Information Security Officer is responsible for the development and maintenance of all ISMS documentation.
- The Information Security Officer shall schedule periodic internal audits with the help of either the internal team or external consultants.
- The Information Security Officer, along with the Head of Engineering, is responsible for building a strategic and comprehensive privacy program that defines, develops, maintains, and implements policies and processes that enable consistent, effective privacy practices which minimize the risk and ensure the confidentiality of Personally Identifiable Information (PII), paper or electronic, across all media types.

11. SCHEDULE

This document is to be reviewed annually and whenever significant changes occur in the organization.