Information Security Roles and Responsibilities Policy

Policy Owner: [Job title of policy owner]

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

Statement of Policy

nexelus.net is committed to conducting business in compliance with all applicable laws, regulations, and company policies. nexelus.net has adopted this policy to outline the security measures required to protect electronic information systems and related equipment from unauthorized use.

Objective

This policy and associated guidance establish the roles and responsibilities within nexelus.net, which is critical for effective communication of information security policies and standards. Roles are required within the organization to provide clearly defined responsibilities and an understanding of how the protection of information is to be accomplished. Their purpose is to clarify, coordinate activity, and actions necessary to disseminate security policy, standards, and implementation.

Applicability

This policy is applicable to all nexelus.net infrastructure, network segments, and systems.

Audience

The audience for this policy includes all nexelus.net employees and contractors who are involved with the Information Security Program. Awareness of this policy applies for all other agents of nexelus.net with access to nexelus.net information and network. This includes, but not limited to partners, affiliates, contractors, temporary employees, trainees, guests, and volunteers. The titles will be referred collectively hereafter as "nexelus.net community".

Roles	**Responsibilities**
Board of Directors	• Oversight over Cyber-Risk and internal control for information security, privacy and compliance • Consults with Executive Leadership to understand nexelus.net IT mission and risks and provides guidance to bring them into alignment
Executive Leadership	• Approves Capital Expenditures for Information Security • Oversight over the execution of the information security risk management program and risk treatments • Communication Path to nexelus.net Board of Directors • Aligns Information Security Policy and Posture based on nexelus.net's mission, strategic objectives and risk appetite

IT Manager	• Oversight over the implementation of information security controls for infrastructure and IT processes • Responsible for the design, development, implementation, operation, maintenance and monitoring of IT security controls • Ensures IT puts into practice the Information Security Framework • Responsible for conducting IT risk assessments, documenting the identified threats and maintaining risk register • Communicates information security risks to executive leadership • Reports information security risks annually to nexelus.net's leadership and gains approvals to bring risks to acceptable levels • Coordinates the development and maintenance of information security policies and standards • Works with applicable executive leadership to establish an information security framework and awareness program • Serve as liaison to the Board of Directors, Law Enforcement, Internal Audit and General Council. • Oversight over Identity Management and Access Control processes
VP of Engineering	• Oversight over information security in the software development process • Responsible for the design, development, implementation, operation, maintenance and monitoring of development and commercial cloud hosting security controls • Responsible for oversight over policy development • Responsible for implementing risk management in the development process
VP of Global Customer Support	• Oversight and implementation, operation and monitoring of information security tools and processes in customer AWS environments • Execution of customer data retention and deletion processes
Systems Owners	• Manage the confidentiality, integrity and availability of the information systems for which they are responsible in compliance with nexelus.net policies on information security and privacy. • Approval of technical access and change requests for non-standard access
nexelus.net Employees, Contractors, temporary workers, etc.	• Acting at all times in a manner which does not place at risk the health and safety of themselves, other person in the workplace, and the information and resources they have use of • Helping to identify areas where risk management practices should be adopted • Taking all practical steps to minimize nexelus.net's exposure to contractual and regulatory liability • Adhering to company policies and standards of conduct • Reporting incidents and observed anomalies or weaknesses
Chief Human Resources Officer	• Ensuring employees and contractors are qualified and competent for their roles • Ensuring appropriate testing and background checks are completed • Ensuring that employees and relevant contractors are presented with company policies and the Code of Conduct (CoC) • Ensuring that employee performance and adherence the CoC is periodically evaluated • Ensuring that employees receive appropriate security training

CFO	• Responsible for oversight over third-party risk management process • Responsible for review of vendor service contracts

Policy Compliance

The [role responsible for measuring compliance, e.g., IT Manager] will measure the compliance to this policy through various methods, including, but not limited to—reports, internal/external audits, and feedback to the policy owner. Exceptions to the policy must be approved by the [approver of exceptions to this policy, e.g., IT Manager] in advance. Non-compliance will be addressed with management and Human Resources and can result in 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]