

Cryptography and Key Management Policy

Purpose

Cryptography protects the confidentiality and integrity of information that Your Organization holds and transmits. Weak algorithms, poorly protected keys, and expired certificates are common causes of avoidable exposure. This policy sets the minimum cryptographic protections and the way keys are managed across their life.

Scope

This policy applies to all Your Organization systems, applications, endpoints, backups, and third-party services that store, process, or transmit Your Organization or customer data, and to every cryptographic key, secret, and certificate used to protect them. It applies to workforce members and to vendors acting on behalf of Your Organization.

Roles and responsibilities

- **The security team** owns this policy, maintains the approved algorithm and protocol list, and reviews exceptions.
- **System and key owners** are accountable for the keys and certificates of the systems they own, including inventory, rotation, and renewal.
- **Engineering and IT** implement the controls and do not create their own cryptographic schemes.

Requirements

1. Use of cryptography

- Data classified as confidential or higher in the Data Classification Policy must be encrypted in transit and at rest.
- All traffic over public or untrusted networks is encrypted. Internal traffic that carries confidential data is encrypted unless a documented exception applies.
- Laptops, mobile devices, and removable media that can hold company data use full-disk or device encryption.
- Databases, object storage, and backups holding confidential data are encrypted at rest using the platform's managed encryption or an equivalent control.
- Where regulations or contracts require validated cryptographic modules (for example, FIPS 140 validated modules for federal or defense data), the validated module is used and the validation certificate is recorded.

2. Approved algorithms and protocols

- The security team maintains the approved list, based on current guidance from recognized standards bodies. Examples of what the list contains: current TLS versions, authenticated encryption for data at rest, strong hash functions for integrity, and modern key-derivation or password-hashing functions for credentials.
- Deprecated or broken algorithms and protocols (for example, obsolete TLS versions, weak hash functions, and short keys) must not be used for new designs and must be retired from existing systems on a plan approved by the security team.
- Developers use vetted cryptographic libraries. Custom or home-grown cryptography is prohibited.

3. Key management

- **Generation.** Keys are generated using approved random sources, in the system or service that will use them, and are never generated from guessable values.
- **Storage.** Keys are stored in a managed key service, hardware security module, or secrets manager. Keys are never stored in source code, tickets, chat, or unprotected configuration files. Key-encrypting keys are kept separate from the data keys they protect.
- **Access.** Access to keys follows least privilege and separation of duties. Use of key administration functions is logged and the logs are reviewed.
- **Rotation.** Keys are rotated on a defined schedule set by the key owner and the security team, and immediately on suspected compromise, on departure of a person with key access, or on a change of trust relationship.
- **Backup and recovery.** Keys needed to recover encrypted data have a protected backup and a tested recovery process.
- **Retirement and destruction.** Retired keys are disabled, retained only as long as required to decrypt archived data, and then securely destroyed.

4. Certificates

- A certificate inventory records each certificate, its owner, its issuer, and its expiry date.
- Public-facing certificates are issued by a trusted certificate authority and renewed automatically where possible. Expiry alerts fire at least 30 days in advance.
- Private keys of certificates are protected under the same rules as other keys.

5. Compromise response

A suspected key or certificate compromise is reported as a security incident under the Incident Response Plan. The affected key is revoked and replaced, data protected by it is assessed for exposure, and the cause is recorded.

Exceptions

An exception must be requested in writing with the business reason, the data affected, the compensating controls, and an expiry date. The security team approves it, and the exception is tracked until closed.

Enforcement

Violations may result in disciplinary action in line with the Acceptable Use Policy, and in suspension of access to the affected system.

Evidence

Evidence of operation includes encryption configuration settings, TLS scan results, key inventory and rotation records, key-service access logs, and the certificate inventory.

Review cadence

This policy and the approved algorithm list are reviewed annually by the security team, or sooner when a standard is deprecated or a relevant vulnerability is disclosed.

Effective date: [the date this policy takes effect]