1. Policy Overview

This policy establishes the framework for managing vulnerabilities within **Log(N) Pacific,** IT infrastructure to ensure the security and integrity of our systems through timely and effective identification, evaluation, and remediation of threats.

2. Scope

This policy applies to all IT assets owned or operated by **Log(N) Pacific,** including networks, servers, endpoints, and associated applications.

3. Responsibilities

- Chief Information Security Officer (CISO): Oversight of the vulnerability management process and ensuring compliance with this policy.
- Chief Information Officer (CIO): Ensuring that vulnerability management is integrated with **[Log(N) Pacific 's** overall IT strategy.
- Department Heads: Responsible for ensuring compliance within their respective departments.

4. Vulnerability Scan Schedule

- Routine Scans: Conduct monthly scans of all IT assets to identify vulnerabilities.
- Ad-Hoc Scans: Perform scans in response to significant security alerts or when new vulnerabilities are reported.

5. Remediation Schedule and Cadence

Based on the Common Vulnerability Scoring System (CVSS):

- Critical (CVSS 9.0-10): Remediate or mitigate within 48 hours.
- High (CVSS 7.0-8.9): Remediate or mitigate within 7 days.
- Medium (CVSS 4.0-6.9): Remediate or mitigate within 30 days.
- Low (CVSS 0.1-3.9): Remediate or mitigate within 90 days.

6. Maintenance Plans

- Routine Patching: Apply security patches and updates on a scheduled monthly basis.
- Emergency Patching: Initiate within 24 hours for critical vulnerabilities that pose immediate risks.
- Emergency Mitigation: Implement temporary measures (e.g., firewall rules, access restrictions) to protect against vulnerabilities while permanent solutions are developed.
- Uncatchable Assets: Implement segmentation, increased monitoring, or phased removal from the environment.

7. Non-Compliance Consequences

Departments failing to comply with this policy will face:

- Immediate review of their procedures.
- Mandatory retraining for involved personnel.
- Escalation to senior management for further disciplinary actions including termination

8. Sign-Off

Chief Information Security Officer (CISO)

Sign: _____

Date: _____

Chief Information Officer (CIO)

Sign: _____

Date: _____

Chief Executive Officer (CEO)

Sign: _____

Date: _____

9. Review and Revision

This policy will be reviewed annually or sooner if necessary to accommodate changes in business processes or to address emerging threats.

Document Control

- Version: 1.0
- Date: 1/12/26
- Author: Junist Aurelien