Secure Development 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 that information security is designed and implemented within the development lifecycle for applications and information systems.

# Scope

All nexelus.net applications and information systems that are business critical and/or process, store, or transmit Confidential data. This policy applies to all internal and external engineers and developers of nexelus.net software and infrastructure.

# Policy

This policy describes the rules for the acquisition and development of software and systems that shall be applied to developments within the nexelus.net organization.

## System Change Control Procedures

Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures. Change control procedures and requirements are described in the nexelus.net Operations Security Policy.

Significant code changes must be reviewed and approved by [who can approve code changes, e.g., a developer or manager within the Review Board] before being merged into any production branch in accordance with the [name of process, e.g., Check In Process] found here: [link to process outline in company wiki]

## Software Version Control

All nexelus.net software is version controlled and synced between contributors (developers). Access to the central repository is restricted based on an employee's role. All code is written, tested, and saved in a local repository before being synced to the origin repository.

## Technical Review of Applications after Operating Platform Changes

When operating platforms are changed, business critical applications shall be reviewed and tested to ensure that there is no adverse impact on organizational operations or security.

## Restrictions on Changes to Software Packages

Modifications to third-party business application packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

## Secure System Engineering Principles

Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

Engineering style guides and technical references can be found in the [name of page with documents, e.g., Development Process Confluence Page] here: [link]

Software developers are expected to adhere to nexelus.net's coding standards throughout the development cycle, including standards for quality, commenting, and security.

## Secure Development Environment

nexelus.net shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life cycle.

## Outsourced Development

nexelus.net shall supervise and monitor the activity of outsourced system development. Outsourced development shall adhere to all nexelus.net standards and policies.

## System Security Testing

Testing of security functionality shall be carried out during development. No code shall be deployed to nexelus.net production systems without documented, successful test results.

## System Acceptance Testing

Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.

Prior to deploying code, a Release Checklist MUST be completed which includes a checklist of all Test Plans which show the completion of all associated tests.

## Protection of Test Data

Test data shall be selected carefully, protected and controlled. Confidential customer data shall be protected in accordance with all contracts and commitments. Customer data shall not be used for testing purposes without the explicit permission of the data owner and the [approver of use of customer data as test data, e.g., VP of Engineering].

## Acquisition of Third-Party Systems and Software

The acquisition of third-party systems and software shall be done in accordance with the requirements of the nexelus.net Third-Party Management Policy.

## Exceptions

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

## Violations & Enforcement

Any known violations of this policy should be reported to the [receiver of reported violations to this policy, e.g., VP of Engineering]. 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] |
|  |  |  |  |  |