SNOWBE ONLINE Policy#SP-3 Mobile Device Management (MDM) Policy

Michael Kohronas:

<Mobile Device Management (MDM) Policy>

Version #3

DATE: 06/2024

<Mobile Device Management (MDM)> – V 3.0
Status: ☒ Working Draft ☐ Approved ☐ Adopted
Document owner: Michael Kohronas
DATE – 06/2024

Table of Contents

Policy

The purpose of the Mobile Device Management policy is to protect company data by ensuring safe use of our mobile devices. This aims to protect company data by securing mobile devices.

Scope

This policy applies to all staff, contractors, and interns who have access to SnowBe’s information via mobile devices. The data this serves to protect is data that is not publicly available that is being held by SnowBe.

Definitions

Acceptable use – The appropriate use of mobile devices and company recourses that may hold private data or run the needed software. Providing a standard of ways SnowBe’s information can be used.

Malware - Malicious software that is loaded onto your computer by a hacker with malicious intent.

Mobile Devices – Portable devices that refer to smartphones, tablets, and laptops that can be used to access SnowBe’s information, data, and network. These devices can connect to the internet and interact with SnowBe’s systems.

VPN – or Virtual Private Network is a secure connection that is encrypted between a remote client device and the internal network to SnowBe. This allows for data to be safely transferred from two different locations. Removing the need for insecure networks like the internet.

Roles & Responsibilities

All Employees, contractors, or interns – When using a device with any of SnowBe’s information on it employees must follow the MDM policy in place.

CISO – Oversee the development, implementation, and maintenance of the MDM policy.

IT Security team – Ensure all mobile devices are being used are following the MDM policy and resolve any misuse of machines.

Policy

The purpose of this Mobile Device Management (MDM) policy is to establish guidelines and procedures for the secure and responsible use of mobile devices within SnowBe

This mobile device policy applies to, but is not limited to, all the devices listed below:
- Smartphones
- Other mobile/cellular devices
- Tablets
- E-readers
- Portable media/gaming devices
- Laptop/notebook/Ultrabook computers
- Wearable computing devices
- Personal digital assistants (e.g. PDAs)
- Any other person device with SnowBe’s information

Acceptable use – Working on a personal mobile device is not permitted unless approved by the IT department. SnowBe assigned mobile device should be used for work purposes only.

Security requirements – All mobile devices must be protected with a strong password and biometric authentication as well. These devices should not be left unattended and should be locked after a period of activity. The device’s data should have encryption enabled.

Device Management – All mobile devices being used on SnowBe’s network must be enrolled into our MDM software.

Accessing companies’ information – Any private company information should only be viewed on a secure connection (VPN).

Exceptions/Exemptions

Exceptions to this Policy will be considered on a case-by-case basis and do not guarantee approval. To request an exception, please submit a written request to the IT Director outlining the following:

How to Request Exceptions/Exemptions?
To request an Exception or Exemption from a Policy that is in place please message ITDirector@SnowBe.com with the following format:

What Exception/Exemption are you requesting?

Why are you requesting this Exception?

How long are you requesting this Exception/Exemption for?

The IT Director, in consultation with relevant stakeholders, will review the request and determine if an exception can be granted. The decision will be based on the potential impact on security, the justification provided, and the availability of alternative secure solutions. Exceptions/Exemptions are subject to change at any point in time to strengthen security posture

Enforcement

The failure to comply with policies, Policys, or Policys will result in a warning or disciplinary action depending on the severity of the infraction.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
v1	06/06/2024	Michael Kohronas		Added the exception and exemption and enforcement as a group
V2	06/07/2024	Michael Kohronas		Fixed issues with text size and font, added name and date to header,
V3	06/24/2024	Michael Kohronas		Created the MDM Policy

Citations

https://www.massey.ac.nz/documents/1709/Mobile_Device_Management_Policy.pdf

https://www.trio.so/blog/wp-content/uploads/2023/12/Mobile-Device-Management-Policy-Template.pdf