SUMMARY OF THE COMPREHENSIVE INFORMATION SECURITY AND CYBERSECURITY POLICY

1. Purpose and Scope

The purpose of this policy is to establish a corporate framework for managing information security and cybersecurity, ensuring the confidentiality, integrity, and availability of both internal and third-party data throughout Multi X's operations.

- Protect information assets from unauthorized access, loss, or manipulation.
- Ensure operational continuity through appropriate controls and preventive measures.
- Promote an organizational culture based on security and digital responsibility.

2. Responsibilities

Senior Management: Responsible for approving and supporting the implementation of the policy.

Security Committee: In charge of overseeing and coordinating security activities.

Process Owners: In charge of overseeing and coordinating security activities.

Users: Must comply with the established policies and procedures.

3. Activity Description

3.1. Main Guidelines

Risk Management: Identification, assessment, and treatment of security risks.

Access Control: Ensure that only authorized personnel have access to information.

Communication Security: Protect information during transmission.

Incident Management: Procedures for detecting, reporting, and responding to cybersecurity incidents.

3.2. Key Control Measures

Implementation of technical and administrative controls to protect information.
Information security training and awareness across the organization.
Monitoring and auditing of information systems to detect and prevent threats.
Commitment to continuous improvement through regular review and updates of the security policy to ensure its effectiveness.

This policy is essential to maintaining the trust of customers, employees, and stakeholders and is part of Multi X's commitment to responsible, traceable, and resilient information security management.

4. Annexes

Reference: PS-TI-PL01- Comprehensive Information Security and Cybersecurity Policy.