SNOWBE ONLINE Policy# SI-7
Endpoint Security

Humberto Gonzalez

Version # 1.0

July 5,2024

Table of Contents

Purpose

The purpose of this policy is to regulate protection of the SnowBe Online network when accessed by “Endpoint” equipment (e.g., such as desktop computers, laptops, tablets, mobile devices or similar).

Scope

This policy covers all Endpoint devices connected to the SnowBe Online network environment.

Definitions

DMZ- DMZ or demilitarized zone is a physical or logical Firewalled network that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. It provides an additional layer of separation between the Internet and the Massey internal network, thereby adding an extra layer of protection.

Endpoint- An electronic device connected to the IT infrastructure that generates or terminates an electronic information stream. These could be computers, servers, tablets, mobile devices, or any similar network enabled device.

Endpoint device management software- Refers to the necessary management software required to audit and review application software versions and license numbers, and manage software installations (where required) on an Endpoint device. This includes Microsoft System Centre Configuration Manager, Casper, and Active Directory services. Refer to the Active Directory Domain Policy for more information.

Firewall- An application running on a device designed to protect and control network traffic to and from the device.

Least Privilege- In information security, this principle requires that in a particular layer of a computing environment, every module (such as a process, a user, a device, or a program depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose (e.g., to perform their role, while at the same time not impacting on academic freedom).

Malware- Programming code, scripts, active content, and other software designed to disrupt, collect private information, or gain unauthorized access to system resources.

Network segmentation- SnowBe computer network is segmented into areas based on zones of trust. Placement in and access between devices located within these segments are based on the sensitivity of information assets within those segments and, and the applicable security controls on the devices in those segments. Sensitive or confidential information will be placed within the more secure network segments, and endpoints must meet stricter requirements to have access to the services within these sensitive zones.

SnowBe Online Network- The SnowBe Online computer network accessible by authorized staff, which is segmented and protected from the internet and other less trusted zones.

VPN- Or Virtual Private Network is a secure and encrypted connection between a remote client device and the internal Massey network. It acts to secure data transmitted over a typically insecure network (such as the internet) to a corporate (private) network.

Roles & Responsibilities

- Employees: Must follow security policies and procedures, attend security awareness training, and immediately report any security problems.

- IT Department: Responsible for overseeing the technical aspects of the security program, including the implementation and maintenance of security controls, system hardening, patch management, network security, and data protection through encryption and backups.

- Senior Management/Executive Team: Sets the tone and direction for information security, and assigns resources to secure information assets.

- Third-Party Vendors: Must comply with SnowBe Online security criteria, safeguard the security of data and systems that interact with SnowBe Online.

Policy

All endpoints must have up-to-date antivirus software, regular security patches, and encryption enabled. Unauthorized software installation is prohibited, and all devices must be configured to lock automatically after a period of inactivity.

Endpoint software Operating Systems (OS) and application software are to be kept up to date with the latest security related patches, as soon as it is practical to do so, i.e.:

Critical security patches are applied within 1 week of them being released by vendors.

Important security patches are applied within 8 weeks of them being released vendors.

Endpoint systems must be restarted following installation, to ensure security patches have been fully installed.

Where possible, it is recommended that Endpoint devices are set to auto-update their security patch levels, and restart if necessary to complete the installation.

- OS that reach end of support life are by default not permitted to connect to the SnowBe Online network. This is because security patches are no longer provided by vendors and this poses a growing security threat to the environment over time. If a special exemption is required, this must be requested formally via the IT department (refer below for contact details) and approved by the CIO.

- IT department will install Endpoint device management software, as required, on any Endpoint connected to the SnowBe Online network in order to manage SnowBe policy, legal, and commercial compliance requirements.

- The removing or disabling of Endpoint device management software without prior approval of IT department is considered a breach of this policy.

- IT department will audit SnowBe owned Endpoint devices on the SnowBe Domain as required, and has the ability to install updates to software on these devices to address software vulnerabilities or licensing issues with IT department managed software.

- Departments who choose to operate and manage their own specific software on Endpoint devices accept responsibility for the associated licensing, installation, updates, and security as it relates this software, in accordance with this policy.

Administrative Access

- In accordance with the principle of least privilege, unnecessary administrative access on SnowBe Online owned Endpoint devices will be restricted.

Authentication

- Endpoint devices containing SnowBe Online information assets that are not publicly available, or devices which attach to SnowBe's network, must be secured as appropriate by a network or locally based user code and password or a PIN.

Antivirus Software & Firewalls

- All Endpoint devices capable of running an antivirus software program are required to do so before being connecting to the SnowBe Online network. Additionally, any such antivirus software must be running the latest virus definitions to accurately detect the latest viruses and malware, and be set to automatically update when newer definitions become available.

- Disabling or removing of Antivirus software, or disabling of Antivirus software definition updates on endpoints is prohibited.

- All Endpoint devices capable of running local Firewall software are required to do so to protect the device from external threats such as hacking by unauthorized parties.

Servers & Web Applications

- All Servers (or devices exposed to the internet, in the DMZ, or running web services), will be ‘hardened’, meaning they will have all the necessary security updates applied to their Operating System’s, hardware patches (firmware updates), and installed software; to reduce the chances of vulnerabilities being exploited. All such updates must be reviewed and maintained regularly to ensure they remain up to date. It is the Server Administrator’s responsibility to manage this.

- New Services that are externally (internet) facing will require independent security vulnerability and penetration testing to be performed by a security specialist prior to implementation, and subsequently added to the IT Security Review Schedule, to provide assurance that data or services won’t be exposed to medium or high risk security threats.

Network Segmentation

- Endpoint devices will be attached to SnowBe’s network within the appropriate network segment as determined by applicable Endpoint security controls.

Personal devices

- Personal devices (i.e., those not purchased or owned by SnowBe Online) that are authorized to connect to the SnowBe Online network remain the responsibility of the owner, and must comply with this policy.

Exceptions/Exemptions

In circumstances where regular security standards cannot be followed, exceptions or exemptions may be requested. To request an exception or exemption, the requester must send a formal written request to the IT department, outlining the precise security protocol that cannot be followed and the justification for the request. The request should include a reason for why the exception or exemption is required, the potential impact on security, and any proposed compensatory controls. The Chief Information Officer (CIO) or a designated senior IT executive has the power to approve or reject such requests. Approved exceptions or prohibitions will be provided for a brief period not exceeding one year unless otherwise justified. The requester must make certain that the exception or exemption is reviewed and re-evaluated before the end of the permitted term.

Enforcement

All SnowBe Online employees, contractors, and third-party entities must comply with this security policy. Failure to follow the policies and procedures outlined will result in disciplinary action, which may include verbal or written warnings for minor infractions, temporary suspension from duty for repeated or serious violations, and termination of employment for severe or repeated noncompliance. If noncompliance results in legal consequences or financial loss for SnowBe Online, the company has the right to take legal action. Contractors and third-party entities that violate this security strategy may face contract termination and legal action, depending on the severity of the breach. All disciplinary actions will be carried out under SnowBe Online policy and any applicable labor laws. Each individual must understand and follow security policies to protect the company's information assets.

Version History Table

Version #	**Implementation Date**	**Document Owner**	**Approved By**	**Description**
1.0	07/05/24	Humberto Gonzalez	TBD	Initial Version

Citations

Endpoint Security Policy- Section (massey.ac.nz)

Exceptions/Exemptions- Sample Detailed Security Policy (bowiestate.edu)

Roles & Responsibilities- Sample Detailed Security Policy (bowiestate.edu)

Enforcement- Sample Detailed Security Policy (bowiestate.edu)