Vendor Management Policy

Nexelus

Purpose

The purpose of this policy is to establish requirements for ensuring third-party service providers/vendors meet Nexelus requirements for preserving and protecting Nexelus information.

Scope

The policy applies to all IT vendors and partners who have the ability to impact the confidentiality, integrity, and availability of Nexelus' technology and sensitive information, or who are within the scope of Nexelus' information security program. This policy also applies to all employees and contractors that are responsible for the management and oversight of IT vendors and partners of Nexelus.

Background

This policy prescribes the minimum standards a vendor must meet from an information security standpoint, including security clauses, risk assessments, service level agreements, and incident management.

Roles and Responsibilities

Either a partner or, the General Manager are responsible for establishing Vendor Management policy. General Manager, Admin Manager and Network Manager are responsible for Vendor Management in general in accordance with Vendor Management Policy. Some of these responsibilities include:

- Working closely with vendors
- Assisting with planning and developing the vendor management policy, program, and procedures
- Facilitating vendor selection and contract negotiation processes
- Continuously monitoring vendor risk even after the vendor contract is executed (e.g., monitoring performance levels and periodically requesting and analyzing current due diligence)
- Communicating with internal departments such as lines of business/business units, internal audit, senior management and more to answer vendor questions and oversee tasks.

Policy

Nexelus makes every effort to assure all 3rd party organizations are compliant and do not compromise the integrity, security, and privacy of Nexelus or its customer data. 3rd parties include customers, partners, subcontractors, and contracted developers.

- IT vendors are prohibited from accessing Nexelus information security assets until a contract containing security controls is agreed to and signed by the appropriate parties.
- All IT vendors must comply with the security policies defined and derived from Nexelus' Information Security Program to include the *Acceptable Use Policy*.
- IT vendors and partners must ensure that organizational records are protected, safeguarded, and disposed of securely. Nexelus strictly adheres to all applicable legal, regulatory, and contractual requirements regarding the collection, processing, and transmission of sensitive data such as Personally Identifiable Information (PII).

Vendor Inventory

An inventory of third-party service providers shall be maintained, and will include:

- Vendor risk level
- Category
- Password Policy to access system, if applicable
- Brief description of services
- Internal owner

Vendor risk level assessment will be based on the following considerations:

- **High**: the vendor stores or has access to sensitive data and a failure of this vendor would have critical impact on your business
- **Moderate:** the vendor does not store or have access to sensitive data and a failure of this vendor would not have critical impact on your business
- **Low:** the vendor doesn't store or have access to any data and a failure of this vendor would have very little to no impact on your business

Vendor Contracts

Formal contracts, where applicable, that address relevant security and privacy requirements must be in place for all third parties that process, store, or transmit confidential data or provide critical services. The following must be included, if applicable, in all such contracts:

- Contracts will acknowledge that the third party is responsible for the security of the institution's confidential data that it possesses, stores, processes, or transmits.
- Contracts stipulate that the third-party security controls are regularly reviewed and validated by an independent party.
- Contracts identify relevant regulations for sub-contracting.
- Contracts implement specific processes for managing information and communication technology component lifecycle and availability and associated security risks.

- Contracts establish responsibilities for responding to direct and indirect security incidents including timing as defined by service-level agreements (SLAs).
- Contracts specify the security requirements for the return or destruction of data upon contract termination.
- Responsibilities for managing devices (e.g., firewalls, routers) that secure connections with third parties are formally documented in the contract.
- Contracts stipulate geographic limits on where data can be stored or transmitted.

Vendor Services Change Management

Changes to the provision of services by vendors, including maintaining and improving existing information security policies, procedures, and controls, should be managed, taking account of business information criticality, systems and processes involved and re-assessment of risks. The following aspects will be considered:

- Changes to supplier agreements.
- Changes made by the organization to implement:
    - Enhancements to the current services offered.
    - Development of any new applications and systems.
    - Modifications or updates of the organization's policies and procedures.
    - New/changed controls to resolve security incidents and improve security.
- Changes in supplier services to implement:
    - Changes and enhancement to networks.
    - Use of new technologies.
    - Adoption of new products or newer versions/releases.
    - New development tools and environments.
    - Changes to physical location of service facilities.
    - Change of suppliers.
    - Subcontracting to another supplier.