Risk 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 define the methodology for assessing and managing nexelus.net's information security risks in order to achieve the company's business and information security objectives.

Scope

The risk assessment process may be applied to all business processes, information, information systems, networks, devices, and information processing facilities that are owned or used by nexelus.net applicants, employees, contractors, consultants, vendors, partners, and other users affiliated with nexelus.net, or others using or accessing nexelus.net networks and/or information systems.

Policy

nexelus.net will ensure that risk management plays an integral part in the governance and management of the organization at a strategic and operational level. The purpose of a risk management policy is designed to ensure that the company achieves its stated business and security goals and objectives.

Risk Management Strategy

nexelus.net has developed processes to identify those risks that would hinder the achievement of its strategic and operational objectives. nexelus.net will therefore ensure that it has in place the means to identify, analyze, control, and monitor the strategic and operational risks it faces using this risk management policy based on best practices.

The IT Manager will ensure the risk management strategy and policy are reviewed regularly and that:

- The risk management policy is applied to relevant areas at nexelus.net
- The risk management policy and its operational application are annually reviewed
- Non-compliance is reported to appropriate company officers and authorities

Practical Application of Risk Management

nexelus.net may use a variety of risk reporting formats for the identification of risks, their classification, and evaluation based on factors such as vendors utilized, methodology employed, and the scope of the assessment. In general, and where possible, risks shall be assessed and ranked according to their impact and their likelihood of occurrence. A formal IT risk assessment, network penetration tests, and nexelus.net production application penetration test will be performed at least [frequency of penetration testing, e.g., annually].

In addition, an internal audit of the information security management system (ISMS) (i.e., information security controls and management processes) shall be performed at least annually.

Security risks shall be evaluated at various stages of the software design and development lifecycle as needed.

Risk Categories

Some risks are within the control of nexelus.net while others may be only to a lesser degree. nexelus.net will consider the risks within each of the following categories:

- Technical
- Reputational
- Contractual
- Economic/Financial
- Regulatory/Compliance
- Fraud

Each identified risk will be assessed as to its likelihood and impact. Likelihood can be assessed as not likely, somewhat likely, or very likely. Impact can be assessed as not impactful, somewhat impactful, and very impactful. The likelihood and impact will be considered together to formulate an overall risk ranking.

Risk Criteria

The criteria for determining risk is the combined likelihood and impact of an event adversely affecting the confidentiality, availability, integrity, or privacy of customer data, personally identifiable information (PII), or business critical systems.

For all risk inputs such as risk assessments, penetration tests, vulnerability scans, etc., nexelus.net management shall reserve the right to modify automated or third-party provided risk rankings based on its assessment of the nature and criticality of the system processing, as well as the nature, criticality and exploitability (or other relevant factors and considerations) of the identified vulnerability.

Risk Response and Treatment

Risks will be prioritized and mapped using the approach contained in this policy. The following responses to risk should be employed. Where nexelus.net chooses a risk response other than "Accept," it shall develop a Risk Treatment Plan.

- Mitigate: nexelus.net may take actions or employ strategies to reduce the risk.
- Accept: nexelus.net may decide to accept and monitor the risk at the present time. This may be necessary for some risks that arise from external events.
- Transfer: nexelus.net may decide to pass the risk on to another party. For example, contractual terms may be agreed to ensure that the risk is not borne by nexelus.net, or insurance may be appropriate for protection against financial loss.
- Eliminate: The risk may be such that nexelus.net could decide to cease the activity or to change it in such a way as to end the risk.

Risk Management Procedure

The procedure for managing risk will meet the following criteria:

- nexelus.net will maintain a Risk Register and Treatment Plan.
- Risks shall be ranked by ‘likelihood' and ‘severity/impact' as critical, high, medium, low, or negligible.
- Overall risk shall be determined through a combination of likelihood and impact.
- Risks may be valuated to estimate potential monetary loss where practical, or may be considered relative to a control objective
- nexelus.net will respond to risks in a prioritized fashion. Remediation priority will consider the risk likelihood and impact, cost, work effort, and availability of resources. Multiple remediations may be undertaken simultaneously.
- Periodic reports will be made to the senior leadership of nexelus.net to ensure risks are being mitigated appropriately, and in accordance with business priorities and objectives.

Risk Acceptance Levels

Role	**Responsibility**
CEO	Ultimately responsible party for the acceptance and/or treatment of any risks to the organization.
VP of Engineering	Can approve the avoidance, remediation, transference, or acceptance of any risk cited in the Risk Register. This person shall be responsible for communicating risks to top management and the board and adopting risk treatments in accordance with executive direction.
IT Manager	Shall be responsible for adherence to this policy.

Amendment & Termination of this Policy

nexelus.net reserves the right to modify, amend or terminate this policy at any time.

Exceptions

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

Violations & Enforcement

Any known violations of this policy should be reported to the [recipient of reports of violations of this policy, e.g., IT Manager]. 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]

Appendix A: Risk Assessment Matrix and Description Key

	RISK **= LIKELIHOOD * IMPACT**	**LIKELIHOOD**		
Very likely: **3**	**Somewhat likely:** **2**	**Not likely:** **1**		
IMPACT	**Very impactful: 3**	9	6	3
Somewhat impactful: 2	6	4	2	
Not impactful: 1	3	2	1	

RISK LEVEL	**RISK DESCRIPTION**
Low (1-2)	A threat event could be expected to have a limited adverse effect on organizational operations, mission capabilities, assets, individuals, customers or other organizations.
Moderate (3-6)	A threat event could be expected to have a serious adverse effect on organizational operations, mission capabilities, assets, individuals, customers or other organizations
High (7-9)	A threat event could be expected to have a severe adverse effect on organizational operations, mission capabilities, assets, individuals, customers or other organizations.

IMPACT LEVEL	IMPACT DESCRIPTION
Not impactful (1)	A threat event could be expected to have a limited adverse effect, meaning: degradation of mission capability yet primary functions can still be performed; minor damage; minor financial loss; or range of effects is limited to some cyber resources but no critical resources.
Somewhat impactful (2)	A threat event could be expected to have a serious adverse effect, meaning: significant degradation of mission capability yet primary functions can still be performed at a reduced capacity; minor damage; minor financial loss; or range of effects is significant to some cyber resources and some critical resources.
Very impactful (3)	A threat event could be expected to have a severe or catastrophic adverse effect, meaning: severe degradation or loss of mission capability and one or more primary functions cannot be performed; major damage; major financial loss; or range of effects is extensive to most cyber resources and most critical resources.

LIKELIHOOD LEVEL	LIKELIHOOD DESCRIPTION
Not likely (1)	Adversary is unlikely to initiate a threat event; non-adversarial threat event (e.g., nature, error, accident) is unlikely to occur; or threat is unlikely to have adverse impacts.
Somewhat likely (2)	Adversary is somewhat unlikely to initiate a threat event; non-adversarial threat event (e.g., nature, error, accident) is somewhat unlikely to occur; or threat is somewhat unlikely to have adverse impacts.
Very likely (3)	Adversary is highly likely to initiate a threat event; non-adversarial threat event (e.g., nature, error, accident) is highly likely to occur; or threat is highly likely to have adverse impacts.