

Configuration Standards

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	2 April 2025	Initial policy creation	Muhammad
2.0	23 April 2025	Updated 7. Microsoft 365 Environment	Esther Mangelsdorf

1. Purpose

The purpose of this policy is to establish standard configuration requirements for all IT systems and devices within BITS Technology Group to ensure compliance with ISO 27001 standards. This policy aims to minimise security risks and ensure the integrity, confidentiality, and availability of information.

2. Scope

This policy applies to all employees, contractors, and third-party service providers who manage, configure, or maintain IT systems and devices for BITS Technology Group.

3. Definitions

- **Baseline Configuration:** A set of specifications for a system or device that has been formally reviewed and agreed upon, which serves as a basis for further development and can be changed only through formal change control procedures.
- **Configuration Management:** The process of maintaining the consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life.
- **Patch Management:** The process of managing a network of computers by regularly performing patch deployment to keep software up to date and secure from vulnerabilities.

4. Roles and Responsibilities

- **Head of Technology:** Responsible for approving baseline configurations, reviewing access logs, and ensuring compliance with this policy.
- **System Administrators:** Responsible for applying patches and performing backups.
- **Cyber Security Engineer:** Responsible for implementing and maintaining baseline configurations.
- **Employees and Contractors:** Responsible for adhering to this policy and reporting any security incidents or deviations from baseline configurations.

5. Workstation Configurations

These controls are designed to ensure consistent service delivery, minimise security risks, and maintain compliance with industry best practices.

The following security tools should be deployed on all workstations:

- NinjaRMM
- Augmentt Discover
- Cisco Umbrella
- Microsoft Defender for Endpoint
- Huntress EDR
- ConnectSecure Vulnerability Scanner

Initial Setup:

- All workstations must be enrolled in Entra ID and Intune
- Intune must automatically deploy NinjaRMM as part of the initial device setup

- Base image must include all security agents: Defender for Endpoint, Huntress EDR, Cisco Umbrella agent
- SaaS application discovery must be enabled via Augmentt Discover
- Local administrator accounts must only be deployed and managed using Microsoft LAPS.

Configuration Management

- All workstations must follow the principle of least privilege
- Local administrator rights must not be granted to standard users
- Application inventory must be maintained through NinjaRMM and Augmentt Discover

The patch management of OS and applications will be performed in line with the Vulnerability management policy.

6. Network Device Policy

Initial Setup

- All network devices must be documented in NinjaRMM
- SNMP must be configured for monitoring where applicable
- Network topology must be documented and kept current

Firmware Updates

- The firmware update must be implemented within the next maintenance period (weekly)
- Update history must be documented

7. Microsoft 365 Environment

The M365 environment should be maintained at minimum as the BITS baseline security configuration policy known as 'Low impact - Baseline Policy' with advance security configurations implemented as deemed necessary. These policies are stipulated and maintained in the tool Inforcer. The M365 configurations should also be backed up using Inforcer.

8. Compliance

This policy must be readily available to all employees. It will be accessible through the company's document management portal, employee handbook, and during onboarding sessions.

Employees are encouraged to review the policy regularly and stay informed about any updates as compliance to this policy is mandatory.

9. Review and Revision

This policy will be reviewed annually or whenever significant changes occur to ensure its continued relevance and effectiveness.