“Vulnerability and Patch Management Policy”

Company: DAS TECHNOLOGY SERVICES LLC
Document Owner: IT Department (Shaheer Nawaz)
Approved by: CEO
Review Frequency: Annual or upon significant infrastructure change

---

1. Purpose

This document outlines the organization’s approach to managing system vulnerabilities and ensuring timely application of patches to minimize security risks and maintain system integrity.

---

2. Scope

This policy applies to all:

- Company-owned systems including servers, laptops, mobile devices, and networking equipment
- Cloud environments and third-party hosted services
- Employees, contractors, and vendors with system access

---

3. Policy Guidelines

3.1 Vulnerability Detection

- Conduct automated vulnerability scans monthly using approved tools (e.g., Nessus, Qualys).
- Trigger immediate scans following major deployments, configuration changes, or security alerts.

3.2 Risk Assessment

- Use CVSS scores to categorize vulnerabilities:
    - **Critical (G.0–10.0):** Address within 48 hours
    - **High (7.0–8.G):** Address within 5 business days

- **Medium (4.0–6.G):** Address within 15 business days
- **Low (0.1–3.G):** Schedule based on resource availability and risk

3.3 Patch Implementation

- Apply patches and updates through automated systems wherever possible.
- Prioritize patches based on risk to business operations.
- Maintain testing procedures and rollback mechanisms to ensure stability.
- Document all patch deployments including systems impacted, dates, and outcomes.

3.4 Exceptions

- Any delay in remediation must be formally documented and approved.
- Implement temporary mitigation strategies if immediate patching is not feasible.

---

4. Roles s Responsibilities

Role	Responsibility
IT Security Team	Scan coordination, threat validation
System Admins	Patch application, testing, and verification
App Owners	Assist with compatibility and business impact
Compliance Officer	Policy enforcement and audit readiness

---

5. Monitoring and Reporting

- Maintain logs of vulnerabilities, patches, exceptions, and related actions.
- Submit monthly security and patch status reports to the executive team.
- Track progress against remediation timelines.

---

6. Enforcement

Non-compliance with this policy may result in disciplinary actions and potential legal consequences. This policy is binding for all employees and associated parties.

---

7. Review s Maintenance

This policy will be reviewed annually by the IT Security Department or sooner if there are significant changes in the threat landscape or operational environment.
