NetGain systems	No of Pages	**1** of **5**
	Document Classification:	Internal
	Effective Date	1 Aug 2025
USER ENDPOINT DEVICES	Doc No	ISMS-TECH-01
	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

The document sets out the controls to protect information against the risks introduced by using user endpoint devices.

SCOPE

This control applies to user endpoint devices including items such as laptops.

REFERENCE

ISO/IEC 27001 Standard	Annex A 8.1 User endpoint devices Annex A 8.23 Web filtering

RESPONSIBILITIES & AUTHORITIES

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

The MR shall ensure that this control is implemented for all user endpoint devices.

PROCEDURE

A. Company-Issued User Device

All user endpoint devices must be kept up to date with the latest security updates and patches. Devices that are no longer capable of receiving regular security updates must not be used and must be promptly replaced to maintain security compliance.

For company-issued devices, the following baseline security and configuration controls must be implemented. These controls are managed by IT and cannot be altered or bypassed by users:

- Creation of a unique employee user account
- Device lock and user authentication
- Enforcement of complex password policies and multi-factor authentication (where applicable)
- Automatic screen lock after 10 minutes of inactivity
- Configuration for secure access to the office Wi-Fi network
- Enabling the device firewall
- Activating web content filtering
- Installation and enforcement of anti-malware software
- Automated operating system patch management
- Automatic scanning of removable media when plugged in

- Clock synchronization with network or standard time sources
- Installation of approved software/applications based on user role
- Access provisioning to business systems based on role-based permissions
- Implementation of backup arrangements as required
- Full disk encryption or secure storage encryption

All users must formally acknowledge and comply with the organisation’s Acceptable Use Policy and related security policies as a condition of using company devices.

B. Use of Personal Devices

Use of personal devices for work purposes is permitted only with prior approval and is subject to the organisation’s Access Control Policy and security requirements. Approved personal devices must meet baseline security standards to protect organisational data and systems.

Employees authorised to use personal devices must ensure the following controls are in place:

- A strong password or equivalent secure authentication method must be configured in line with the organisation’s Password Policy.
- The device must be regularly updated and capable of receiving current security patches.
- Anti-malware protection must be enabled and up to date.
- An automatic screen lock must activate after 5 minutes of inactivity.
- Where technically feasible, device encryption should be enabled.

Employees using personal devices for work-related access are responsible for:

- Immediately reporting any suspected unauthorised access or data breach involving the personal device to MR/IT.
- Promptly reporting lost or stolen personal devices used to access organisational systems or data.
- Complying with the organisation’s Acceptable Use Policy and all applicable information security policies when accessing organisational information on a personal device.

C. Web Filtering

The organisation enforces web filtering through Microsoft Defender for Endpoint to prevent access to inappropriate, harmful, or non-business-related web content. As the office operates in a shared network environment not controlled by the organisation, web filtering is applied directly at the device level using Defender’s built-in capabilities.

Web content filtering is managed through policies configured in Microsoft Defender. These policies restrict access to high-risk or non-business-related categories, such as adult content, gambling, malware, phishing, and other security threats.

The underlying list of URLs and domains within each blocked category is continuously updated by Microsoft’s threat intelligence. As new threats or inappropriate websites emerge, Defender automatically blocks access if they fall under a restricted category. If there is a need to manually block a specific site or content type not covered by existing categories, administrators can configure custom rules directly via the Microsoft 365 Defender portal.