NetGain systems	No of Pages	**1** of **5**
	Document Classification:	Internal
	Effective Date	1 Aug 2025
MANAGEMENT OF TECHNICAL VULNERABILITIES	Doc No	ISMS-TECH-03
	Revision	1.0

AMENDMENTS LOG

Revision History

Version	Revision Author	Reviewer / Approver	Date	Summary of Changes
1.0	Nor Asfiah Binte Jamalludin (ISMS MR)	James Chia (CEO)	1 Aug 2025	Initial Release

TABLE OF CONTENTS

PURPOSE **3**

SCOPE **3**

REFERENCE **3**

RESPONSIBILITIES & AUTHORITIES **3**

PROCEDURE **3**

A. IDENTIFICATION OF TECHNICAL VULNERABILITIES 3
B. ASSESSMENT, PRIORITIZATION AND RISK-BASED TREATMENT 3
C. REMEDIATION AND MITIGATION MEASURES 4
D. EXCEPTIONS 4
E. VERIFICATION 5

FORM **5**

PURPOSE

This document sets out the need to identify existing vulnerabilities in information systems that could be exploited by an attacker. These could include known software vulnerabilities that have not been patched, configuration errors that need to be corrected or examples of inadequate security practice that need to be addressed.

SCOPE

This control covers all information systems in use within the organisation.

REFERENCE

ISO/IEC 27001 Standard	Annex A 8.8 Management of technical vulnerabilities

RESPONSIBILITIES & AUTHORITIES

Top Management has the prime responsibility and approval authority for this control.

The MR shall ensure that vulnerability findings are reported, tagged, and tracked to resolution in accordance with the SLAs defined herein.

PROCEDURE

A. Identification of Technical Vulnerabilities

The company shall identify relevant technical vulnerabilities through the following:

- Threat intelligence and vendor updates: Subscribe to and monitor trusted security advisories, and vendor notifications for systems and software used in the development and delivery of services.
- Vulnerability and Security Assessments: Perform vulnerability and security assessments at least annually, or upon significant system changes.

B. Assessment, Prioritization and Risk-Based Treatment

All identified vulnerabilities are reviewed and assigned a risk rating and priority level based on the following:

Priority Level	SLA	Definition	Examples
Critical and High	Within 30 days	Vulnerabilities with potential for privilege escalation, remote code execution, data exfiltration, or service disruption	RCE, SQL Injection, Auth Bypass, SSRF, XXE
Medium	Within 90 days	Exploits that affect multiple users, have lower impact, or require user interaction	Reflected XSS, Insecure Direct Object Reference
Low	As determined by management	Low-impact issues requiring specific user actions or unlikely scenarios	Information disclosure, Mixed content, Debug artifacts

C. Remediation and Mitigation Measures

Upon classification, vulnerabilities shall be addressed by one or more of the following:

- Applying validated patches from legitimate sources.
- Disabling affected services or features.
- Implementing compensating controls, such as:
  - Enhanced access controls
  - Web application firewalls (WAF)
  - Input validation or code-level mitigations
- Monitoring for exploitation attempts using observability tools and SIEM solutions.

Remediation actions must be tested in staging environments where applicable before production deployment.

D. Exceptions

Exceptions to the SLA or standard remediation process may be requested if:

- A patch or fix is not available or cannot be applied (e.g., compatibility issues).
- The asset is scheduled for decommissioning.
- Mitigation measures provide sufficient risk reduction.

Requirements for exception approval:

- A documented compensating control that reduces risk to an acceptable level.
- Formal risk acceptance by the risk owner and top management.
- Periodic review (at least annually) of approved exceptions.

E. Verification

Once the vulnerabilities have been addressed, a re-test will be arranged after implementation of the remediation plans to ensure that the same vulnerabilities do not resurface and remediations taken are effective.

Remediation, any exceptions, and verification shall be recorded in the Vulnerability Action Plan.

FORM

ISMS-TECH-03-F1	Vulnerability Action Plan