Document Reference:	ISMS	Effective Date:	10 May 2024
Document Name:	Endpoint Security	Expiry Date:	10 May 2025

Endpoint Security

Redback Operations

Document Owner:	Kaleb Bowen	Last Modified By:	Kaleb Bowen
Next Review Date:	1 May 2025	Last Modified on:	27 April 2024

Version	Modified By	Approver	Date	Changes made
1.0	Kaleb Bowen			Creation

Table of Contents

1 Purpose *4*

2 Scope *4*

3 Definitions and References *4*

4 Roles and Responsibilities *5*

Leadership 5

IT and Security Teams 5

End Users 5

5 Physical Security *6*

Storage 6

Devices 6

Device Storage 6

Asset Management 6

Accessories to Endpoints 6

Unattended Devices 7

6 Digital Security *7*

Patching 7

Least Privilege 7

Malware Protection 8

Authentication 8

Redundancy and Backups 8

Training 8

1 Purpose

The purpose of this policy is to provide formal structure and minimum security standards for endpoint devices owned by or through direct affiliation of Redback Operations. This is to ensure security is standardised for all users, to the best possible solutions that can be offered in the varies ways that users connect to Redback digital assets.

The Endpoint Security policy will ensure the appropriate measures in place to protect users and company assets whilst ensuring that usage of these systems is not compromised by threats or overly impeded by these measures. A balance of practicality and security is essential in the ongoing protection.

The policy also intends to ensure ongoing assurance to support Redback Operations in its evolution over time, ensuring that this policy reflects the continuous needs of endpoint security, and so supporting business continuity, as well as promoting a mature security culture.

2 Scope

The scope of this policy applies to all usage of physical endpoints owned or operated by Redback Operations and its affiliated contributors. Including but not limited to laptops, desktops, phones, servers, and research devices under Redback Operations such as the smart wearables and smart bikes.

Endpoint security also extends to software ran on Redback Operations' devices, as these have potential to cause harm to the organisation or owner of the device.

The policy will cover Redback-owned devices and contributor-owned devices separately and will be complimented by the BYOD policy for those contributor endpoints, as well as the broader Information Security Management System (ISMS) policy.

3 Definitions and References

Primary definitions can be used from the Information Security Management System and ISO / IEC 27001. All referenced framework controls also come from ISO 27001. Additional definitions for this document:

- ISMS: Information Security Management System, the primary policy document for Redback Operations.
- Affiliated contributors: Deakin University SIT capstone students working within the Redback Operations project.

- Redback-owned device: This includes devices such as exercise bikes owned by Deakin University and thus used by Redback Operations.

4 Roles and Responsibilities

Roles and Responsibilities are necessary to ensure appropriate delegation of tasks, accountabilities, and responsibilities are spread to the correct stakeholders in the organisation.

Leadership

Those in leadership roles have overall ownership and top level responsibility for the endpoints. Strategic decisions regarding the applicability of policies, overall security oversight, and design of the security structure are likewise a responsibility.

IT and Security Teams

Responsible for the process of design to development of implementation for the endpoint policies. This includes thorough testing of the implementation through test environments and gradual rollouts to ensure full security accountability. IT and Security must also consult with both leadership and the end users to ensure practical solutions, whilst maintaining a secure environment, built upon least privilege.

End Users

End users, being the device users and / or owners, are responsible for the usage of the devices in which they own or have personal data on.

For Owners

Owners must ensure that they are compliant in updating their device to the required software and hardware specifications determined by leadership. They must also ensure that any usage by people other than themselves is compliant with the policy.

For Users

Users must take care when accessing Redback endpoints. Their usage must ensure that no data is compromised, and that their digital hygiene remains a high priority.

5 Physical Security

Storage

Whilst cloud storage is the preferred storage method for Redback Operations, some situations may arise that demand use of portable storage methods such as USB drives or portable HDD / SSDs. Attention must be given to these devices to ensure the adequate security. Storage devices with sensitive data should be stored in locked containers when not in use. When in transit, these devices should be kept on the user or as close to as possible.

Devices

Device Storage

Portable devices that contain sensitive data should be locked in secure containers when not in use to ensure full protection. Access to this storage should only be for approved users. Testing devices specific to Redback Operations such as VR headsets or exercise bicycles that may not be able to be contained in safes or secured draws should be kept in rooms with controlled access management and surveillance.

Asset Management

Corporate devices should be registered in the company asset register, including current device holder and storage location. Corporate devices should have their asset number printed on them, as well as information for their return if found.

Accessories to Endpoints

Attention should be given to any accessories connected to Redback Operations affiliated devices. This includes peripherals such as keyboards, mice, headsets, and monitors, as well as storage devices and other devices that may have the ability to transmit data. Accessories should be purchased from trusted sites, and only used in a safe matter consistent with safe online practices. Any evidence of tampering or malicious files should be responded to with seizure of using the accessory and seeking assistance from IT leadership in taking the next steps to ensure safety of personal and corporate information on the host device.

Unattended Devices

Endpoints must engage a lock-out of content through a shutdown or sign-out after 15 minutes of inactivity to prevent potential bad actors getting access to the device. Regardless, users, especially those with privileged access, should be locking their devices immediately when leaving the direct area around it. Devices used for testing or experimental purposes may be configured to stay awake for the duration of their tasking if adequate signage is in place, or the presence of an approved user is nearby, additionally programs not necessary to the tasking should be locked down where relevant.

6 Digital Security

Patching

Operating systems and software deployed by Redback Operations should be monitored for newly released updates and patches. Critical security patches must be applied within 48 hours of notification, whilst non-critical should be applied at the earliest reasonable time.

Operating systems and software that reaches end-of-life should be removed from devices with alternatives identified as the security of these cannot be guaranteed.

Least Privilege

User access to endpoints should be implemented in accordance with the principle of least privilege. That being, users should only have access to the necessary functions to complete their tasking. This access should be reviewed regularly, on both intervals and when a user changes roles in the organisation.

Administrative access should be restricted to those with an absolute need, such system owners. Where possible, select permissions should be given rather than administrative access.

Least privilege should also be implemented in the case of sub-systems within the operating systems of Redback-owned devices. Non-administrative users should be logging onto accounts which are locked down appropriately to avoid changes being made to core aspects of the operating system. This should be implemented through group policy.

Malware Protection

All Windows endpoints must, at a minimum, be running Windows Defender to the full settings available.

Authentication

In every instance where the software allows it, 2-factor authentication, or multi-factor authentication should be used. The preferred method for this is through password and a token generator, such as Authy or Google Authenticate, or a physical token such as Yubikey.

Attention should also be given to the storage of passwords. Each user accessing a Redback Operations endpoint should use a password manager, as well as maintaining healthy password practices including the usage of passphrases or complex passwords, and regularly checking against breach sites for leaked passwords.

Redundancy and Backups

Regular backups should be conducted to ensure data redundancy practices are in place. Sensitive and business-critical data should not be primarily stored on the local endpoints, instead being stored on shared cloud repositories with other relevant users. Where possible, offsite physical backups should also be used as another added layer of redundancy.

Training

Users should complete company-standard training before having privileged access to systems.