Vulnerability Management Process

BITS Technology Group Pty Ltd

Action	Name	Title
Prepared By	Muhammad Nauman Mustafa	Cyber Security Engineer
Reviewed By	Blair Munro	Head of Technology
Approved By	Bernard Mangelsdorf	Chief Executive Officer

Version	Date	Description of Change	Updated By
1.0	12 March 2025	Initial Policy Creation	Muhammad

1. Purpose

The purpose of this policy is to establish a comprehensive and systematic approach to identifying, assessing, and mitigating security vulnerabilities within the IT infrastructure of BITS. This policy aims to protect assets, ensure compliance with relevant regulations, and maintain the integrity and availability of systems.

2. Scope

This policy applies to all employees, contractors, and third-party vendors involved in the management and maintenance of the IT environments. It covers all hardware, software, network configurations, and personnel.

3. Definitions

- **Vulnerability:** A weakness in a system, application, or network that can be exploited by a threat actor.
- **Vulnerability Management:** The process of identifying, assessing, prioritizing, and mitigating vulnerabilities.

4. Roles and Responsibilities

Vulnerability Management Team:

- Consists of the Head of Technology, the Cyber Security Engineer and the IT Development and Operations Engineer.
- Responsible for the overall management of the vulnerability management process, including scanning, assessment, and remediation.
- Assist in the implementation of remediation actions and ensure systems are configured securely.
- Ensure that vulnerability management practices comply with relevant regulations and standards.

5. Vulnerability Management Process

5.1 Identification and Scanning

- Conduct regular vulnerability scans using automated tool named Connect Secure (Cyber CNS) vulnerability scanner to identify potential vulnerabilities in systems.
- Perform manual assessments as needed to complement automated scans, where required. The critical vulnerabilities identified will be emailed to the vulnerability management team.
- Maintain an inventory of all assets to ensure comprehensive scanning coverage.

5.2 Assessment and Prioritization

- Assess identified vulnerabilities based on their severity, potential impact on operations, and exploitability.
- Use Cyber CNS's vulnerability grading system to prioritize vulnerabilities that pose the highest risk.

5.3 Remediation

- Develop and implement remediation plans for identified vulnerabilities based on their priority level.

- Apply patches, configuration changes, or other mitigation measures to address vulnerabilities.
    - The security patches for the OS will be deployed automatically.
    - The patches for the installed applications will be deployed automatically.

5.4 Continuous Improvement

- The leadership team will annually review and update the vulnerability management process to incorporate new best practices and address emerging threats.
- Conduct periodic training for relevant staff to ensure they are aware of the latest vulnerability management techniques and tools.
- The leadership team will solicit feedback from the team to improve the effectiveness of the vulnerability management program.

6. Compliance and Enforcement

- Ensure compliance with relevant regulations and standards, such as SMB1001 Diamond and ISO 27001.
- Conduct regular audits to verify adherence to this policy.

7. Review and Revision

This policy will be reviewed annually and updated as necessary to reflect changes in technology, threat landscape, and regulatory requirements.