elevaite365

TECH THAT MATTERS

Elevaite365

Vendor Management Policy

Version 1.0

PURPOSE

This Vendor Management Policy ensures that all external providers, including vendors, suppliers, service providers, and sub-service organizations (such as cloud service providers), are introduced, maintained, and controlled through defined processes. The policy seeks to mitigate risks associated with third-party relationships, protect the Organization's assets and information, and ensure that external providers comply with the Organization's security and operational standards.

SCOPE

This policy applies to all vendors, suppliers, outsourced contractors, service providers, and sub-service organizations, including cloud service providers, who work with Elevaite365 (herein referred to as "the Organization") and its various departments to provide goods, services, or workforce. Specifically, it encompasses:

1. **All External Providers**: Vendors, suppliers, contractors, consultants, service providers, sub-service organizations, and cloud service providers.
2. **IT Systems**: All systems that process, store, or transmit confidential, private, or business-critical data.
3. **Risk Considerations**: Both medium-to-long-term strategic risks and day-to-day operational risks.
4. **Risk Management Systems**: Processes aimed at achieving maximum benefit without increasing bureaucratic burdens or affecting core service delivery.
5. **Materiality of Risk**: Focus on material risks in developing risk management systems and processes.
6. **Applicable Individuals and Entities**: All employees of the Organization and external parties, including consultants, contractors, business partners, vendors, suppliers, outsourced service providers, and other third-party entities with access to the Organization's networks and system resources.

DEFINITIONS

Following is an explanation of various terms used within this document:

- **Vendor**: External person, entity, or organization that provides goods, services, or human resources to the Organization on a one-time or ongoing basis. This includes vendors, suppliers, contractors, consultants, service providers, sub-service organizations, and cloud service providers.

- **Outsourcing**: The use of third-party services to perform activities generally undertaken by the Organization, either now or in the future. This excludes services typically not expected to be carried out internally, such as legal or banking services. A legal contract must exist for all outsourcing activities.

- **Sub-Service Organization**: An entity that a service organization uses to perform some of the services provided to customers (user entities). The service organization relies on processes and controls implemented at the sub-service organization to meet the SOC report's control objectives or trust services principles.

- **CSP**: Cloud Service Provider – An external provider that offers cloud-based services and infrastructure.

- **SLA**: Service Level Agreement – A commitment of service and its deliverables between a service provider and service recipient (the Organization).

- **OLA**: Operational Level Agreement—This agreement defines interdependent relationships in support of an SLA. It describes the responsibilities of each internal support group towards other support groups, including the process and timeframe for service delivery.

- **NDA**: Non-Disclosure Agreement – A contract wherein one or more parties agree not to disclose confidential or sensitive information shared during business engagements.

- **MSA**: Master Service Agreement – A contract between the Organization and a vendor outlining the terms (SOW, SLA) governing future transactions or agreements.

- **SOW**: Statement of Work – An annexure to a service agreement/MSA containing milestones, timelines for deliverables, SLAs, reports, etc. It serves as the basis for executing and framing specific service agreements.

- **BCP**: Business Continuity Plan – A plan to ensure business operations can continue during and after a significant disruption or disaster.

- **DR**: Disaster Recovery – Procedures and processes to recover and protect an organization’s IT infrastructure in a disaster.
- **ISG**: Information Security Group – The team responsible for overseeing and implementing information security policies and procedures within the Organization.
- **LT**: Leadership Team – The senior management team responsible for strategic decision-making within the Organization.

RESPONSIBILITIES

Chief Information Security Officer (CISO)

- Risk Acceptance: Ultimately responsible for accepting and/or treating any risks to the Organization.
- Approval Authority: Can approve the avoidance, remediation, transference, or acceptance of any risk cited in the Risk Register.
- Strategic Oversight: Ensures alignment of risk management with the Organization’s strategic objectives.

Chief Technology Officer (CTO)

- Risk Identification: Identifies and develops treatment plans for all information security-related risks.
- Risk Treatment Plans: Oversees the creation and implementation of risk treatment plans.
- Communication: Communicates risks to top management and ensures risk treatments are adopted by executive direction.

Information Security Group (ISG)

- Policy Implementation: Develops and enforces the Vendor Management Policy in collaboration with relevant departments.
- Monitoring and Compliance: Ensures adherence to the policy through regular audits and inspections.
- Training and Awareness: Conducts training sessions to educate employees and contractors about vendor management best practices.
- Incident Response Coordination: Coordinates responses to identified vendor-related risks and security incidents.

Department Heads

- Vendor Oversight: Oversee vendor engagements within their respective departments.
- Due Diligence: Ensure due diligence is conducted for all new vendor relationships.
- Performance Monitoring: Monitor vendor performance and compliance with contractual obligations.

Vendors, Suppliers, and Service Providers

- Compliance: Adhere to the Organization’s security and operational standards as defined in contracts and agreements.
- Reporting: Promptly report any security incidents, breaches, or vulnerabilities to the Organization.
- Continuous Improvement: Implement continuous improvements based on feedback and assessments from the Organization.

POLICY

VENDOR CLASSIFICATION

Organization classifies vendors to determine the level of management and oversight required:

1. Critical Vendor: Meets either of the following criteria:
   - A vendor whose products or services store, process, or transmit any “Confidential” information.
   - A vendor who provides the Organization with essential products or services crucial to business operations.
2. Non-Critical Vendor: Any vendor not qualifying as a Critical Vendor must not be managed under this process but may still need to comply with essential contractual obligations.

VENDOR ONBOARDING

Vendor Due Diligence

The ISG and department heads are responsible for conducting due diligence on vendor engagements. This includes:

1. **Research and Assessment:**
   - Detailing expected functionality, technology requirements, security controls, and commercial viability.
   - Ensure vendors know the organization’s internal security requirements and address any concerns.

2. **Selection Process:**
   - All vendors must undergo a selection process before shortlisting or onboarding.
   - Selection Criteria:
     a. Experience
     b. Cost
     c. Competency
     d. Required compliances, including licenses, permits, registrations, etc.
     e. Organizational strengths and structure
     f. References from existing customers
3. **Agreements and Contracts:**
   - Non-Disclosure Agreement (NDA): Must be signed with all vendors before exchanging or onboarding any confidential information.
   - Master Service Agreement (MSA): Establishes the overarching terms governing future transactions or agreements.
   - Statement of Work (SOW): Defines specific deliverables, milestones, timelines, SLAs, and reporting requirements.
4. **Access Control:**
   - Access to the Organization’s network or information systems is provided on a need-to-know basis with proper approvals.
5. **Background Verification:**
   - The human resource team must conduct appropriate background verifications and screenings for vendors involved in critical activities through third-party or internal reference checks.

VENDOR MONITORING

1. **Performance Monitoring:**
   - Deliverables and commitments defined in SLAs are monitored periodically by the concerned department.
   - Services, deliveries, uptimes, resolutions, and responses are tracked against agreed terms.
2. **Discrepancy Management:**
   - Appropriate escalations are initiated with the external provider for any discrepancies or breaches in SLAs, including penalties if applicable.
3. **Access Monitoring:**
   - Vendor access is monitored and reviewed regularly.
   - Logs of access, transactions, etc., involving the vendor are maintained for analysis.
4. **Audits and Assessments:**
   - Vendors may be audited for their services and compliance with applicable laws.
   - Information security controls implemented by vendors are verified through Information Security Audit Reports, ISO 27001 reports, or SOC 2 Reports.
5. **Critical Vendor Reviews:**
   - An annual list of essential vendors is documented.
   - A plan to review a sample of these vendors is maintained and performed with the ISG and department heads.
   - Documentation supporting vendor reviews is retained.

MANAGING CHANGES TO VENDOR SERVICES

Change Management:

- Changes to the provision of services for critical vendors, including policy, procedure, and control updates, are managed based on the criticality of business systems and processes.

Internal Changes:

- Enhancements to current services, development of new applications and systems, modifications or updates to policies and procedures, and implementation of new controls.

Vendor-Initiated Changes:

- Changes and enhancements to networks, adoption of new technologies, use of newer product versions/releases, changes to the physical location of service facilities, and vendor changes.

Risk Re-Assessment:

- Re-assessing risks associated with any changes to ensure continued alignment with the Organization’s risk appetite and security requirements.

VENDOR OFFBOARDING

Termination Scenarios:

- Offboarding may occur at the end of tenure, contract period, or upon termination of services.

Separation Process:

- Define and follow the process, requirements, and steps involved during vendor separation.

Data and Asset Handover:

- Planned and conducted the smooth handover of data, information, copyright material, intellectual property, source codes, transaction logs, backups, etc., avoiding disruption.

Access Revocation:

- Revoke all vendor access immediately at the end of tenure.
- Verify and confirm the revocation of administrative access by the ISG.

Asset Return:

- Ensure all assets, information, or software provided to the vendor are returned.
- Obtain acknowledgment from the vendor and update the Asset Inventory accordingly.

CLOUD SERVICE PROVIDER

In addition to the general vendor management procedures, the following points are relevant to managing Cloud Service Providers (CSP):

1. **Geographical Compliance:**
   - Confirm the geographical locations of the CSP’s organization and the countries where data is stored, considering applicable laws and regulations.
2. **Authentication Controls:**
   - Ensure CSPs provide sufficient authentication techniques for cloud service administrators based on identified risks.
3. **Cryptographic Controls:**
   - Implement cryptographic controls for cloud services if justified by risk analysis.
   - Review and confirm that CSP-provided cryptographic capabilities meet the Organization’s policies and are compatible with existing protections.
4. **Secure Disposal:**
   - Request confirmation that the CSP has policies and procedures for the secure disposal or reuse of resources.
5. **Change Notifications:**
   - Ensure CSPs provide information regarding changes to cloud services that could adversely affect service delivery.
6. **Capacity Monitoring:**
   - Monitor the use of cloud services and forecast capacity needs to ensure ongoing performance.
7. **Backup Capabilities:**
   - Verify CSPs’ backup capabilities meet the Organization’s requirements.
8. **Vulnerability Management:**
   - Request information from CSPs about the management of technical vulnerabilities affecting cloud services.
9. **Tenant Segregation:**
   - Ensure CSPs enforce segregation between tenants in multi-tenant environments and between CSP’s internal administration environment and the Organization’s cloud computing environment.
10. **Digital Evidence Procedures:**
    - Agree upon procedures with CSPs to respond to requests for potential digital evidence or other information from the cloud computing environment.
11. **Regulatory Compliance:**
    - Ensure CSPs comply with relevant regulations and standards required for the Organization’s business.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	-	Initial Release	Borhan	-	-