Vulnerability Management Policy: Production

1. Policy Overview

This policy outlines the framework for identifying, assessing, and addressing security vulnerabilities within **LogN Pacific's IT environment**. The goal is to maintain the confidentiality, integrity, and availability of systems by ensuring threats are handled in a timely and effective manner.

2. Scope

This policy applies to **all IT assets** managed by LogN Pacific, including:

- Networks
- Servers
- Endpoints
- Business-critical applications

3. Roles and Responsibilities

- **Chief Information Security Officer (CISO):** Provides oversight of the vulnerability management program and ensures overall compliance.
- **Chief Information Officer (CIO):** Ensures vulnerability management aligns with LogN Pacific's broader IT strategy.
- **Department Heads:** Ensure their teams follow this policy and meet remediation requirements.

4. Vulnerability Scan Schedule

- **Routine Scans:** Conducted monthly across all IT assets to detect potential risks.
- **Ad-Hoc Scans:** Performed in response to significant security advisories, major incidents, or newly disclosed vulnerabilities.
- **Workstations:** Local agents are deployed to monitor end-user devices for vulnerabilities.

5. Remediation Timelines (Based on CVSS)

- **Critical Zero-Day RCE (CVSS 9.0–10):** Remediation or mitigation within **48 hours**.
- **Critical (CVSS 9.0–10):** Remediation or mitigation within **7 days**.
- **High (CVSS 7.0–8.9):** Remediation or mitigation within **14 days**.
- **Medium (CVSS 4.0–6.9):** Remediation or mitigation within **30 days**.
- **Low (CVSS 0.1–3.9):** Remediation or mitigation within **90 days**.

6. Maintenance and Patching

- **Scheduled Patching:** Monthly security updates applied across systems.
- **Emergency Patching:** Critical fixes deployed within **24 hours** of discovery.
- **Temporary Mitigations:** Short-term safeguards (firewall rules, access restrictions, etc.) used when permanent fixes are not immediately available.
- **Unpatchable Assets:** Must be segmented, closely monitored, or gradually decommissioned.

7. Non-Compliance

Departments failing to comply with this policy may face:

- Immediate review of their vulnerability management practices.
- Mandatory retraining of affected personnel.

- Escalation to senior leadership for possible disciplinary action, up to and including termination.

8. Approval and Sign-Off

- **Chief Information Security Officer (CISO)**
    - *Signed:* Sandra Liu – 22 May 2024
- **Chief Information Officer (CIO)**
    - *Signed:* Fred Smooch – 24 May 2024
- **Chief Executive Officer (CEO)**
    - *Signed:* Bruce Thornton – 23 May 2024

9. Review and Updates

This policy will be reviewed annually, or earlier if required by changes in operations, business processes, or the evolving threat landscape.

Document Control:

- **Version:** 1.1
- **Date:** 26 Jan 2025
- **Author:** Bruce Thornton