Generate a policy for key management.

**Key Management Policy**

**1. Purpose**

The purpose of this policy is to establish guidelines and procedures for the secure management of cryptographic keys within [Organization Name]. This policy aims to ensure the confidentiality, integrity, and availability of keys used for encryption, decryption, authentication, and digital signatures.

**2. Scope**

This policy applies to all employees, contractors, and third parties who have access to [Organization Name]'s information systems and cryptographic keys.

**3. Key Management Roles and Responsibilities**

* **Key Owner**: Responsible for the overall management and security of cryptographic keys.
* **Key Custodian**: Responsible for the day-to-day management and protection of keys.
* **Key User**: Individuals who use keys for encryption, decryption, or digital signatures.
* **Security Officer**: Oversees compliance with this policy and investigates any security incidents.

**4. Key Generation**

* Keys must be generated using approved cryptographic algorithms and key lengths.
* Key generation must be performed using secure, trusted systems.
* Keys must be generated in a secure environment to prevent unauthorized access.

**5. Key Storage**

* Keys must be stored in secure, access-controlled environments such as Hardware Security Modules (HSMs) or secure key vaults.
* Access to stored keys must be restricted to authorized personnel only.
* Backup copies of keys must be stored in secure, off-site locations.

**6. Key Usage**

* Keys must be used only for their intended purposes.
* Keys must not be shared or disclosed to unauthorized individuals.
* Key usage must be logged and monitored for suspicious activities.

**7. Key Rotation**

* Keys must be rotated periodically to reduce the risk of compromise.
* The frequency of key rotation must be based on the sensitivity of the data and the risk assessment.
* Old keys must be securely archived or destroyed after rotation.

**8. Key Revocation and Destruction**

* Keys must be revoked immediately if they are suspected to be compromised.
* Revoked keys must be added to a Certificate Revocation List (CRL) or other revocation mechanisms.
* Keys must be securely destroyed when they are no longer needed.

**9. Key Recovery**

* Procedures must be in place for the secure recovery of keys in case of loss or corruption.
* Key recovery processes must be documented and tested regularly.

**10. Incident Response**

* Any suspected or confirmed compromise of keys must be reported immediately to the Security Officer.
* Incident response procedures must be followed to investigate and mitigate the impact of key compromises.

**11. Compliance and Auditing**

* Compliance with this policy must be regularly audited.
* Audits must include reviews of key management practices, access controls, and incident response procedures.
* Non-compliance with this policy may result in disciplinary action.

**12. Review and Update**

* This policy must be reviewed and updated regularly to ensure its effectiveness and relevance.
* Updates to this policy must be communicated to all relevant personnel.

**Approval**

This Key Management Policy has been approved by:

[Name] [Title] [Date]