

Third-Party Access Policy

1. Purpose

This policy defines requirements for granting third-party access to company information systems and data. Its purpose is to ensure the security and privacy of organizational assets when accessed or handled by external parties.

2. Scope

This policy applies to all third-party vendors, contractors, partners, and service providers who require access to company information systems, networks, or data.

3. Policy

- Authorization:** All third-party access must be formally requested, reviewed, and approved by authorized personnel.
- Agreement:** Third parties must sign a Non-Disclosure Agreement (NDA) and comply with all relevant security policies and procedures.
- Access Controls:** Access shall be limited to the minimum required for the agreed purpose and be time-bound.
- Monitoring:** All third-party activities may be monitored to detect and prevent unauthorized access.
- Termination:** Access rights will be immediately revoked when no longer required or upon contract termination.
- Compliance:** Third parties must comply with all applicable laws, regulations, and company policies.

4. Responsibilities

It is the responsibility of the IT department and department heads to ensure third-party access is provided according to this policy. Third parties are responsible for complying with all stated requirements.

5. Enforcement

Violation of this policy may result in suspension of access, contract termination, and potential legal action.

6. Review

This policy shall be reviewed annually and updated as needed.