Generate a policy for key management.

**Key Management Policy**  
**Effective Date:** [Insert Date]  
**Last Reviewed:** [Insert Date]  
**Policy Owner:** [IT Security Team/Chief Information Security Officer]

**1. Purpose**

This policy establishes guidelines for the secure generation, distribution, storage, rotation, and destruction of cryptographic keys to protect sensitive data and systems. It ensures compliance with regulatory requirements (e.g., GDPR, HIPAA, PCI-DSS) and mitigates risks associated with unauthorized access or misuse of keys.

**2. Scope**

Applies to:

* All employees, contractors, and third parties who generate, manage, or use cryptographic keys.
* All cryptographic keys, including symmetric (e.g., AES), asymmetric (e.g., RSA, ECC), API keys, SSH keys, and digital certificates.

**3. Key Generation**

* **Standards**:
  + Symmetric keys: Minimum 256-bit (e.g., AES-256).
  + Asymmetric keys: RSA-3072 or higher, ECC with 256-bit or higher.
  + Use FIPS 140-2/3-validated or ISO-certified tools for generation.
* **Randomness**: Secure, approved algorithms (e.g., NIST-approved DRBGs).
* **Prohibited Actions**:
  + Hardcoding keys in source code or configuration files.
  + Reusing keys across multiple systems or applications.

**4. Key Storage & Access Control**

* **Storage**:
  + Hardware Security Modules (HSMs) or secure key vaults (e.g., AWS KMS, Azure Key Vault).
  + Keys must never be stored in plaintext.
* **Access**:
  + Least privilege: Access granted only to authorized roles (e.g., system admins, security team).
  + Multi-factor authentication (MFA) required for accessing key management systems.
  + Split knowledge (e.g., Shamir’s Secret Sharing) for master keys.
* **Logging**: All access attempts and modifications must be audited.

**5. Key Distribution**

* **Secure Channels**: TLS 1.2+ or equivalent for transmission.
* **Encryption**: Keys in transit must be encrypted with a stronger key than the payload.
* **Automation**: Prefer automated, audited distribution mechanisms over manual processes.

**6. Key Rotation & Expiration**

* **Rotation Intervals**:
  + Asymmetric keys: 12–24 months.
  + Symmetric keys: 90 days (high-risk systems) to 1 year.
  + Immediate rotation if compromise is suspected.
* **Expiration**: Keys must have defined expiration dates aligned with data sensitivity. Notify stakeholders 30 days prior to expiration.

**7. Key Revocation & Destruction**

* **Revocation**: Immediately revoke keys if:
  + Compromised or suspected of compromise.
  + Personnel with access depart the organization.
* **Destruction**:
  + Use cryptographic erasure or physical destruction (e.g., degaussing).
  + Document destruction with a certificate of disposal.

**8. Audit & Monitoring**

* **Audits**: Conduct bi-annual reviews of key management practices.
* **Monitoring**: Real-time alerts for unauthorized access or usage anomalies.
* **Log Retention**: Retain access/audit logs for at least 2 years.

**9. Incident Response**

* Report suspected key breaches to the Security Team within 1 hour.
* Isolate affected systems and revoke compromised keys immediately.
* Post-incident review to update policies and prevent recurrence.

**10. Compliance & Enforcement**

* **Training**: Annual training for personnel with key management responsibilities.
* **Penalties**: Non-compliance may result in disciplinary action, up to termination.

**11. Roles & Responsibilities**

* **Security Team**: Oversee policy implementation and audits.
* **IT Operations**: Manage daily key lifecycle operations.
* **Data Owners**: Approve key usage for their systems.

**12. Policy Review**

Reviewed annually or after significant security incidents/regulatory changes.

**Approved By:** [CISO/Executive Leadership Name]  
**Revision History:** [List dates and changes]