INFORMATION SECURITY REQUIREMENTS FOR THIRD PARTIES AND SUPPLIERS

1. OBJECTIVE

To establish general information security requirements for third parties that access or interact with the organization's systems, networks, applications, servers, information, or other resources. The objective is to reduce the risks of unauthorized access, misuse, compromised credentials, information exposure, and the spread of external threats.

2. SCOPE

This guideline applies to suppliers, contractors, consultants, and service providers that require connectivity, remote access, or authorized interaction with information assets or technology resources. Controls are applied proportionately based on service criticality, access level, information processed, exposure, and potential impact.

3. GENERAL PRINCIPLES

- Prior authorization for third-party remote access through a formal request and the corresponding approvals.
- Individual and traceable identities.
- Least privilege.
- Multi-factor authentication for remote access.
- Limited validity while a legitimate business need exists.
- Controls proportionate to risk and prevention and response capabilities.

4. THIRD-PARTY OBLIGATIONS

- Use access exclusively for the approved activity.
- Protect credentials and authentication mechanisms; do not share accounts.
- Do not attempt to access unauthorized resources.
- Maintain general security conditions on the devices used.
- Allow a general security validation of the device, when applicable.
- Report suspected compromises or incidents and cooperate with containment and remediation efforts.

5. ACCESS MANAGEMENT AND APPROVAL

All access must be requested through the established corporate channels and approved by the responsible internal party. Before access is enabled, the third party, business need, requested scope, and person responsible for the access must be identified.

Control rule: Approval of the business relationship does not, by itself, authorize access to technology resources.

6. REMOTE ACCESS SECURITY

When warranted by the level of risk, the organization may use a checklist to validate the device's general security conditions. The review may consider whether the technology environment in use is current and up to date, the implementation of threat protection mechanisms, the application of device security controls, and other measures intended to preserve the confidentiality, integrity, and availability of information. Access may be conditional upon remediation of any findings.

Third parties must use individual and traceable identities. Generic or shared accounts should be avoided whenever possible. Permissions are restricted to the resources necessary for the approved purpose, applying least privilege and segregation of duties when appropriate.

7. THREAT MONITORING AND DETECTION

The organization conducts monitoring and threat detection activities related to third-party access and connectivity. Identified situations may lead to preventive or corrective measures, including, when appropriate, temporary blocking or suspension of connectivity until the risk has been assessed and mitigated.

8. INCIDENT MANAGEMENT

In the event of a threat or potential compromise, the organization may coordinate validation, containment, and remediation with the third party. Depending on the risk, measures may include changing or revoking credentials, temporarily suspending access, preventive blocking, and restoring access once the risk has been mitigated.

9. NON-COMPLIANCE, REVIEW, AND IMPROVEMENT

Failure to comply with the obligations, security requirements, or access conditions established in this guideline may result in privilege restrictions, changes to or revocation of credentials, suspension or disabling of access, preventive blocking, and a request for remediation. Continued or restored access is subject to risk mitigation and the continued existence of a legitimate business need.

The organization periodically reviews the appropriateness of access granted to third parties and adjusts security measures when the business need, scope, or associated risk level changes.