Third-Party Risk Management Policy and Procedure

1. Purpose

This policy establishes a framework for managing risks associated with third-party providers and vendors, ensuring that their engagement does not compromise the organization's security, compliance, and operational standards.

2. Scope

This policy applies to all third-party engagements, including vendors, suppliers, contractors, and service providers, with whom the organization interacts or relies upon for products and services.

3. Policy Statement

The organization is committed to a systematic approach to managing third-party risks through effective classification, inventory management, risk assessment, ongoing monitoring, and decommissioning processes.

4. Responsibilities

- **Third-Party Risk Management Team (TPRMT)**: Responsible for implementing and overseeing the third-party risk management process.
- **Department Heads**: Accountable for ensuring that their third-party engagements comply with this policy.
- **Procurement Team**: Works in coordination with the TPRMT to vet and onboard new third-party providers.

5. Procedures

5.1 Classification

- Categorize third-party providers based on the level of risk they pose, considering factors such as the sensitivity of data accessed, the criticality of services provided, and compliance requirements.

5.2 Inventory

- Maintain an up-to-date inventory of all third-party providers, including details of the services provided, contract terms, and contact information.
- Regularly review and update the inventory to reflect any changes in the third-party relationships.

5.3 Risk Assessment

- Conduct thorough risk assessments for each third-party provider, evaluating potential threats and vulnerabilities associated with their services or products.
- Use standardized assessment tools and methodologies to ensure consistency and completeness.

5.4 Monitoring

- Implement ongoing monitoring procedures to assess the third-party providers' compliance with the agreed-upon security and performance standards.
- Regularly review third-party performance reports, audit results, and security assessments to identify any changes in the risk profile.

5.5 Decommissioning

- Establish clear procedures for the orderly termination of third-party relationships, including the secure transfer or destruction of any shared data and the revocation of access privileges.
- Conduct a final risk assessment to ensure that all potential risks associated with the decommissioning process are managed.

6. Compliance

- Non-compliance with this policy may lead to disciplinary actions and increased risk exposure.
- The TPRMT will monitor compliance and report findings to the executive management team.

7. Review and Revision

- Review and update the third-party risk management policy and procedures at least annually or when significant changes in the business or third-party landscape occur.
- Revisions should be approved by senior management and communicated across the organization.

By adopting and adhering to this third-party risk management policy and procedure, the organization ensures a structured and consistent approach to managing the risks associated with third-party engagements, thereby protecting its assets, reputation, and operational capabilities.