Cryptography Policy

SIT374 Team Project A

Redback Operations

Version	Modified By	Approver	Date	Changes made
V0.2	Daniel McAulay	Daniel McAulay	8/04/2024	Document Creation

Contents

Purpose

The primary purpose of this Encryption/Cryptography Cybersecurity Policy (hereafter referred to as "the policy") is to ensure the confidentiality, integrity, and availability of the organization's digital assets.

Encryption and cryptography are vital components of our information security strategy, protecting sensitive data against unauthorized access, disclosure, alteration, and destruction. This policy outlines the requirements for the use of cryptographic measures to safeguard data in transit, at rest, and during processing.

Scope

This policy applies to all employees, contractors, and third-party partners of Redback Operations who have access to I.T. systems and data owned, controlled, or managed by the organization.

The scope covers all forms of sensitive information that the organization processes, stores, or transmits, including but not limited to personally identifiable information (PII), financial records, intellectual property, and any other data classified as confidential by the organization. For further details regarding sensitive information types & relevant classifications, refer to the **Data Classification & Data Loss Prevention Policies** outlined in the ISMS.

Compliance with this policy is mandatory for all applicable entities within the scope. Failure to adhere to the policy's guidelines may result in disciplinary action, up to and including termination of employment or contracts and legal action.

Framework References:

The Cryptography Policy references the following framework controls:

ISO 27001 Controls:

A.5.24: Cryptographic Controls

A.8.6: Secure Log-on Procedures

A.8.7: Information Transfer

A.9.4: Physical Entry Controls

A.10.1: Management of Technical Vulnerabilities

A.10.2: Backups

A.10.7: Information Disposal

A.10.8: Logging and Monitoring

CIS Controls:

Control 3: Data Protection

Control 4: Vulnerability Management

Control 6: Account Management

Control 8: Audit Log Management

Control 10: Data Recovery

Control 12: Network Infrastructure Management

Roles and Responsibilities

The purpose of the Roles and Responsibilities section of this policy is to clearly define the duties & accountabilities of various stakeholders in implementing and upholding Redback Operations' encryption practices.

The section defines specific encryption-related tasks & identifies broad scenarios of individual stakeholders to ensure the secure handling of sensitive information, aligning with regulatory obligations and enhancing overall data security. This clarity helps establish accountability and streamline efforts across the organization for effective encryption management.

Chief Information Security Officer (CISO)

Leads encryption strategy and policy, ensures regulatory compliance, and manages encryption-related breaches.

- Leads the development and implementation of encryption strategies.
- Ensures policy compliance with business objectives and regulations.
- Directs incident response for encryption-related breaches.

IT Department

Implements encryption technologies, maintains security infrastructure, and provides technical support.

- Implements and maintains encryption solutions.
- Provides technical support for encryption issues.
- Manages encryption infrastructure and auditing.

Security Team

Identifies encryption needs through risk assessments, oversees encryption compliance, and conducts security training.

- Identifies data needing encryption through risk assessments.
- Oversees the effectiveness and compliance of encryption measures.
- Delivers encryption best practices training.

Developers

Incorporates encryption into applications, adheres to encryption standards, and secures application data in collaboration with IT and Security.

- Integrates encryption into software/app development life cycles.
- Ensures applications comply with encryption standards.
- Collaborates with IT and security teams to secure application data.

End-Users

Follows encryption protocols for data handling, engages in security training, and reports encryption security incidents.

- Follows encryption guidelines for handling sensitive information.
- Participates in encryption training and awareness initiatives.
- Reports security incidents involving encrypted data.

Data Owners

Classifies sensitive data for encryption and maintains ongoing compliance with encryption policies.

- Classifies data and ensures it's encrypted according to policy.
- Regularly reviews data classification and encryption needs.

The summary of stakeholders and end-user scenarios ensures that all parties involved in the data lifecycle at Redback Operations are aware of their duties regarding encryption, contributing to the organization's overall data security posture.

Compliance with this policy is the responsibility of all individuals who have access to the organization's information systems and data. The roles and responsibilities outlined above are not exhaustive and may include additional duties as required by the organization's needs and as technologies evolve.

RACI Chart

A RACI chart is a management tool that outlines the roles and responsibilities of different team members for specific tasks or processes. The chart helps clarify expectations, improves communication, and ensures that all tasks have clear ownership, making it easier to manage projects and processes efficiently.

Legend:

R (Responsible):

Person or group who performs the activity.

A (Accountable):

Person who is ultimately accountable and has Yes/No/Veto power.

C (Consulted):

Person or group that provides information and/or expertise.

I (Informed):

Person or group that needs to be informed after the decision or action is taken.

Activity/Role	CISO	IT Department	Security Team	Developers	End-Users	Data Owners
Develop Encryption Strategy	A	C	R	C	I	I
Implement Encryption Tools	C	R	A	R	I	I
Conduct Risk Assessments	A	C	R	I	I	R
Oversee Compliance	A	C	R	C	I	C
Deliver Training Programs	C	R	A	R	R	I
Report Security Incidents	C	C	R	C	R	C
Integrate Encryption in Apps	C	R	C	A	I	I
Classify and Encrypt Data	I	C	C	C	I	A

Data Classification

To ensure the effective application of encryption controls and to safeguard sensitive information, Redback Operations classifies data into categories based on its sensitivity, regulatory requirements, and the impact on the organization should the data be disclosed, altered, or destroyed without authorization.

Classification Levels

- ***Public****:* Data intended for public disclosure. Encryption is not required for public data, but best practices for integrity should still be applied.
- ***Internal Use Only****:* Data that is not sensitive but is intended for use within the organization. Basic encryption controls are recommended to prevent unauthorized disclosure.
- ***Confidential****:* Sensitive data that could cause harm to the organization or individuals if disclosed. Encryption in transit and at rest, using industry-standard algorithms and key strengths, is required.
- ***Restricted****:* Highly sensitive data that if disclosed could result in significant harm or legal/regulatory non-compliance. Strong encryption, both in transit and at rest, with strict access controls and key management procedures, is mandatory.

Implementation Guidelines

Implementation Guidelines provide a practical roadmap for applying Redback Operations' encryption protocols across all relevant data handling activities. It outlines actionable steps for encrypting data in various states, whether at rest, in transit, or in use, and specifies the use of approved encryption technologies and methodologies.

This section ensures consistent and effective encryption practices are followed, enhancing the security of sensitive information throughout the organization.

- *Risk-Based Approach:* The application of encryption must be based on a risk assessment, considering the nature of the data, the context in which it is used, and the potential impact of its compromise.
- *Default Encryption:* Unless classified as Public, all data stored on mobile devices, transmitted over public or untrusted networks, or stored in the cloud must be encrypted by default.
- *Data at Rest:* All Confidential and Restricted data stored on servers, workstations, laptops, or removable media must be encrypted.
- *Data in Transit:* Encryption must be applied to all Confidential and Restricted data being transmitted over any network, including internal networks, using secure protocols such as TLS, SSH, or VPN.
- *End-to-End Encryption:* For highly sensitive communications, end-to-end encryption must be used to prevent interception or man in the middle attacks by unauthorized parties.

Data Stewardship

Data owners are responsible for classifying their data according to this policy and ensuring appropriate encryption measures are applied and maintained. IT and security teams must provide the necessary tools and support to enable data owners, developers, and users to comply with these requirements.

This classification and the accompanying guidelines ensure that sensitive information receives the highest level of protection, while less sensitive information is protected in a manner proportionate to its value and risk.

Encryption Standards

Redback Operations is committed to using secure encryption standards to protect sensitive and confidential data against unauthorized access. This section outlines the approved encryption algorithms, protocols, and key management practices.

Secure Protocols

- **Data in Transit**
  - TLS (Transport Layer Security) 1.2 or higher must be used for all data transmitted over public networks. This includes the use of secure versions of protocols for email, file transfer, and other communications.
  - Insecure protocols such as SSL2, SSL3, TLS 1.0 & TLS 1.1 are forbidden to be utilized without an existing security exemption. These protocols contain known vulnerabilities and should not be utilized.
- **Data at Rest**
  - **Symmetric Encryption**
    - For internal encryption needs, including data at rest, AES (Advanced Encryption Standard) with key sizes of 256 bits is approved.
  - **Asymmetric Encryption**
    - For digital signatures and key exchange mechanisms, RSA with a minimum key size of 2048 bits or ECC with a minimum key size of 256 bits are approved.
  - **Hashing**
    - SHA-256 or higher is approved for hashing operations.

Compliance and Auditing

- All use of encryption must comply with these standards, and exceptions must be approved by the Chief Information Security Officer (CISO).
- Regular audits should be conducted by the security & I.T. teams (refer to RACI chart) to ensure compliance with these encryption standards, identifying and mitigating any scenarios that do not comply with this policy.

Adhering to these encryption standards is mandatory for all personnel involved in the handling of sensitive and confidential data. This ensures that Redback Operations' data remains secure against emerging threats and vulnerabilities.

Key Management

Effective key management is a requirement to maintain the confidentiality, integrity & availability of encrypted data. Note that at the time of writing this document, technical controls are limited due to pending infrastructure deployments, however this policy assumes the future use of Active Directory Certificate Authorities in the design of this solution.

Private Key Infrastructure

Note: The following section is a theoretical high-level design due to the nature of upcoming implementations. No PKI solution is implemented at the time of writing this policy.

Private Key Infrastructure (PKI) is a framework used to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. At the core of PKI is the Certificate Authority (CA), which issues digital certificates to verify the ownership of a public key by the named subject of the certificate.

This system enables users and computers to exchange data securely over the internet and verify the authenticity of the party they're communicating with, essentially underpinning various internet security and data encryption protocols. CAs play a crucial role in the PKI by ensuring the digital certificates they issue are created and distributed in a secure manner, providing the foundation for a trusted digital environment.

Redback Operations' Certificate Authority (CA) Hierarchy is structured to secure digital certificates crucial for encrypted communications and secure identity verification. The hierarchy includes:

Root Certificate Authority (Root CA)

Serves as the trust anchor, issuing certificates to Intermediate CAs. The Root CA's operations are highly secure, with its key stored offline to minimize risk. It has a long validity period due to its foundational role in the trust chain.

Intermediate Certificate Authorities (Intermediate CAs)

Intermediate CA’s sit between the Root CA and end entities, issuing certificates to devices, servers, and users. This layer of the certificate hierarchy adds flexibility and enhances security by limiting the Root CA's direct exposure and delegating certificate management roles between Intermediate CA’s. Certificates from Intermediate CAs have shorter validity periods for security and operational efficiency.

End Entity Certificates

Issued to devices, servers, and users for secure communication within Redback Operations' network. Managed by Intermediate CAs to maintain the Root CA's integrity.

The CA Hierarchy employs Certificate Revocation Lists (CRLs) and the Online Certificate Status Protocol (OCSP) to manage the revocation status of certificates, ensuring the immediate identification and distrust of compromised certificates.

The CA operations comply with industry best practices and regulatory standards, including the CA/Browser Forum Baseline Requirements. Regular internal and external audits ensure the integrity of CA operations, certificate issuance, management, and revocation processes. This structured approach is critical for maintaining secure and trusted communication within and outside Redback Operations.

Certificate Authority Hierarchy

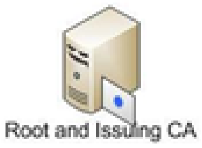
The following section is based on a theoretical design for an upcoming virtualized environment deployment on-premises. While the initial deployment for Redback Operations will be Single Tier, our future target state will be based on improving our maturity for certificate management by moving to an environment that uses delegated CA roles in a more complex hierarchy.

Single/One Tier Hierarchy (Current)

- **Structure**: Combines the roles of Root Certificate Authority (CA) and Issuing CA into a single entity.
- **Use Case**: Suited for simple implementations where manageability and cost are more critical than the highest levels of security.
- **Security**: Can be enhanced with a Hardware Security Module (HSM) to protect the CA’s keys, though this adds to the cost.

Example:

References: (Microsoft Learn, Designing & Implementing a PKI, 2024)

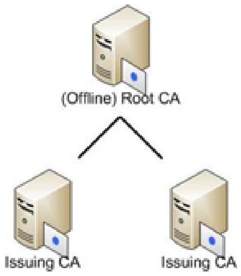


Two Tier Hierarchy

- Structure: Consists of an offline Root CA and one or more online Subordinate (Issuing) CAs.
- Use Case: Balances security, scalability, and flexibility, meeting the needs of most organizations.
- Security: The offline Root CA enhances security by protecting the root key from compromise. Scalability is achieved through the possibility of having multiple Issuing CAs under the Root CA.

Example:

References: (Microsoft Learn, Designing & Implementing a PKI, 2024)

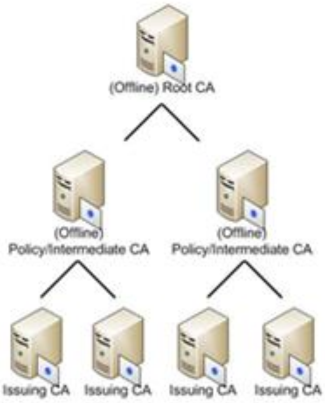


Three Tier Hierarchy

- Structure: Introduces an additional layer between the Root CA and the Issuing CAs, often referred to as a Policy CA.
- Use Case: Provides enhanced security and policy enforcement, serving as an administrative boundary within larger or more security-conscious organizations.
- Security: Allows for more granular control over certificate issuance policies and further isolates the Root CA from exposure, as the Policy CA handles specific operational policies or geographical distinctions.

Example:

References: (Microsoft Learn, Designing & Implementing a PKI, 2024)


(Offline) Root CA
(Offline) Policy/Intermediate CA
(Offline) Policy/Intermediate CA
Issuing CA
Issuing CA
Issuing CA
Issuing CA

Key Management

Note: The following section is a theoretical high-level design due to the nature of upcoming implementations. No PKI solution is implemented at the time of writing this policy.

This section of the cryptography policy refers to standards that must be followed, and guidelines that provide direction and support subject to the context of a system being built or audited.

Key Generation

Key generation is defined as the process of creating cryptographic keys that are used to encrypt and decrypt data. It's the foundation of an organization's communication and data protection initiative.

Redback Operations Key Generation standard ensures that the keys generated are strong and secure enough to protect against unauthorized access and decryption attempts. Additionally, it ensures that specific cryptographic algorithms are recommended and followed due to their proven security strength and effectiveness.

Guideline & Standards

- Utilize cryptographic modules compliant with FIPS 140-2 Level 3 or higher for key generation, ensuring high entropy and unpredictability. Algorithms such as:
  - RSA (4096-bit for added security)
  - ECC (Curve P-384)
  - AES (256-bit)
- Only use cryptographic modules certified under global standards such as:
  - FIPS 140-2
  - Common Criteria EAL4+

Key Distribution

Key distribution is the secure method of transferring cryptographic keys from one entity to another, ensuring that the keys are received and utilized solely by intended recipients. The Redback Operations Key Distribution standard safeguards the transmission and authentication process, thereby guaranteeing that the distribution of keys does not compromise their security.

Guideline & Standards

- Ensure the use of secure encryption protocols such as TLS 1.3 ciphers for the transmission of keys over networks.
  - This protocol enhances the security of key exchanges by ensuring encryption keys are not compromised, even if the server key is.
  - For internal transfer, use secure, encrypted containers with two-factor authentication for access.
- Secure authentication utilizing Multi-Factor Authentication & digital signatures. This step is crucial to ensure that cryptographic keys are only issued to verified individuals, thereby preventing unauthorized access.

Key Storage

Key storage concerns the secure preservation of cryptographic keys, ensuring they are accessible solely by authorized systems and personnel.

The Redback Operations Key Storage standard focuses on encrypting and physically securing keys to prevent unauthorized access and compromise.

Guideline & Standards

- Apply AES-256 encryption for storing keys digitally.
    - This method utilizes a strong symmetric key algorithm to ensure the confidentiality and integrity of stored keys.
    - Use hardware security modules (HSMs) that are FIPS 140-2 Level 3 certified for high-security environments.
- Store physical storage media in tamper-evident containers within secure facilities.
    - Access should only be granted through biometric verification and Multi-Factor Authentication, further ensuring the security of physical keys.
- Adhere to established IDAM/IAM (Identity and Access Management) policies, ensuring minimal privilege access based on job roles.
    - Employ access logging and continuous monitoring for unauthorized access attempts.

Key Rotation

Key rotation involves the regular updating of cryptographic keys to mitigate the risk associated with the compromise of a single key. The Redback Operations Key Rotation standard specifies the frequency and procedure for changing keys, aiming to enhance the security of encrypted data over time.

Guideline & Standards

- Implement automated key rotation for sensitive systems every 90 days or based on the sensitivity of the data being protected. Critical systems may require more frequent rotations.
  - Implement an automated key rotation schedule that mandates the updating of cryptographic keys at predefined intervals.
  - For keys protecting highly sensitive data, rotate at least every 90 days. For less sensitive data, a rotation period of up to 180 days may be acceptable.
  - Document and justify any deviations from the standard rotation periods based on specific risk assessments or operational requirements.
- Automate the rotation process where possible using key management systems such as ACME **(Automatic Certificate Management Environment)** that support seamless rollover to new keys without service interruption, ensuring all old keys are replaced securely across systems.

Key Recovery

Key recovery ensures that cryptographic keys can be securely retrieved in case of loss or compromise, maintaining the availability and integrity of encrypted data. The Redback Operations Key Recovery standard establishes protocols for the backup and recovery of keys, ensuring that data remains accessible under all circumstances.

Guideline & Standards

- Implement automated backups of keys into secure, segregated storage solutions, with encryption in transit and at rest.
  - Ensure backups are geographically distributed/redundant to mitigate against regional failures.
- Establish strict protocols for key recovery, requiring dual authorization from senior security personnel and logging all recovery actions for audit purposes.

Key Destruction

Key destruction involves the secure deletion or destruction of cryptographic keys when they are no longer necessary, preventing unauthorized access to encrypted data. The Redback Operations Key Destruction standard focuses on methods that ensure keys are irrecoverably destroyed, safeguarding against unauthorized data decryption.

Guideline & Standards

- Use cryptographic erasure techniques to render keys unrecoverable from storage media. Approved techniques include:
    - Cryptographic Erasure (Crypto Shredding) – Directly deletes the encryption key, making encrypted data permanently inaccessible.
    - Physical Destruction – Physically damages storage media (shredding, drilling, crushing) to prevent key retrieval.
    - Overwriting – Writes random data over the location of the key multiple times to erase it.
    - Degaussing – Uses a powerful magnet to disrupt magnetic fields, erasing data on magnetic storage media.
        - Secure Deletion Software – Employs software to overwrite the key space with zeros and ones, following data destruction standards.
    - Hardware Security Module (HSM) – Functions Utilizes HSMs' built-in functions for secure key deletion, ensuring keys within are irrecoverable.
- Maintain detailed logs of key destruction processes, including the justification for destruction and the methods used.

Audit and Compliance

Audit and compliance within key management ensure adherence to established policies and regulatory requirements through regular monitoring, logging, and review. Redback Operations' Audit and Compliance standard emphasizes the need for continuous oversight and validation of key management practices to maintain the integrity and security of cryptographic operations.

Guideline & Standards

- Maintain detailed logs of all key management activities, including generation, distribution, storage, rotation, recovery, and destruction of keys. Use Security Information and Event Management (SIEM) tools for real-time monitoring and analysis. Refer to the **Monitoring & Logging Policy** for more information.
- Conduct a regular audit schedule following the below guidelines:
  - Conduct internal audits bi-annually to evaluate adherence to key management policies and identify areas for improvement.
  - Ensure audit findings are benchmarked against established industry frameworks referenced in the Information Security Management System (ISMS).
  - Update key management policies and practices based on findings from audits and reviews, as well as in response to new threats, technological advances, and regulatory changes.
- Regularly review key management processes and policies to ensure they align with the latest industry standards, regulatory requirements, and best practices.
- Adhere to existing **Incident Response and Remediation** strategies detailed as part of Redback Operations cyber security strategy:
  - Ensure that incident response & remediation plans are implemented for solutions impacted under this policy.
  - Ensure incidents are raised for addressing non-compliance issues and security vulnerabilities identified during audits.
- Document all remediation actions taken and perform follow-up audits to ensure effective resolution.

Key Lifecycle Summary

Adherence to these key management practices ensures the security of cryptographic keys throughout their lifecycle, thereby protecting the encrypted data they secure. This comprehensive approach to key management is a cornerstone of Redback Operation's initiative to maintain data security and privacy.

End-User Encryption Guidelines

To ensure the security of sensitive data and compliance with Redback Operations' encryption policy, all end-users are required to adhere to the following encryption guidelines.

Note: Content provided in this section should correlate to other ISMS policies & training modules that is referenced in the Redback Operations' ISMS. Refer to these policies for further details relating to guidance and compliance.

Email & File Encryption

- Emails containing sensitive or confidential information must be encrypted. Use the organization-approved email encryption tool.
- Encrypt attachments containing sensitive data before sending them via email.
- Verify the identity of email recipients before sending sensitive information.
- Encrypt files containing sensitive data before storing them on drives or sharing them through file-sharing platforms.
- Use approved encryption tools and follow the provided instructions for encrypting files.
- If a password is used to encrypt a file, ensure it is strong and shared securely with the recipient.

Secure Data Transmission

- Use secure methods, such as VPNs or encrypted file transfer services, for transmitting sensitive data.
    - Avoid transmitting sensitive information over public Wi-Fi networks. If necessary, use a secure VPN connection.
- Ensure that any sensitive data stored on or accessed from mobile devices is encrypted.

Best Practices for Encryption

- Be aware of the types of data that require encryption according to the data classification policy.
- Use strong, unique passwords for accessing encrypted data and change them regularly.
- Keep devices that store or access encrypted data secure. Implement physical security measures and ensure devices are locked when not in use.
- Immediately report any suspected security incidents or difficulties in using encryption tools to the IT or security department.

Adherence to these guidelines is critical for maintaining the confidentiality and integrity of sensitive information within Redback Operations. All employees, contractors, and third-party partners are expected to comply with these guidelines to protect themselves and the organization from data breaches and other security risks.

Policy Review and Update

To ensure the encryption/cryptography policy remains effective and relevant, Redback Operations commits to a regular review and update process.

The objective of the Policy Review and Update section is to ensure that the Encryption/Cryptography Cybersecurity Policy remains current, effective, and aligned with the evolving landscape of cybersecurity threats, technological advancements, regulatory changes, and organizational needs. Regular reviews and updates will facilitate the continuous improvement of encryption practices to safeguard sensitive data effectively.

Review Schedule & Update Process

The encryption policy will be reviewed at least bi-annually to assess its effectiveness and compliance with current laws and regulations. Additional reviews will be conducted in response to significant changes in the cybersecurity landscape, including new threats, vulnerabilities, technologies, or regulatory requirements.

Review Guidance & Considerations

- Gather input from key stakeholders, including IT, security teams, legal, compliance, and business units, to identify areas for improvement.
- Incorporate emerging best practices and standards in encryption and data protection.
- Update the policy to reflect advances in encryption technologies and methodologies.
- Ensure the policy aligns with current legal and regulatory requirements related to data protection and privacy.
- Communicate any changes to the encryption policy to all affected parties promptly (Refer to the RACI chart for further information).
- Update training and awareness programs to reflect changes in the policy and emerging threats.

The commitment to continuous improvement through training, awareness, and regular policy reviews is essential for maintaining the security and integrity of sensitive information within Redback Operations.