Newspeak Technologies Vulnerability Management Policy

1. Policy Overview

This policy establishes the framework for managing vulnerabilities within **Newspeak Technologies** IT infrastructure, ensuring the security, integrity, and availability of our systems. It provides a structured approach to the timely identification, assessment, and remediation of vulnerabilities, aiming to reduce security risks and protect the organization's information assets.

2. Scope

This policy applies to all IT assets owned or operated by **Newspeak Technologies**, including networks, servers, endpoints, laptops, mobile devices, databases, applications, cloud resources, and network-connected peripherals. It encompasses both on-premises and cloud environments.

3. Responsibilities

- **Chief Information Security Officer (CISO):** Provides overall oversight of the vulnerability management program and ensures compliance with this policy.
- **Chief Information Officer (CIO):** Ensures that vulnerability management activities are aligned with **Newspeak Technologies** overall IT strategy and objectives.
- **Department Heads:** Accountable for enforcing compliance with this policy within their respective departments and supporting remediation efforts as needed.

4. Vulnerability Scan Schedule

- **Routine Scans:** Conduct monthly vulnerability scans across all IT assets to proactively identify security weaknesses.
- **Ad-Hoc Scans:** Perform additional scans in response to significant security alerts, emerging threats, or newly disclosed vulnerabilities to ensure timely detection and remediation.
- **Local Agent:** Used for vulnerability assessments on end-user workstations.

5. Remediation Schedule and Cadence

Vulnerabilities are prioritized and remediated based on the **Common Vulnerability Scoring System (CVSS)**:

- **Critical RCE ZERO DAY (CVSS 9.0-10):** Remediate or mitigate within **48 hours**.
- **Critical (CVSS 9.0-10.0):** Remediate or mitigate within **7 days**.
- **High (CVSS 7.0-8.9):** Remediate or mitigate within **14 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**.

This schedule ensures timely mitigation of the most severe vulnerabilities while maintaining a structured approach to overall risk reduction.

6. Maintenance Plans

- **Routine Patching:** Apply security patches and updates on a scheduled monthly basis to maintain system integrity.
- **Emergency Patching:** Deploy patches within **24 hours** for critical vulnerabilities that pose immediate risks.
- **Emergency Mitigation:** Implement temporary controls, such as firewall rules or access restrictions, to protect vulnerable assets while permanent solutions are developed.
- **Unpatchable Assets:** Apply compensating controls, including network segmentation, enhanced monitoring, or phased removal from the environment, to reduce risk exposure.

7. Non-Compliance Consequences

Departments or personnel that fail to comply with this policy will be subject to the following actions:

1. **Immediate Review:** Assessment of departmental procedures and processes to identify gaps.
2. **Mandatory Retraining:** Required training for all involved personnel to ensure understanding and adherence to policy requirements.
3. **Escalation:** Referral to senior management for further disciplinary measures, which may include formal warnings or termination, depending on the severity and impact of non-compliance.

8. Review and Updates

This policy will be reviewed at least **annually** or whenever significant changes occur in the IT environment, technology stack, or regulatory requirements. Updates and revisions will be communicated to all relevant stakeholders to ensure continued compliance and effectiveness of the vulnerability management program.

9. Sign-Off

Chief Information Security Officer (CISO)

Sign: *O'Brien*

Date: **April 4, 1984**

Chief Information Officer (CIO)

Sign: *Julia*

Date: **April 4, 1984**

Chief Executive Officer (CEO)

Sign: *WinstonSmith*

Date: **April 4, 1984**

Document Control

All changes to this policy will be recorded and tracked under the organization's document control procedures. Version history, review dates, and approval records will be maintained to ensure accountability and compliance.

- Version: 1.1
- Date: January 1st, 2000
- Author: Danny Cologero