Generate a Secure policy for key management. Ensure security best practices.

Key Management Policy

**1. Purpose**

To establish secure practices for generating, storing, distributing, rotating, and destroying cryptographic keys to protect sensitive data and systems against unauthorized access, breaches, or loss.

**2. Scope**

Applies to all employees, contractors, and systems handling cryptographic keys (e.g., encryption keys, API keys, SSH keys, TLS certificates) across the organization.

**Policy Requirements**

**3. Key Generation**

* **Algorithm & Strength**:
  + Use industry-standard algorithms (e.g., AES-256, RSA-2048+, ECC-384).
  + Generate keys via FIPS 140-2/3-validated or NIST-recommended cryptographic modules.
* **Randomness**: Keys must be generated using certified cryptographically secure random number generators (CSPRNGs).
* **Environment**: Keys must be generated in isolated, secure environments (e.g., HSMs, secure enclaves).

**4. Key Storage**

* **At Rest**:
  + Store keys in hardened, access-controlled vaults (e.g., AWS KMS, HashiCorp Vault, Azure Key Vault).
  + **Prohibit**: Plaintext storage in code, config files, databases, or unprotected disks.
* **In Memory**: Keys must be wiped from memory immediately after use.
* **Access Controls**:
  + Enforce least privilege (e.g., RBAC) and multi-person approval for key access.
  + Require MFA for accessing key management systems.

**5. Key Distribution**

* **Encryption in Transit**: Distribute keys via secure channels (e.g., TLS 1.2+, SSH).
* **Segregation**: Keys must never be transmitted with data they protect.
* **Authentication**: Verify recipient identities before distribution.

**6. Key Usage**

* **Separation of Duties**: Different keys for distinct purposes (e.g., encryption vs. authentication).
* **Audit Logs**: All key usage must be logged (e.g., access attempts, operations).
* **Temporal Validity**: Keys must expire after a defined period (see *Rotation*).

**7. Key Rotation**

* **Frequency**:
  + **Symmetric keys**: Every 90 days (e.g., database encryption keys).
  + **Asymmetric keys**: Annually (e.g., TLS certificates).
  + **High-risk keys**: Immediately upon compromise suspicion.
* **Process**:
  + Generate new keys before retiring old ones.
  + Maintain previous keys briefly for data decryption (with phased retirement).

**8. Key Backup & Recovery**

* **Encrypted Backups**: Store backups in geographically dispersed locations with equivalent security to primary storage.
* **Testing**: Validate recovery procedures biannually.
* **Limitations**: Backups must exclude plaintext keys and enforce dual controls for restoration.

**9. Key Revocation & Destruction**

* **Revocation**: Immediately revoke keys if:
  + Compromise is suspected.
  + An employee/contractor with access leaves the organization.
* **Destruction**:
  + Use secure deletion methods (e.g., NIST SP 800-88).
  + Log all destruction events with audit trails.
  + Render keys irrecoverable (e.g., overwrite storage, HSM crypto-shredding).

**10. Incident Response**

* **Compromise Protocol**:
  + Revoke compromised keys immediately.
  + Investigate root cause and impact.
  + Rotate affected keys and re-encrypt data.
  + Report to the Security Team within 1 hour of detection.

**Roles & Responsibilities**

* **Security Team**: Policy enforcement, audits, incident response.
* **System Owners**: Key lifecycle management, access controls, logging.
* **Employees**: Compliance with key handling procedures; report suspected breaches.

**Compliance & Auditing**

* **Audits**: Quarterly reviews of key usage logs, access controls, and policy compliance.
* **Pen Testing**: Annual penetration testing of key management systems.
* **Violations**: Non-compliance may result in disciplinary action, up to termination.

**Policy Review**

Reviewed annually or after significant security incidents/regulatory changes.

*Approved by: [Chief Information Security Officer]*  
*Effective Date: [Date]*  
*Revision: 1.0*

**Implementation Guidance**:

* Use dedicated tools (e.g., HSMs, KMS solutions) for automated key lifecycle management.
* Train staff on key handling annually.
* Align with standards like NIST SP 800-57, ISO 27001, and GDPR/CCPA requirements.