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

**Cryptographic Key Management Security Policy**

**1. Purpose and Scope**

This policy establishes security requirements and procedures for the management of cryptographic keys throughout their lifecycle to protect organizational data and systems. It applies to all personnel, systems, applications, and third-party services that generate, store, distribute, use, or destroy cryptographic keys.

**2. Key Classification and Inventory**

**2.1 Key Categories**

* **Master Keys**: Root keys used to encrypt other keys
* **Data Encryption Keys (DEKs)**: Keys used to encrypt data at rest
* **Key Encryption Keys (KEKs)**: Keys used to encrypt other keys
* **Session Keys**: Temporary keys for communication sessions
* **Authentication Keys**: Keys for digital signatures and identity verification
* **Transport Keys**: Keys for secure data transmission

**2.2 Key Inventory Requirements**

* Maintain a comprehensive inventory of all cryptographic keys
* Document key purpose, classification, owner, and expiration dates
* Track key usage and access patterns
* Regular audits of key inventory (minimum quarterly)

**3. Key Generation Standards**

**3.1 Cryptographic Requirements**

* Use FIPS 140-2 Level 3 or higher certified random number generators
* Minimum key lengths:
  + AES: 256 bits
  + RSA: 3072 bits (4096 bits recommended)
  + ECC: 384 bits (P-384 curve)
* Generate keys in secure, isolated environments
* Prohibit weak or predictable key generation methods

**3.2 Key Generation Process**

* Keys must be generated by authorized personnel only
* Use approved cryptographic libraries and algorithms
* Document key generation events in audit logs
* Verify key quality and randomness before deployment

**4. Key Storage and Protection**

**4.1 Hardware Security Modules (HSMs)**

* Store master keys and high-value keys in FIPS 140-2 Level 3+ HSMs
* Implement tamper-evident and tamper-resistant controls
* Use dedicated HSMs for production environments
* Maintain HSM firmware and security patches

**4.2 Key Encryption**

* Encrypt all keys at rest using AES-256 or stronger algorithms
* Implement key wrapping for additional protection
* Use separate encryption keys for different environments
* Never store keys in plaintext format

**4.3 Access Controls**

* Implement role-based access control (RBAC) for key access
* Require multi-person authorization for critical key operations
* Use principle of least privilege
* Implement strong authentication (multi-factor authentication required)

**5. Key Distribution and Exchange**

**5.1 Secure Distribution Channels**

* Use authenticated and encrypted channels for key distribution
* Implement out-of-band verification for key exchanges
* Use established protocols (TLS 1.3, IPSec) for transmission
* Verify recipient identity before key distribution

**5.2 Key Escrow and Recovery**

* Implement key escrow for business continuity purposes
* Store escrowed keys in geographically separate locations
* Require dual control for key recovery operations
* Document all key recovery activities

**6. Key Usage and Operational Security**

**6.1 Usage Restrictions**

* Use keys only for their intended cryptographic purpose
* Prohibit key reuse across different applications or environments
* Implement key usage limits and monitoring
* Separate keys for encryption and digital signatures

**6.2 Operational Controls**

* Monitor key usage patterns for anomalies
* Implement automated key rotation schedules
* Log all key-related operations
* Regular security assessments of key usage

**7. Key Rotation and Renewal**

**7.1 Rotation Schedules**

* **High-risk keys**: Every 90 days
* **Medium-risk keys**: Every 180 days
* **Low-risk keys**: Annually
* **Emergency rotation**: Within 24 hours when compromise suspected

**7.2 Rotation Process**

* Automated rotation where technically feasible
* Coordinate rotation across dependent systems
* Verify successful rotation before decommissioning old keys
* Maintain overlap period for gradual transition

**8. Key Compromise and Incident Response**

**8.1 Compromise Detection**

* Monitor for unauthorized key access attempts
* Implement real-time alerting for suspicious activities
* Regular vulnerability assessments of key management systems
* Threat intelligence integration for proactive protection

**8.2 Incident Response Procedures**

* Immediate isolation of compromised systems
* Emergency key rotation within 4 hours
* Forensic analysis of compromise extent
* Notification to relevant stakeholders and authorities
* Post-incident review and remediation

**9. Key Destruction and End-of-Life**

**9.1 Secure Destruction**

* Use cryptographically secure deletion methods
* Overwrite key storage locations multiple times
* Physical destruction of hardware containing keys when necessary
* Verify complete key destruction

**9.2 Destruction Documentation**

* Log all key destruction activities
* Maintain records for compliance and audit purposes
* Certificate of destruction for high-value keys
* Regular cleanup of expired and unused keys

**10. Personnel Security**

**10.1 Background Checks**

* Conduct thorough background investigations for key management personnel
* Regular re-verification of personnel security clearances
* Implement insider threat monitoring programs
* Separation of duties for critical key operations

**10.2 Training and Awareness**

* Mandatory security training for all key management personnel
* Regular updates on emerging threats and best practices
* Simulation exercises for incident response
* Competency assessments and certifications

**11. Compliance and Audit**

**11.1 Compliance Requirements**

* Align with relevant standards (NIST, ISO 27001, Common Criteria)
* Meet industry-specific regulations (PCI DSS, HIPAA, SOX)
* Regular compliance assessments and gap analyses
* Maintain evidence for regulatory audits

**11.2 Audit and Monitoring**

* Continuous monitoring of key management activities
* Regular internal and external audits
* Automated compliance reporting
* Remediation tracking for identified vulnerabilities

**12. Business Continuity and Disaster Recovery**

**12.1 Backup and Recovery**

* Maintain secure backups of critical keys
* Test key recovery procedures regularly
* Implement geographic distribution of key backups
* Document recovery time objectives (RTO) and recovery point objectives (RPO)

**12.2 Continuity Planning**

* Develop alternate key management procedures for emergency situations
* Cross-train personnel for key management functions
* Maintain redundant systems and communication channels
* Regular testing of business continuity plans

**13. Third-Party and Cloud Considerations**

**13.1 Vendor Management**

* Due diligence assessments of key management service providers
* Contractual security requirements and right-to-audit clauses
* Regular security reviews of third-party services
* Maintain control over key generation and management

**13.2 Cloud Security**

* Use cloud-native key management services with appropriate controls
* Implement customer-managed encryption keys (CMEK) where available
* Regular assessment of cloud provider security practices
* Data residency and sovereignty considerations

**14. Governance and Policy Management**

**14.1 Policy Maintenance**

* Annual review and update of key management policies
* Change management process for policy modifications
* Stakeholder approval for significant policy changes
* Version control and distribution of policy updates

**14.2 Roles and Responsibilities**

* **Chief Information Security Officer (CISO)**: Overall policy ownership
* **Key Management Officer**: Day-to-day operational oversight
* **Security Team**: Implementation and monitoring
* **System Administrators**: Technical implementation
* **Audit Team**: Compliance verification and reporting

**15. Enforcement and Sanctions**

Violations of this policy may result in:

* Disciplinary action up to and including termination
* Legal action for willful misconduct
* Financial penalties where applicable
* Reporting to relevant authorities for criminal violations

**Policy Version**: 1.0  
**Effective Date**: [Current Date]  
**Review Date**: [Annual Review Date]  
**Approved By**: [CISO Name and Signature]