Document Reference:	ISMS	Effective Date:	12/05/2024
Document Name:	Server Security Policy	Expiry Date:	12/05/2025

Server Security & Hardening Policy

SIT374 Team Project A

Redback Operations

Document Owner:	Daniel McAulay	Last Modified By:	Daniel McAulay
Next Review Date:	12/05/2025	Last Modified on:	12/05/2024

Version	Modified By	Approver	Date	Changes made
V0.2	Daniel McAulay	Daniel McAulay	12/05/2024	Document Creation

Contents

Scope 6
Purpose 7
Objectives 7
Definitions 8
Guiding Principles 9
General Obligations 10
Key Assets and Data Categories 11
Framework References 12
Conclusion: 13
Roles and Responsibilities 14
Key Roles 14
Security Team 14
IT Department 14
System Administrators 14
Management 14
End Users 14
RACI Chart 15
Operating System Hardening 18
Operating System Selection 18
Operating System Releases and Versions 18
Standard Operating Environments (SOEs) 18
Hardening Operating System Configurations 18
OS Security Protections 19
Control References 19
Application Management and Control 20
Application Management 20
Application Control 20
Command Shell 20
PowerShell 20
Control References 21

Intrusion Prevention, Software Firewalls, Antivirus, and Device Access Control 22
Host-Based Intrusion Prevention System (HIPS) 22
Software Firewall 22
Antivirus Software 22
Device Access Control Software 22
Control References 23
Operating System Event Logging 24
Control Reference: 24
User Application Hardening 25
User Applications 25
User Application Selection 25
User Application Releases 25
Hardening User Application Configurations 26
Control References: 27
Microsoft Office Macros 28
Control References 29
Server Application Hardening 30
Server Applications 30
Server Application Selection 30
Server Application Releases 30
Hardening Server Application Configurations 30
Restricting Privileges for Server Applications 31
Control References 31
Microsoft Active Directory Domain Services (AD DS) Hardening 32
Microsoft AD DS Domain Controllers 32
Microsoft AD DS Account Hardening 32
Microsoft AD DS Security Group Memberships 33
Control References 33
Authentication Hardening 34
Account and Authentication Types 34
Authenticating to Systems 34
Insecure Authentication Methods 34

Multi-Factor Authentication (MFA) 34
Single-Factor Authentication 35
Setting Credentials for User Accounts 35
Setting Credentials for Break Glass, Local Administrator, and Service Accounts 35
Changing Credentials 35
Protecting Credentials 36
Account Lockouts 36
Session Termination 36
Session and Screen Locking 36
Logon Banner 37
Control Reference: 37
Virtualization Hardening 40
Hypervisors 40
Containerization 40
Functional Separation Between Computing Environments 40
Control References: 40
Policy Review 41
Responsibility for Reviews 41
Frequency of Reviews 41
Proposing and Approving Changes 41
Communication Plan for Updates 41
Appendix 42

Scope

The Server Security Policy applies to all server assets, including physical and virtual servers, as well as related server infrastructure managed or operated by Redback Operations. This policy encompasses all servers utilized across the organization, irrespective of their geographical location or deployment model (on-premises, cloud-hosted, or hybrid environments).

Server Security in the context of this policy involves the protection of servers from unauthorized access, threats, and vulnerabilities that could compromise the confidentiality, integrity, and availability of the data they store and process. It includes the implementation of physical security measures, network security controls, operating system configurations, and application-level protections.

The policy aims to establish guidelines for:

- Access Control
  - Ensuring that access to servers is strictly controlled and monitored, with authentication mechanisms in place to verify the identity of users.
- Data Protection
  - Implementing procedures to protect sensitive and critical data stored on servers, including encryption, data masking, and secure data disposal practices.
- System Configuration
  - Standardizing server configurations to minimize vulnerabilities and ensure that all servers operate in accordance with organizational security standards.
- Patch Management
  - Regularly updating servers with the latest security patches and updates to mitigate exposure to known threats and vulnerabilities.
- Security Monitoring
  - Utilizing tools and techniques to continuously monitor server activity for signs of security incidents or breaches.
- Incident Response
  - Preparing and executing a coordinated response to security incidents that impact server operations to minimize damage and restore normal operations as quickly as possible.

This scope ensures comprehensive coverage of all server-related security aspects, integrating seamlessly with other cybersecurity policies in place at Redback Operations as part of the broader Information Security Management System.

Note: This policy serves as a foundational element of our broader IT security strategy, which may include future deployments of additional security solutions such as intrusion detection systems (IDS), intrusion prevention systems (IPS), and advanced threat protection services.

Purpose

The Server Security Policy is designed to ensure Redback Operations achieves and maintains strict security and compliance standards throughout its server infrastructure. This policy aims to safeguard the integrity, confidentiality, and availability of all server data and applications. By defining comprehensive controls and procedures, this policy serves as a foundational guide for securing and managing all server resources effectively.

Objectives

The objectives that this Server Security Policy intends to achieve are:

- Enhance Security Posture:
  - Identify, evaluate, and mitigate risks and threats to servers and their hosted data proactively.
- Compliance and Regulatory Adherence:
  - Ensure server security practices align with applicable legal, regulatory, and contractual requirements, mitigating the risk of legal and financial penalties.
- Operational Excellence:
  - Monitor and optimize server performance to ensure system reliability, availability, and business continuity.
- Incident Management and Response:
  - Establish a systematic approach for detecting, analysing, and responding to server security incidents promptly, minimizing impact and preventing recurrence.
- Forensic Capabilities:
  - Implement accurate and comprehensive logging practices to support investigations and establish accountability and traceability.
- Confidentiality, Integrity, and Availability (CIA):
  - Protect the CIA of company systems and infrastructure by aligning the policy with the Redback Operations Information Security Management System.
- Configuration Management and Hardening:
  - Establish standardized server configurations and hardening measures to minimize vulnerabilities.
- Threat Detection and Analysis:
  - Implement processes to detect and analyse threats quickly, identifying and addressing potential breaches.

This policy supports both technical and strategic security goals while fostering a culture of security compliance across all server environments in Redback Operations. It lays a solid groundwork for the effective protection of sensitive data and server infrastructure.

Definitions

The table below expands on definitions and components specific to server security:

Term	Definition
Access Control	Procedures to limit server access to authorized individuals only, often through user accounts, roles, and permissions.
Configuration Management	Managing and maintaining standard server configurations to reduce vulnerabilities.
Hardening	The process of reducing the attack surface by disabling unnecessary services and tightening security configurations.
Patch Management	The systematic process of identifying, prioritizing, and applying patches to servers to mitigate security vulnerabilities.
Backup and Recovery	Strategies for duplicating critical data and restoring it in case of system failure or security incident.
Multi-Factor Authentication (MFA)	Security protocol requiring multiple verification steps before gaining access to a system.
Intrusion Detection System (IDS)	A system that monitors network traffic or server behaviour for suspicious activity or known attack patterns.
Security Information and Event Management (SIEM)	A tool for aggregating and analysing server logs and network activity to identify and respond to security incidents.
Forensic Analysis	The process of investigating server logs to understand the cause of a security incident and gather evidence.

Guiding Principles

Here are the guiding principles that Redback Operations should follow for server security:

Principle	Description
Confidentiality	Ensure that server data remains accessible only to authorized individuals through strict access control measures.
Integrity	Maintain the accuracy and completeness of server data, preventing unauthorized modifications.
Availability	Ensure server data and services are reliably available to authorized users by implementing redundancy and backup measures.
Security	Apply comprehensive security measures that align with industry standards to protect server data from internal and external threats.
Scalability	Ensure server security measures can scale with the growth of the organization and changes in infrastructure.
Resilience	Build and maintain server configurations that can withstand failures and continue operations with minimal disruption.
Monitoring	Continuously monitor server performance and security to detect potential threats and operational issues proactively.
Compliance	Adhere to applicable legal, regulatory, and contractual requirements in server management practices.

General Obligations

Redback Operations adheres to the following obligations under the Server Security Policy:

Obligation	Description
Patch Management	Regularly update server software and operating systems with the latest security patches to mitigate vulnerabilities.
Access Control	Implement and periodically review role-based access controls to minimize unauthorized access risks.
Data Protection	Encrypt sensitive data at rest and in transit to protect confidentiality.
Configuration Management	Ensure standardized server configurations minimize vulnerabilities and are regularly updated to reflect the latest security practices.
Security Monitoring	Monitor server logs and network traffic continuously for unusual activity that could signal a potential threat.
Incident Response	Establish and maintain a coordinated plan for investigating and responding to server security incidents.
Training	Regularly train IT staff and other stakeholders on server security best practices and compliance requirements.

These sections outline essential components of the Server Security Policy, providing clarity on terminology, guiding principles, and obligations for Redback Operations.

Key Assets and Data Categories

For Redback Operations, identifying the critical systems, applications, and data sets that require protection is crucial. This includes any sensitive information that needs heightened security measures. Here are typical IT assets and data categories that are critical and covered under the scope of this policy:

- **IT Assets**:
  - Servers (web, application, database)
  - Network devices (routers, switches, firewalls)
  - End-user devices (laptops, smartphones)
  - Cloud services and storage solutions
  - Critical software applications (CRM, ERP, custom applications)
- **Data Categories**:
  - Customer data (personal identification information, payment details)
  - Employee data (personal details, HR records)
  - Intellectual property (trade secrets, proprietary technology)
  - Financial data (transaction records, financial reports)
  - Operational data (logs, configuration files)

These assets and data types require monitoring to ensure they are protected from unauthorized access, modifications, or any other cyber threats.

Framework References

The Server Security Policy for Redback Operations incorporates specific controls from the Australian Signals Directorate (ASD's) Information Security Manual. References to the ASD ISM security controls are referenced further in the policy, however the policy itself overlaps and aligns with ISO 27001:2022 standards and the CIS Security Controls v8 to ensure a comprehensive and robust approach to server security and risk management.

These frameworks provide recognized best practices for maintaining the security, integrity, and availability of information systems.

ISO 27001:2022 Controls:

- **A.5.14 Information Security Policy:** Mandates developing, implementing, and maintaining an information security policy that aligns with organizational objectives, ensuring secure data processing and compliance.
- **A.8.1 Asset Management:** Highlights maintaining an inventory of information assets and assigning ownership, promoting accountability and protection.
- **A.9.1 Access Control:** Focuses on securing access to systems based on business and security requirements, minimizing unauthorized access.
- **A.12.1 Operations Security:** Stresses managing IT operations securely, including controlling changes, protecting data at rest, and preventing malware infections.
- **A.12.4 Logging and Monitoring:** Emphasizes monitoring and analysing system logs to detect, understand, and respond to security incidents.
- **A.13.1 Network Security Management**: Focuses on protecting information in networks and its supporting infrastructure from unauthorized access, misuse, and denial of service.
- **A.14.1 System Development:** Ensures security is integrated across the software development lifecycle, reducing vulnerabilities, and supporting secure design.
- **A.14.2 Security in Development and Support Processes**: Ensures that information security is an integral part of information systems across the lifecycle, including development and support.

CIS Controls:

- **Control 1: Inventory and Control of Enterprise Assets:** Ensures all devices and software are identified and managed, reducing unauthorized or unmanaged hardware and software.
- **Control 3: Data Protection:** Safeguards sensitive data throughout its lifecycle, using encryption and access controls.
- **Control 5: Secure Configuration of Enterprise Assets and Software:** Advises on maintaining a hardened configuration for both hardware and software to reduce vulnerabilities.
- **Control 7: Continuous Vulnerability Management:** Encourages identifying vulnerabilities promptly and implementing remediation strategies.
- **Control 9: Email and Web Browser Protections:** Recommends securing email clients and web browsers against common attacks like phishing and drive-by downloads.
- **Control 10: Data Recovery Capabilities**: Emphasizes the importance of establishing and maintaining robust data recovery processes to ensure timely recovery in the event of a security incident.
- **Control 11: Secure Configuration for Network Devices**: Includes guidelines for securely configuring network devices such as firewalls, routers, and switches.
- **Control 12: Boundary Defence**: Ensures that defences are effective at detecting, preventing, and correcting the flow of information transferring networks of different trust levels.
- **Control 13: Network Monitoring and Defence:** Establishes effective network security monitoring to detect, analyse, and respond to security incidents in real time.

Conclusion:

ISO 27001 controls and CIS benchmarks have been carefully selected to address the specific security needs of server environments at Redback Operations.

By aligning the Server Security Policy with these established standards, Redback Operations ensures that its servers are well-protected against threats and are compliant with international best practices and regulatory requirements.

This alignment not only secures the infrastructure but also supports the organization’s goals of maintaining operational integrity and business continuity.

Roles and Responsibilities

A clear definition of roles and responsibilities is crucial for effective server security management. At Redback Operations, the following roles play key parts in maintaining the security and integrity of servers:

Key Roles

The success of the Server Security Policy at Redback Operations relies on clearly defined roles and responsibilities. It is crucial for all stakeholders to understand their duties to ensure effective implementation, compliance, and maintenance of security standards.

Security Team

- Develop, review, and update the server security policy; implement security controls and measures; monitor security compliance; conduct regular security assessments; respond to security incidents.
- Accountable For: Maintaining the overall security posture of the organization's server environments.

IT Department

- Assist in implementing security controls; manage and maintain server hardware and software; ensure timely application of patches and updates; support the Security Team in incident response activities.
- Operational management of servers and ensuring their compliance with the security policy.

System Administrators

- Apply security configurations and settings; monitor system performance and logs; enforce access controls and permissions; directly handle the installation, maintenance, and upgrading of servers.
- Day-to-day management of servers, ensuring they are secure from unauthorized access and threats.

Management

- Approve security policies and resource allocations; ensure organization-wide compliance with security practices; foster a culture of security awareness.
- Strategic oversight and ensuring that security objectives align with the organization's business goals.

End Users

- Adhere to security policies and procedures; report any suspected security vulnerabilities or incidents to the IT or Security Team.
- Using server resources responsibly and maintaining awareness of security implications.

RACI Chart

To delineate responsibilities, the following RACI chart indicates who is Responsible, Accountable, Consulted, and Informed for key server security activities:

Task	Security Team	IT Department	System Administrators	Management	End Users
Develop Security Policy	A	-	-	C	-
Implement Security Controls	R	A	C	-	-
Monitor Compliance	A	R	I	-	-
Patch and Update Management	I	A	R	-	-
Incident Response	A	R	R	I	-
Approve Policies	I	-	-	A	-
Resource Allocation	C	R	I	A	-
Security Training	R	I	I	-	C

Legend:

- R: Responsible – Performs the actual work to achieve the task.
- A: Accountable – Ultimately accountable for the completion and quality of the task.
- C: Consulted – Provides input and advice; engaged in two-way communication.
- I: Informed – Kept up to date on progress; one-way communication.

Strategic Overview & Controls

The server security policy for Redback Operations is developed in line with the Australian Signals Directorate's Information Security Manual (ISM) and the Essential 8 Framework. It provides a holistic approach to safeguarding IT infrastructure against a broad spectrum of security threats.

This section of the Server Security Policy details key topics covered under these frameworks, and provides guidance and reasoning regarding adherence to security controls:

We prioritize credential management and authentication to tightly control system access, ensuring that identity verification, random credential generation, secure distribution, enforced changes on first use, and prevention of credential reuse are all in place. These measures establish a strong foundation for managing both internal and external threats effectively.

Session and screen locking practices are incorporated to secure inactive sessions from unauthorized access. Automatic locking after inactivity, or when manually locked by users, ensures that active sessions are secure, and systems remain protected when temporarily unattended.

Logon practices are emphasized with logon banners to remind users of their security responsibilities and the sensitivity of the systems they handle. These practices reinforce a security-conscious mindset across the organization.

In virtualization and hypervisor hardening, we emphasize secure configurations, regular patching, and vendor selection based on secure-by-design principles to protect virtual environments just as rigorously as physical ones. This approach prevents attackers from exploiting virtualization vulnerabilities.

Functional separation between computing environments and server roles is an effective strategy to prevent breaches from spreading via lateral movement. By enforcing both physical and logical isolation and ensuring secure software-based isolation mechanisms, we protect the integrity of each computing environment independently.

The Essential 8 Framework strategies referenced in this Server Security policy include references to controls such as:

- *Application whitelisting*
- *Regular patching of software and operating systems*
- *Restricting administrative privileges*
- *Multi-factor authentication*
- *Application Hardening*
- *Microsoft Office Macro Settings & Microsoft Security Baseline Policies*

These strategies are chosen for their effectiveness in mitigating malware infections, minimizing the impact of security incidents, and enabling rapid data recovery.

Monitoring and log analytics are central to our continuous security assessment, aggregating and analysing logs from critical systems to detect potential security incidents swiftly. This proactive

approach enhances threat detection while ensuring compliance and supporting forensic investigations.

The strategies referenced in this policy form a comprehensive, layered defence to protect Redback Operations from evolving threats while aligning with national and international industry standards. Each control and strategy work cohesively to deliver proactive security measures that create a culture of security-consciousness and readiness.

Note: Backup Controls are referenced in the Redback Operations Business Continuity Plan. Refer to this policy for further details.

Further detail regarding Server Security Guidelines can be found here: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-hardening

(Australian Signals Directorate, Guidelines for System Hardening, May 12 2024)

Operating System Hardening

Operating System Selection

Choosing the right operating system is fundamental to building a secure server environment. Redback Operations should prioritize vendors that:

- Adhere to secure-by-design and secure-by-default principles.
- Utilize memory-safe programming languages where possible (e.g., C#, Go, Java, Ruby, Rust, Swift).
- Follow secure programming practices and demonstrate a strong commitment to maintaining the security of their products.

Operating System Releases and Versions

Regular updates and patches are crucial in maintaining secure servers:

- Use the latest or the previous release of operating systems, ensuring access to the latest security features.
- Where possible, choose 64-bit versions of operating systems, which support additional security functionalities.

Standard Operating Environments (SOEs)

Standardization improves consistency and reduces vulnerabilities:

- Ensure consistent server environments through standardized SOEs, delivered via automated build processes or golden images.
- When SOEs are obtained from third parties, scan them for malicious code or configurations.
- Review and update SOEs annually to maintain current security baselines.

Hardening Operating System Configurations

Secure configurations ensure resilient operating systems:

- Develop, implement, and maintain approved configurations for all operating systems.
- Follow ASD and vendor hardening guidelines, prioritizing the most restrictive recommendations if conflicts arise.
- Unneeded accounts, services, and features must be disabled or removed.
- Default credentials and accounts must be changed.
- Disable automatic execution for removable media.
- Disable or remove Internet Explorer 11 to reduce vulnerabilities.
- Remove .NET Framework 3.5, including .NET 2.0 and 3.0, if possible.

OS Security Protections

Enable all available OS security protections:

- Ensure operating system exploit protection is enabled.
- Enable Secure Boot & TPM Modules
- Prevent unprivileged users from disabling or modifying security features or running script execution engines.

Control References

- ISM-1743: Operating systems are chosen from vendors with a proven security commitment.
- ISM-1407: The latest or previous operating system release is used.
- ISM-1408: 64-bit versions are used when supported.
- ISM-1406: SOEs are used for all servers.
- ISM-1608: Third-party SOEs are scanned for malicious code and configurations.
- ISM-1588: SOEs are reviewed and updated annually.
- ISM-1914: Develop, implement, and maintain approved OS configurations.
- ISM-1409: Harden OS configurations per ASD and vendor guidance.
- ISM-0380: Disable or remove unneeded OS components.
- ISM-0383: Change default credentials and accounts.
- ISM-0341: Disable automatic execution of removable media.
- ISM-1654: Disable or remove Internet Explorer 11.
- ISM-1655: Disable or remove .NET Framework 3.5.
- ISM-1492: Enable OS exploit protection.
- ISM-1745: Enable Early Launch Antimalware, Secure Boot, Trusted Boot, and Measured Boot.
- ISM-1584: Prevent unprivileged users from bypassing security features.
- ISM-1491: Prevent unprivileged users from running script execution engines.

These guidelines ensure that Redback Operations' server operating systems remain hardened and resistant to threats, aligning with the most restrictive security practices outlined by ASD ISM and CIS Security Controls.

Application Management and Control

Application Management

To minimize the risk posed by malicious applications, Redback Operations implements strict controls on application management:

- Unprivileged users are not allowed to install unapproved software.
- Approved software must be installed from organization-managed repositories or trusted application marketplaces.
- Unprivileged users cannot uninstall or disable approved software, preventing the removal of security features or critical system functions.

Application Control

Application control helps to prevent the execution of malicious code on servers. Redback Operations follows a structured approach to application control:

- Develop rulesets based on business requirements, including specific executable, script, installer, and driver types.
- Use cryptographic hash rules, publisher certificate rules, or path rules while ensuring hardening measures are in place.
- Log and analyse application control events centrally to detect and investigate malicious behaviour.

Command Shell

Command shells, while useful for automating system tasks, can be exploited by malicious actors. By centrally logging command line process creation events, Redback Operations can detect malicious behaviour promptly.

- Command line process creation events are centrally logged.

PowerShell

PowerShell is a powerful tool but can be dangerous if exploited. The following controls protect against unauthorized usage:

- Disable or remove Windows PowerShell 2.0 to prevent attacks that exploit vulnerabilities in older versions.
- Set PowerShell's language mode to Constrained Language Mode, balancing security with functionality.
- Log PowerShell module, script block, and transcription events centrally to monitor the security posture and detect malicious actions.
- Protect PowerShell script block logs using Protected Event Logging.
- Ensure PowerShell remote execution policy is configured to use RemoteSigned.

Control References

- ISM-1592: Unprivileged users cannot install unapproved software.
- ISM-0382: Unprivileged users cannot uninstall or disable approved software.
- ISM-1490: Application control implemented on internet-facing servers.
- ISM-1656: Application control implemented on non-internet-facing servers.
- ISM-1870: Application control applied to user profiles and temporary folders.
- ISM-1871: Application control applied to all locations besides user profiles and temporary folders.
- ISM-1657: Execution restricted to an organization-approved set of executables, libraries, scripts, installers, compiled HTML, and control panel applets.
- ISM-1658: Execution of drivers restricted to an organization-approved set.
- ISM-0955: Application control uses cryptographic hash rules, publisher certificate rules, or path rules.
- ISM-1471: When using publisher certificate rules, both publisher and product names are used.
- ISM-1392: Path rules only allow approved users to modify files and folders.
- ISM-1746: Path rules only allow approved users to change file system permissions.
- ISM-1544: Microsoft's application blocklist is implemented.
- ISM-1659: Microsoft’s vulnerable driver blocklist is implemented.
- ISM-1582: Application control rulesets are validated annually or more frequently.
- ISM-0846: All users, except local admin and break-glass accounts, cannot bypass or disable application control.
- ISM-1660: Allowed and blocked application control events are centrally logged.
- ISM-1889: Command line process creation events are centrally logged.
- ISM-1621: Disable or remove Windows PowerShell 2.0.
- ISM-1622: Configure PowerShell to use Constrained Language Mode.
- ISM-1623: Log PowerShell module, script block, and transcription events centrally.
- ISM-1624: Protect PowerShell script block logs with Protected Event Logging.

Intrusion Prevention, Software Firewalls, Antivirus, and Device Access Control

Host-Based Intrusion Prevention System (HIPS)

Signature-based detection can miss new variants of malware. A Host-based Intrusion Prevention System (HIPS) uses behaviour-based detection to identify and block malicious activity, providing an extra layer of security for both workstations and critical servers at Redback Operations.

Software Firewall

Network firewalls generally control communication between network segments based on ports and protocols but often fail to prevent malware propagation or data exfiltration. Software firewalls offer more granular control, allowing communication restrictions based on specific applications or services, effectively safeguarding servers, and workstations.

Antivirus Software

Malicious actors frequently reuse known vulnerabilities, and antivirus software on workstations and servers provides protection by leveraging signature-based, heuristic, and reputation-rating detection. Regular scanning and timely updates reduce the risk of exploitation.

Device Access Control Software

External communication interfaces that facilitate Direct Memory Access (DMA) or removable media can be exploited if improperly managed, posing significant security risks. Device access control software or disabling external interfaces minimizes the risk.

Control References

- ISM-1034: Implement a HIPS on critical and high-value servers.
- ISM-1416: Implement a software firewall on workstations and servers to control inbound and outbound network connections to an approved set of applications and services.
- ISM-1417: Implement antivirus software with:
    - Signature-based detection enabled at a high level.
    - Heuristic-based detection enabled at a high level.
    - Reputation rating functionality enabled.
    - Ransomware protection functionality enabled.
    - Signature updates configured for daily updates.
    - Regular scanning of all fixed disks and removable media.
- ISM-1418: If there is no business requirement for reading from removable media and devices, disable this functionality using device access control software or by disabling external communication interfaces.
- ISM-0343: If there is no business requirement for writing to removable media and devices, disable this functionality.
- ISM-0345: Disable external communication interfaces that allow DMA.

Operating System Event Logging

Note: Refer to the Monitoring & Log Analytics Policy within the ISMS for further information.

Centrally logging and analysing operating system events is essential for monitoring system security, detecting malicious activity, and supporting investigations following cybersecurity incidents. At Redback Operations, the following operating system events are logged centrally:

- Track when applications or the operating system experience crashes or generate error messages.
- Record changes to security policies or system configurations that could impact the security posture.
- Monitor successful and failed user logons and account lockouts.
- Log process and service failures, restarts, and changes to important processes or services.
- Record requests made to access internet resources for anomaly detection.
- Document security product-related events, such as antivirus or firewall actions.
- Capture information about when systems start up and shut down.

Control Reference:

- ISM-0582: Centrally log these operating system events:
    - Track when applications or the operating system experience crashes or generate error messages.
    - Record changes to security policies or system configurations that could impact the security posture.
    - Monitor successful and failed user logons and account lockouts.
    - Log process and service failures, restarts, and changes to important processes or services.
    - Record requests made to access internet resources for anomaly detection.
    - Document security product-related events, such as antivirus or firewall actions.
    - Capture information about when systems start up and shut down.

User Application Hardening

User Applications

This section pertains to applications typically installed on workstations and occasionally on servers (such as Remote Desktop Servers), such as office productivity suites, web browsers, email clients, PDF software, and security products like antivirus and firewalls.

User Application Selection

To minimize vulnerabilities, Redback Operations should prioritize vendors that adhere to secure-by-design and secure-by-default principles, use memory-safe programming languages, follow secure programming practices, and maintain their products' security. Redback Operations should prioritize vendors that:

- Follow secure-by-design and secure-by-default principles.
- Use memory-safe programming languages when possible.
- Demonstrate secure programming practices and maintain their products' security.

User Application Releases

Newer releases often contain improved security features that make exploitation more difficult. Using the latest releases ensures protection against known vulnerabilities.

Hardening User Application Configurations

Proper configuration hardening prevents exploitation by malicious actors. The following controls should be followed:

- Develop, implement, and maintain approved configurations for all user applications.
- Change default accounts or credentials, including pre-configured accounts.
- Disable or remove unneeded components and features.
- Restrict add-ons, extensions, and plug-ins to an approved set.
- Microsoft Office:
    - Block creating child processes, executable content, or injecting code.
    - Prevent activation of Object Linking and Embedding packages.
    - Harden office productivity suites per ASD and vendor guidance.
    - Prevent changes to office security settings by users.
- Web Browsers:
    - Block Java and web advertisements from the Internet.
    - Harden web browsers per ASD and vendor guidance.
    - Prevent changes to browser security settings by users.
- PDF Software:
    - Block creating child processes.
    - Harden per ASD and vendor guidance.
    - Prevent changes to PDF security settings by users.
- Prevent changes to email client security settings by users.
- Prevent changes to security product settings by users.
- Implement Microsoft's attack surface reduction rules where applicable.

Control References:

- ISM-1915: Approved configurations developed, implemented, and maintained.
- ISM-1806: Change default accounts and credentials.
- ISM-1470: Disable/remove unneeded components.
- ISM-1235: Restrict add-ons and plug-ins.
- ISM-1667: Microsoft Office blocked from creating child processes.
- ISM-1668: Microsoft Office blocked from creating executable content.
- ISM-1669: Microsoft Office blocked from injecting code.
- ISM-1542: Prevent activation of Object Linking and Embedding packages.
- ISM-1859: Harden office productivity suites.
- ISM-1823: Prevent changes to Office security settings.
- ISM-1486: Web browsers blocked from processing Java.
- ISM-1485: Web browsers blocked from processing web advertisements.
- ISM-1412: Harden web browsers.
- ISM-1585: Prevent changes to browser security settings.
- ISM-1670: Block PDF software from creating child processes.
- ISM-1860: Harden PDF software.
- ISM-1824: Prevent changes to PDF security settings.
- ISM-1601: Implement Microsoft's attack surface reduction rules.
- ISM-1748: Prevent changes to email client security settings.
- ISM-1825: Prevent changes to security product security settings.

Microsoft Office Macros

Microsoft Office macros are written in Visual Basic for Applications and can automate tasks, enhancing productivity. However, macros can be exploited by malicious actors to compromise systems. Therefore, Redback Operations enforces strict controls over macro usage to minimize risks.

- Disable Microsoft Office macros for users who lack a demonstrated business need.
- Prevent macros in Microsoft Office files originating from the internet.
- Enable Microsoft Office macro antivirus scanning.
- Stop Microsoft Office macros from making Win32 API calls.
- Allow macros only if they run within a sandboxed environment, Trusted Location, or are signed by a trusted publisher.
- Verify macros are free from malicious code before signing or placing them in Trusted Locations.
- Limit modification rights to Trusted Location content to privileged users responsible for macro verification.
- Block macros signed by untrusted publishers or those using non-V3 signatures via the Message Bar or Backstage View.
- Validate Microsoft Office's list of trusted publishers annually or more frequently.
- Prevent users from changing Microsoft Office macro security settings.
- Log all allowed and blocked macro execution events centrally.

Control References

- ISM-1671: Disable Microsoft Office macros for users without a demonstrated business requirement.
- ISM-1488: Block macros in Microsoft Office files originating from the internet.
- ISM-1672: Enable Microsoft Office macro antivirus scanning.
- ISM-1673: Block Microsoft Office macros from making Win32 API calls.
- ISM-1674: Allow macros only if running from within a sandboxed environment, Trusted Location, or digitally signed by a trusted publisher.
- ISM-1890: Verify that macros are free of malicious code before signing or placing them in Trusted Locations.
- ISM-1487: Only privileged users can modify Trusted Location content.
- ISM-1675: Block macros digitally signed by untrusted publishers via the Message Bar or Backstage View.
- ISM-1891: Block macros signed with non-V3 signatures via the Message Bar or Backstage View.
- ISM-1676: Validate Microsoft Office's list of trusted publishers annually or more frequently.
- ISM-1489: Prevent users from changing Microsoft Office macro security settings.
- ISM-1677: Centrally log allowed and blocked Microsoft Office macro execution events.

Server Application Hardening

Server Applications

This section covers applications with specific server functionality, such as Microsoft Active Directory Domain Services (AD DS), database management systems, email servers, and web hosting software.

Note: User applications are covered under user application hardening.

Server Application Selection

Selecting server applications from vendors that follow secure-by-design and secure-by-default principles is critical to minimizing vulnerabilities. Vendors should also use memory-safe programming languages (C#, Go, Java, Ruby, Rust, Swift) and maintain secure programming practices. Redback Operations should prioritize vendors that:

- Follow secure-by-design and secure-by-default principles.
- Use memory-safe programming languages where possible (C#, Go, Java, Ruby, Rust, Swift).
- Maintain secure programming practices and product security.

Server Application Releases

Newer server application releases include improved security features that complicate exploitation by malicious actors. Using unsupported versions leaves organizations exposed to previously mitigated vulnerabilities.

Hardening Server Application Configurations

Default or unapproved configurations can lead to an insecure environment, making server applications prime targets for exploitation. Redback Operations should:

- Develop, implement, and maintain approved configurations for server applications.
- Use ASD and vendor guidance for hardening, prioritizing the most restrictive advice in case of conflicts.
- Modify default accounts or credentials, including pre-configured accounts.
- Disable or remove unneeded accounts, components, services, and features.
- Remove installation files and logs once applications are fully installed.

Restricting Privileges for Server Applications

If a server application runs as a local administrator or root account, it can pose a significant security risk. Applications should:

- Configure server applications to run as separate accounts with the minimum privileges needed.
- Restrict the file system access of accounts under which server applications run.

Control References

- ISM-1826: Choose server applications from vendors committed to secure principles and practices.
- ISM-1483: Use the latest release of internet-facing server applications.
- ISM-1916: Develop and maintain approved configurations.
- ISM-1246: Harden server applications using ASD and vendor guidance.
- ISM-1260: Change default accounts and credentials.
- ISM-1247: Disable or remove unneeded features.
- ISM-1245: Remove temporary installation files and logs.
- ISM-1249: Configure server applications to run as separate accounts with minimal privileges.
- ISM-1250: Limit file system access for server application accounts.

Microsoft Active Directory Domain Services (AD DS) Hardening

Microsoft AD DS Domain Controllers

Microsoft AD DS domain controllers contain highly sensitive data, including hashed credentials. Dedicated domain administrator accounts should be exclusively used for AD DS management, ensuring they can't be used to administer other systems.

- Disable the Print Spooler service on these controllers.
- Avoid using passwords in Group Policy Preferences
- Centrally log security events.

Microsoft AD DS Account Hardening

Misconfigured accounts pose a significant security risk. Malicious actors can gain access to AD DS and move laterally throughout the network. Redback Operations mitigates these risks by implementing the following guidelines:

- Only configure service and computer accounts with Service Principal Names (SPNs).
- Ensure service accounts have minimal privileges and exclude them from the domain administrators' group.
- Prevent duplicate SPNs within the domain.
- Configure privileged accounts as sensitive and prevent delegation.
- Require user accounts to use Kerberos pre-authentication.
- Password Management:
    - Don't use "password never expires" or "password not required" settings.
    - Avoid storing passwords in properties accessible to unprivileged users.
    - Don't use reversible encryption.
- Domain Access Control:
    - Prevent unprivileged users from adding machines to the domain.
    - Use dedicated service accounts for adding machines.
- Review user accounts with unconstrained delegation annually and remove those lacking a business requirement.
- Prevent non-domain controller computer accounts from being trusted for delegation.

Microsoft AD DS Security Group Memberships

Built-in security groups have elevated permissions that can be exploited. Limit vulnerabilities by ensuring:

- Privileged accounts are members of the Protected Users group.
- Remove disabled accounts from security groups.
- Ensure no user accounts are part of the Pre-Windows 2000 Compatible Access group.

Control References

- ISM-1827: Administer AD DS using dedicated domain administrator accounts.
- ISM-1828: Disable the Print Spooler service on AD DS domain controllers.
- ISM-1829: Avoid using passwords and passwords in Group Policy Preferences.
- ISM-1830: Centrally log AD DS security-related events.
- ISM-1832 to ISM-1844: Apply comprehensive account hardening controls.
- ISM-1620: Add privileged accounts to the Protected Users security group.
- ISM-1845: Remove disabled accounts from security groups.
- ISM-1846: Ensure the Pre-Windows 2000 group contains no user accounts.

Authentication Hardening

Account and Authentication Types

These guidelines apply to all account types, including unprivileged, privileged, break glass, and service accounts, covering both interactive and non-interactive authentication.

Authenticating to Systems

Users must be authenticated before gaining access to a system and its resources. This can be achieved via multi-factor authentication (MFA), such as a username with a passphrase and security key, or through single-factor authentication (SFA) as a less secure alternative.

- Authenticate users before granting system access.

Insecure Authentication Methods

Authentication methods must resist theft, interception, duplication, forgery, unauthorized access, and modification. Weak hashing algorithms in Local Area Network (LAN) Manager and NT LAN Manager (NTLM) can be easily compromised. Disable these protocols and use Kerberos for Windows authentication.

- Disable authentication methods susceptible to replay attacks.
- Disable LAN Manager and NTLM authentication methods.

Multi-Factor Authentication (MFA)

MFA uses two or more factors to confirm user identity:

- Knowledge Factors: Memorized secrets (e.g., PINs, passwords).
- Possession Factors: Security keys, smart cards, or OTP tokens.
- Inherence Factors: Biometric data (e.g., fingerprints, facial recognition).

MFA is vital for administrative activities, online services, privileged accounts, and data repositories. It helps slow down or prevent attackers from gaining unrestricted access. Key points include:

- Ensure MFA used for authenticating online services, data repositories, and systems is phishing resistant.
- Log successful and unsuccessful MFA events centrally.

Single-Factor Authentication

Single-factor authentication (SFA) remains vulnerable to credential cracking tools. If multi-factor authentication (MFA) is not supported, use SFA with strong passphrases. Key recommendations include:

- Use passphrases consisting of at least four random words (or longer, depending on classification level).
- Avoid categorically predictable words, meaningful sentences, or publicly available material.
- Log successful and unsuccessful SFA events centrally to detect malicious behaviour.

Setting Credentials for User Accounts

Ensure credentials for user accounts are securely issued and managed:

- Verify the user's identity before issuing new credentials.
- Credentials should be randomly generated.
- Provide credentials via a secure channel or split into two parts (user and supervisor).
- Ensure users change credentials on first use.
- Prevent users from reusing memorized credentials across systems.

Setting Credentials for Break Glass, Local Administrator, and Service Accounts

Common usernames or weak credentials can lead to rapid exploitation of break glass, local administrator, and service accounts. Secure these accounts by following these guidelines:

- Ensure credentials are long (at least 30 characters), unique, and unpredictable.
- Use Microsoft's group Managed Service Accounts (gMSA) to automatically manage service account credentials.
- Credentials for break glass, local administrator, and service accounts are long, unique, and managed.
- Credentials for these accounts are a minimum of 30 characters.
- Create service accounts as group Managed Service Accounts.

Changing Credentials

Credentials typically do not require frequent changes unless specific conditions arise:

- Update credentials when compromised, suspected of compromise, stored/transferred in the clear, shared account membership changes, or when not changed in 12 months.
- Change KRBTGT credentials twice if the domain is compromised, suspected of compromise, or if not updated in 12 months.

Protecting Credentials

Protect credentials by following these guidelines:

- Keep credentials separate from systems they authenticate to unless used for authentication activities.
- Conceal credentials as they are entered into systems to prevent screen scrapers and shoulder surfers.
- Use memory integrity, Local Security Authority, Credential Guard, and Remote Credential Guard functionality, preferably with UEFI lock.
- Limit cached credentials to one previous logon.
- Protect credentials with a password manager, hardware security module, or by hashing, salting, and stretching them before storage in a database.
- Regularly scan networks to identify and remediate credentials stored in the clear.

Account Lockouts

Locking accounts after several failed attempts reduces the success rate of brute-force attacks like credential guessing or spraying. Implement these practices:

- Lock accounts (except break glass) after a maximum of five failed logon attempts.

Session Termination

Terminating user sessions daily and after inactivity supports system maintenance and helps remove malicious actors lacking persistence.

Session and Screen Locking

Session and screen locks prevent unauthorized access to authenticated sessions. Key requirements include:

- Activate after 15 minutes of inactivity or when manually triggered.
- Ensure session content is concealed and the screen does not enter power-saving mode before locking.
- Require users to authenticate to unlock.
- Deny users the ability to disable the screen lock.

Logon Banner

A logon banner reminds users of security responsibilities when accessing systems. Include:

- System sensitivity/classification, access requirements, usage policies, and monitoring activities.

Control Reference:

- ISM-1546: Users are authenticated before they are granted access to a system and its resources.
- ISM-1603: Authentication methods susceptible to replay attacks are disabled.
- ISM-1055: LAN Manager and NT LAN Manager authentication methods are disabled.
- ISM-1504: Multi-factor authentication is used to authenticate users to their organisation's online services that process, store, or communicate their organisation's sensitive data.
- ISM-1679: Multi-factor authentication is used to authenticate users to third-party online services that process, store, or communicate their organisation's sensitive data.
- ISM-1680: Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store, or communicate their organisation's non-sensitive data.
- ISM-1892: Multi-factor authentication is used to authenticate users to their organisation's online customer services that process, store, or communicate their organisation's sensitive customer data.
- ISM-1893: Multi-factor authentication is used to authenticate users to third-party online customer services that process, store, or communicate their organisation's sensitive customer data.
- ISM-1681: Multi-factor authentication is used to authenticate customers to online customer services that process, store, or communicate sensitive customer data.
- ISM-1173: Multi-factor authentication is used to authenticate privileged users of systems.
- ISM-0974: Multi-factor authentication is used to authenticate unprivileged users of systems.
- ISM-1505: Multi-factor authentication is used to authenticate users of data repositories.
- ISM-1401: Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are.
- ISM-1872: Multi-factor authentication used for authenticating users of online services is phishing-resistant.
- ISM-1873: Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option.

- ISM-1874: Multi-factor authentication used for authenticating customers of online customer services is phishing-resistant.
- ISM-1682: Multi-factor authentication used for authenticating users of systems is phishing-resistant.
- ISM-1894: Multi-factor authentication used for authenticating users of data repositories is phishing-resistant.
- ISM-1559: Memorised secrets used for multi-factor authentication are a minimum of 6 characters unless more stringent requirements apply.
- ISM-1560: Memorised secrets used for multi-factor authentication on SECRET systems are a minimum of 8 characters.
- ISM-1561: Memorised secrets used for multi-factor authentication on TOP SECRET systems are a minimum of 10 characters.
- ISM-1683: Successful and unsuccessful multi-factor authentication events are centrally logged.
- ISM-0417: When systems cannot support multi-factor authentication, single-factor authentication using passphrases is implemented instead.
- ISM-0421: Passphrases used for single-factor authentication are at least 4 random words with a total minimum length of 14 characters unless more stringent requirements apply.
- ISM-1557: Passphrases used for single-factor authentication on SECRET systems are at least 5 random words with a total minimum length of 17 characters.
- ISM-0422: Passphrases used for single-factor authentication on TOP SECRET systems are at least 6 random words with a total minimum length of 20 characters.
- ISM-1558: Passphrases used for single-factor authentication are not a list of categorised words; do not form a real sentence in a natural language; and are not constructed from song lyrics, movies, literature, or any other publicly available material.
- ISM-1895: Successful and unsuccessful single-factor authentication events are centrally logged.
- ISM-1593: Users provide sufficient evidence to verify their identity when requesting new credentials.
- ISM-1227: Credentials set for user accounts are randomly generated.
- ISM-1594: Credentials are provided to users via a secure communications channel or, if not possible, split into two parts with one part provided to users and the other part provided to supervisors.
- ISM-1595: Credentials provided to users are changed on first use.
- ISM-1596: Credentials, in the form of memorised secrets, are not reused by users across different systems.

- ISM-1685: Credentials for break glass accounts, local administrator accounts, and service accounts are long, unique, unpredictable, and managed.
- ISM-1795: Credentials for break glass accounts, local administrator accounts, and service accounts are a minimum of 30 characters.
- ISM-1619: Service accounts are created as group Managed Service Accounts.
- ISM-1590: Credentials are changed if:
    - they are compromised.
    - they are suspected of being compromised.
    - they are discovered stored on networks in the clear
    - they are discovered being transferred across networks in the clear
    - membership of a shared account changes
    - they have not been changed in the past 12 months.
- ISM-1847: Credentials for the Kerberos Key Distribution Centre's service account (KRBTGT) is changed twice, allowing for replication to all Microsoft Active Directory Domain Services domain controllers in-between each change, if:
    - the domain has been directly compromised.
    - the domain is suspected of being compromised.
    - they have not been changed in the past 12 months.
- ISM-0418: Credentials are kept separate from systems they are used to authenticate to, except for when performing authentication activities.
- ISM-1597: Credentials are obscured as they are entered into systems.
- ISM-1896: Memory integrity functionality is enabled.
- ISM-1861: Local Security Authority protection functionality is enabled.
- ISM-1686: Credential Guard functionality is enabled.
- ISM-1897: Remote Credential Guard functionality is enabled.
- ISM-1749: Cached credentials are limited to one previous logon.
- ISM-1402: Credentials stored on systems are protected by a password manager; a hardware security module; or by salting, hashing, and stretching them before storage within a database.
- ISM-1875: Networks are scanned at least monthly to identify any credentials that are being stored in the clear.
- ISM-0428: Implement comprehensive session/screen locking practices.
- ISM-0428: Implement comprehensive session/screen locking practices.
- ISM-0408: Display a logon banner reminding users of security responsibilities.
- ISM-0428: Implement comprehensive session/screen locking practices.

Virtualization Hardening

Hypervisors

Both Type 1 and Type 2 hypervisors must be treated according to their role:

- Type 1 Hypervisors: Run on bare metal and should be treated as lightweight operating systems.
- Type 2 Hypervisors: Run on top of general-purpose operating systems and should be treated as applications.

Containerization

Containers offer versatile deployment but must be managed like any system.

- Applying patches and ensuring patched images are used is crucial.

Functional Separation Between Computing Environments

Malicious actors can exploit misconfigurations or vulnerabilities in software-based isolation mechanisms to compromise multiple environments. Key practices include:

- Choose isolation mechanism vendors following secure-by-design and secure-by-default principles while maintaining product security.
- Restrict administrative access and remove unnecessary functionality from isolation mechanisms.
- Secure the underlying operating system through comprehensive hardening.
- Promptly apply patches, updates, and mitigations for both the isolation mechanism and underlying OS.
- Replace outdated isolation mechanisms and OS software.
- Perform integrity and log monitoring for both isolation mechanisms and underlying OS.
- Physical servers used for SECRET and TOP SECRET computing environments should only host environments of the same classification and security domain.

Control References:

- ISM-1460: Select isolation mechanisms from secure vendors.
- ISM-1604: Harden isolation mechanisms and restrict administrative access.
- ISM-1605: Harden the underlying OS.
- ISM-1606: Apply patches, updates, and mitigations promptly.
- ISM-1848: Replace isolation mechanisms and OS when unsupported.
- ISM-1607: Monitor integrity and logs of isolation mechanisms and OS.
- ISM-1461: Use servers of the same classification/security domain for SECRET/TS environments.

Policy Review

The objective of this policy review section is to ensure that the security controls and guidelines within the Server Security Policy remain relevant, effective, and aligned with evolving security threats, organizational needs, and compliance requirements.

Note: Company layout and infrastructure does not reflect the standards outline in this policy at the time of this document's creation and is considered a long-term strategy to implement when company maturity has improved.

Responsibility for Reviews

The Chief Information Security Officer (CISO) is designated as the primary initiator of the reviews for the cyber security policy at Redback Operations. A review committee assists in evaluating the effectiveness and relevance of the policy.

Frequency of Reviews

Reviews are scheduled to occur at least annually. However, more frequent reviews are conducted if there are significant changes in technology, business practices, or compliance requirements. Ad-hoc reviews are also permitted in response to security incidents or major failures in the existing policy.

Proposing and Approving Changes

Any member of the review committee can propose changes during the review process. These proposals should be supported by a rationale and, where possible, data to substantiate the change. After a thorough discussion within the committee, the CISO presents the proposed changes to senior management for approval.

Communication Plan for Updates

Once changes are approved, the updated policy is communicated to all stakeholders through internal memos, meetings, and training sessions. All employees must understand the changes and how they impact their roles and responsibilities. Regular training sessions are updated to reflect the new policy standards.

Appendix

https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-hardening

(Australian Signals Directorate, Guidelines for System Hardening, May 12 2024)