Document Reference:	ISMS	Effective Date:	1 May 2024
Document Name:	ISMS Manual	Expiry Date:	1 May 2025

Information Security Management Systems Manual

Redback Operations

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

Version	Modified By	Approver	Date	Changes made
1.0	Kaleb Bowen	Ben Stephens	5 April 2024	Creation

Table of Contents

1. Scope ***4***

2. Normative References ***4***

3. Terms and Definitions ***4***

4. Context of the Organisation ***4***

5. Leadership ***6***

6. Planning ***7***

7. Support ***7***

8. Documented Information ***8***

9. Operation ***9***

10. Performance Evaluation ***9***

11. Improvement ***10***

1. Scope

The Information Security Management System (ISMS) establishes the guiding principles and policies for Redback Operations, being the comprehensive and overarching system complying with ISO/IEC 27001. This document is intended to provide a framework for Redback Operations and affiliated contributors to implement and continuously manage the security of its information assets.

The scope of this ISMS includes all information assets, including but not limited to:

- Data Classification & Data Loss Prevention (DLP)
- Cloud Security
- Server Security & Hardening
- Endpoint Security
- Encryption / Cryptography
- Monitoring & Log Analysis
- User Awareness Training
- External Attack Surface Management
- BYOD & MDM

2. Normative References

This section is not applicable with Redback Operations but is kept in to ensure further section numbering is compliant with ISO/IEC 27001.

3. Terms and Definitions

For the purpose of this document, ISO/IEC 27001 apply unless specified otherwise.

4. Context of the Organisation

4.1. Understanding the Organisation and its Context

Redback Operations is a student-led, open-source project (referred to as Redback Operations, or “the company”) with a focus on human biometrics, including through the use of wearable devices, fitness apparatus, and monitoring and tracking devices. The result of which leads Redback Operations to handle sensitive and personal data

that may be required to be handled in such a way to comply with relevant legislation. Additional ISMS processes may also be adopted in consideration with the efforts and needs of the company and the appropriate protections following.

4.2. Understanding the Needs and Expectations of Interested Parties

Interested parties relevant to the project include Deakin University and its affiliated tutors and staff connected to the Redback Operations project, and students enrolled in SIT374/SIT764 and SIT478/SIT768. Tutors and students are split into individual projects within the company, as such students and tutors may have different needs and expectations depending on their role.

Stakeholders	Internal / External	Issues
Tutors, Staff	Internal	Organisation structure, roles and accountabilities, top-level delegations.
Project Leads, Team Leads, Students	Internal	Delegation of tasks, fulfilment of commitments, compliance to policy and guidelines.
Government	External	Fulfilling the legal and regulatory requirements.

4.3. Determining the Scope of the Information Security Management System

The ISMS encompasses all digital and physical items owned by or in direct affiliation with Redback Operations. Redback Operations does not have a physical headquarters, and has contributors in many different legal jurisdictions, so this must be taken into consideration when legislation or government policies are discussed.

4.4. Information Security Management System

As per the requirements of ISO/IEC 27001, Redback Operations has implemented this Information Security Management System (ISMS) and established procedures to continually improve the system following the structure of the organisation as a student-run, trimester-based project. If a response to a requirement can be written in small-form-factor, it will be done so in this manual, otherwise, this manual will

reference the appropriate documentation and its location within the documentation system to provide further extended policy explanation. For the purpose of continuity, all auxiliary documentation will be listed in section 12 with links to the Redback Operations documentation website.

5. Leadership

5.1. Leadership and Commitment

Deakin University, staff, tutors, and student leaders affiliated with the Redback Operations company must be committed to continue high-level information security and thus ensuring that the overall organisation is taking sufficient steps in ensuring the organisation's security policies and objectives are in line with modern practices and the general strategic direction.

5.2. Policy

Protection of Redback Operations is regulated across several policies relating to the type of information or systems rather than one central policy. These policies are mentioned in section 1 and available to view in section 12. Further policies may be requested by company leaders as needed, or existing policies be reviewed, as is the nature of the continual evolution of this ISMS and other policies.

5.3. Organisational Roles, Responsibilities, and Authorities

Presently, responsibility of this ISMS and other policies falls within the Cyber Security team of Redback Operations. As such, it is their responsibility to ensure compliance with ISO/IEC 27001 and all relevant legislation and governance on which Redback Operations falls within. Company leaders have the right to request review of the ISMS and affiliated policies, which again falls within the Cyber Security team. The Cyber Security team may request assistance from other teams to ensure complete understanding of their projects and what that entails in relation to the company policies; additionally, they may ask to delegate new / updated policies from a team should they have someone willing and able to complete it.

6. Planning

6.1. Actions to Address Risk and Opportunities

6.1.1. General

Following the issues and requirements outlined in sections 4.1 and 4.2, the following items should be addressed:

- Assurance that this ISMS can achieve its intended outcomes.
- Preventing avoidable IT-related incidents.
- Achieving continual improvement.

Following supplementary policy should sufficiently address the above mentioned in a way that also covers potential data breaches and their impact on Redback Operations, data protection, managing risks, and proactive remediation.

6.1.2. Information Security Risk Assessment

In accordance with ISO/IEC 27001, a Risk Analysis and Treatment Plan, along with a Statement of Applicability should be created to work alongside this ISMS to ensure understanding of risks associated with Redback Operations are sufficiently known.

6.1.3. Information Security Risk Treatment

As above.

6.1.4. Information Security Objectives and Planning

To manage the company's information security posture effectively and efficiently, it is essential to develop objectives, measurements, and reporting tools, compiled within an Information Security Metrics Repository (ISMP). The ISMP will ensure consistent information security measurement across all aspects of the company.

7. Support

7.1. Resources

Redback Operations, as a student-lead project, does not have the same resources as the typical IT organisation. As such, roles such as HR, Ethics and Policy Managers, and Risk Advisors are split amongst students, typically of the Cyber Security team, who wish to undertake tasks within these areas. This organisation structure also means Redback Operations does not have a Management Review Board as required by ISO/IEC 27001, however it can be determined that company leaders act in a similar capacity in terms of review and request of changes to the ISMS.

7.2. Competence

Redback Operations is committed to ensuring that all staff and students working on projects that use IT systems or handle sensitive information are working within the ISMS. This may include the need to provide training or time to get up to speed with the company standards, as well as implementing compliance and competence tracking systems on tasks that require so.

7.3. Awareness

Redback Operations ensures that all documentation relevant and including the ISMS are easily accessible via the documentation site, and formatted in an easily viewable and accessible means for all that require.

7.4. Communication

Changes to the ISMS or other policies affecting the overall company will be communicated internally via the company's Microsoft Teams platform. Changes to documentation will be reflected within the documentation itself via versioning notes, and where possible previous versions will be viewable as a way to reflect on changes.

8. Documented Information

8.1. General

All controlled versions of Redback Operations documentation can be found on the documentation site. All locally saved or printed copies are uncontrolled versions and may not be the most current.

8.2. Creating and Updating

Creation of policy is formed through discussion of relevant teams, with team leaders, mentors, and company leaders having overall ownership of all documents. The student(s) responsible for creating specific documents also have ownership for the duration of their time within Redback Operations.

8.3. Control of Documented Information

Given the size and nature of Redback Operations, at present the use of a Document Control Procedure and Document Control System Master Listing is not necessary. This should be reviewed on an ad-hoc basis.

9. Operation

9.1. Operational Planning and Control

The Redback Operations Information Security Management System, under the direction of the Cyber Security team and company leaders, outlines the processes necessary to secure company information from threats. As with 8.3, the size of Redback Operations does not deem it necessary to have internal audit procedure or management review procedures, and these should be conducted on an ad-hoc schedule. Future growth or needs of the company may determine formal policy to cover these audits.

10. Performance Evaluation

10.1. Monitoring, Measurement, Analysis, and Evaluation

Performance of policies should be reviewed on a regular basis, no less than once every year. Adjustments should be made and noted using version control. This can be in

conjunction with previous sections of this ISMS that cover yet-to-exist audits due to the size of the company.

10.2. Internal Audit

As above.

10.3. Management Review

Redback Operations does not operate with a typical management structure and as such quarterly meetings, as outlined in ISO/IEC 27001 are not reasonable. Company goals and policy reviews should be done on an ad-hoc basis.

11. Improvement

11.1. Nonconformity and Corrective Action

When an instance of nonconformity is identified within the jurisdiction of the ISMS and affiliated policies, team and / or company leaders may act on it by implementing corrective actions. This should begin with identifying the issue itself and the ramifications it may bring, developing a fix for the issue and implementing it, and developing or fixing current solutions to ensure the nonconformity is unlikely to happen again.

11.2. Continual Improvement

The company is committed to continually improving this ISMS and other policy documents as the company evolves over time.

12. Supplementary Policies

This section contains links to supplementary policies affiliated with Redback Operations and this ISMS.