Third-Party Management Policy

Policy Owner: [Job title of policy owner]

Effective Date: [Date you choose, after which there will be consequences for personnel for non-compliance]

Purpose

To ensure protection of the organization's data and assets that are shared with, accessible to, or managed by suppliers, including external parties or third-party organizations such as service providers, vendors, and customers, and to maintain an agreed level of information security and service delivery in line with supplier agreements.

This document outlines a baseline of security controls that nexelus.net expects partners and other third-party companies to meet when interacting with nexelus.net Confidential data.

Scope

All data and information systems owned or used by nexelus.net that are business critical and/or process, store, or transmit Confidential data. This policy applies to all employees of nexelus.net and to all external parties, including but not limited to nexelus.net consultants, contractors, business partners, vendors, suppliers, partners, outsourced service providers, and other third-party entities with access to nexelus.net data, systems, networks, or system resources.

Policy

Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.

For all service providers who may access nexelus.net Confidential data, systems, or networks, proper due diligence shall be performed prior to provisioning access or engaging in processing activities. Information shall be maintained regarding which regulatory or certification requirements are managed by or impacted by each service provider, and which are managed by nexelus.net as required. Applicable regulatory or certification requirements may include ISO 27001, SOC 2, PCI-DSS, CCPA, GDPR or other frameworks or regulations.

Information Security in Third-Party Relationships

Addressing Security in Agreements

Relevant information security requirements shall be established and agreed with each supplier that may access, process, store, or transmit Confidential data, or provide physical or virtual IT infrastructure components for nexelus.net.

For all service providers who may access nexelus.net production systems, or who may impact the security of the nexelus.net production environment, written agreements shall be maintained that include the service provider's acknowledgment of their responsibilities for the confidentiality of company and customer data, and any commitments regarding the integrity, availability, and/or privacy controls that they manage in order to meet the standards and requirements that nexelus.net has established in accordance with nexelus.net's information security program or any relevant framework.

Technology Supply Chain

nexelus.net will consider and assess risk associated with suppliers and the technology supply chain. Where warranted, agreements with suppliers shall include requirements to address the relevant information security risks associated with information and communications technology

services and the product supply chain.

Third-Party Service Delivery Management

Monitoring & Review of Third-Party Services

nexelus.net shall regularly monitor, review, and audit supplier service delivery. Supplier security and service delivery performance shall be reviewed at least annually.

Management of Changes to Third-Party Services

Changes to the provision of services by suppliers, including changes to agreements, services, technology, policies, procedures, or controls, shall be managed, taking account of the criticality of the business information, systems, and processes involved. nexelus.net shall assess the risk of any material changes made by suppliers and make appropriate modifications to agreements and services accordingly.

Third-Party Risk Management

nexelus.net will ensure that potential risks posed by sharing Confidential data are identified, documented and addressed according to this policy. Risk management plays an integral part in the governance and management of the organization at a strategic and operational level. The purpose of a partner and third-party security policy is to ensure that partnerships and services achieve their business plan aims and objectives, and are consistent with nexelus.net's requirements for information security.

nexelus.net shall not share or transmit Confidential data to a third-party without first performing a third-party risk assessment and fully executing a written contract, statement of work or service agreement which describes expected service levels and any specific information security requirements.

Third-Party Security Standards

All third-parties must maintain reasonable organizational and technical controls as assessed by nexelus.net.

Assessment of third-parties which receive, process, or store Confidential data shall consider the following controls as applicable based on the service provided and the sensitivity of data stored, processed or exchanged.

Information Security Policy

Third-parties maintain information security policies supported by their executive management, which are regularly reviewed.

Risk Assessment & Treatment

Third-parties maintain programs that assess, evaluate, and manage information and technology risks.

Operations Security

Third-parties implement commercially reasonable practices and procedures designed, as appropriate, to maintain operations security. Protections may include:

- Technical testing
- Protection against malicious software

- Network protection and management
- Technical vulnerability management
- Logging and monitoring
- Incident response
- Business continuity planning

Access Control

Third-parties maintain a technical access control program.

Secure System Development

Third-parties maintain a secure development program consistent with industry software and systems development best practices including risk assessment, formal change management, code standards, code review and testing.

Physical & Environmental Security

If third-parties are storing or processing confidential data, their physical and environmental security controls should meet the requirements of the nexelus.net Physical Security Policy.

Human Resources

Third-parties maintain human resource policies and processes which include criminal background checks for any employees or contractors who access nexelus.net Confidential information.

Compliance & Legal

nexelus.net shall consider all applicable regulations and laws when evaluating suppliers and third parties who will access, store, process or transmit nexelus.net Confidential data. Third-party assessments should consider the following criteria:

- Protection of customer data, organizational records, and records retention and disposition
- Privacy of Personally Identifiable Information (PII)

Exceptions

Requests for an exception to this Policy must be submitted to the [approver of requests for exceptions to this policy, e.g., CFO] for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the [person responsible for receiving policy violation reports, e.g., CFO]. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
[1.0]	[29-Apr-2020]	[First Version]	[OWNER]	[APPROVER]