Generate a policy for key management.

**Cryptographic Key Management Policy**

**1. Purpose and Scope**

This policy establishes the standards and procedures for the secure management of cryptographic keys throughout their entire lifecycle within the organization. It applies to all employees, contractors, and third parties who handle cryptographic keys used to protect organizational data and systems.

**2. Policy Statement**

The organization is committed to protecting sensitive information through the implementation of robust cryptographic key management practices. All cryptographic keys must be managed in accordance with industry best practices and regulatory requirements to ensure confidentiality, integrity, and availability of protected data.

**3. Key Management Lifecycle**

**3.1 Key Generation**

* All cryptographic keys must be generated using cryptographically secure random number generators (CSRNGs)
* Key generation must occur in secure, controlled environments
* Minimum key lengths must comply with current industry standards:
  + AES: 256-bit keys
  + RSA: 2048-bit minimum (4096-bit recommended)
  + ECC: 256-bit minimum
* Weak or predictable keys are strictly prohibited

**3.2 Key Distribution**

* Keys must be distributed through secure, authenticated channels
* Key splitting or key escrow mechanisms must be used for high-value keys
* Keys must never be transmitted in plaintext over unsecured networks
* Digital certificates and public key infrastructure (PKI) should be used where applicable
* Key distribution must be logged and auditable

**3.3 Key Storage**

* All keys must be stored in hardware security modules (HSMs) or equivalent secure storage systems
* Software-based key storage is only permitted for low-risk applications with appropriate safeguards
* Keys must be encrypted when stored (key-encrypting-keys)
* Access to key storage systems must be strictly controlled and monitored
* Physical security controls must protect key storage infrastructure

**3.4 Key Usage**

* Keys must only be used for their intended cryptographic purpose
* Key usage must be logged and monitored for anomalous activity
* Automated key usage monitoring and alerting systems must be implemented
* Keys must not be used beyond their designated validity period

**3.5 Key Recovery and Backup**

* Critical keys must have secure backup and recovery procedures
* Key recovery mechanisms must not compromise key security
* Recovery procedures must be tested regularly
* Backup keys must be stored in geographically separate, secure locations
* Key recovery activities must be logged and audited

**3.6 Key Rotation**

* Keys must be rotated according to established schedules:
  + High-risk applications: Every 12 months or less
  + Medium-risk applications: Every 24 months or less
  + Low-risk applications: Every 36 months or less
* Emergency key rotation procedures must be established for compromise situations
* Key rotation must not result in service disruption

**3.7 Key Revocation and Destruction**

* Compromised or expired keys must be immediately revoked
* Certificate revocation lists (CRLs) or online certificate status protocol (OCSP) must be maintained
* Keys must be securely destroyed using approved methods that prevent recovery
* Key destruction activities must be documented and audited

**4. Roles and Responsibilities**

**4.1 Chief Information Security Officer (CISO)**

* Overall accountability for key management policy implementation
* Approval of key management procedures and standards
* Oversight of key management audit activities

**4.2 Key Management Administrator**

* Day-to-day management of cryptographic keys
* Implementation of key lifecycle procedures
* Monitoring and reporting on key management activities
* Coordination of key rotation and renewal activities

**4.3 System Administrators**

* Implementation of key management controls in assigned systems
* Compliance with key usage and storage requirements
* Reporting of suspected key compromise incidents

**4.4 Application Owners**

* Identification of cryptographic requirements for applications
* Compliance with key management standards in application design
* Coordination with key management administrators for key provisioning

**5. Technical Requirements**

**5.1 Hardware Security Modules (HSMs)**

* FIPS 140-2 Level 3 or higher certification required
* Redundant HSM configuration for high-availability applications
* Regular HSM firmware updates and security patches

**5.2 Key Management Systems**

* Centralized key management platform for enterprise-wide key governance
* Role-based access controls with multi-person authorization for sensitive operations
* Comprehensive audit logging and monitoring capabilities
* Integration with existing security information and event management (SIEM) systems

**5.3 Cryptographic Standards**

* Use of approved cryptographic algorithms as defined by NIST or equivalent standards bodies
* Regular review and update of approved algorithm lists
* Migration plans for deprecated algorithms

**6. Access Controls**

**6.1 Authentication**

* Multi-factor authentication required for all key management system access
* Privileged access management (PAM) solutions for administrative access
* Regular access reviews and recertification

**6.2 Authorization**

* Principle of least privilege for key access
* Separation of duties for critical key management operations
* Approval workflows for key generation and distribution

**6.3 Monitoring**

* Real-time monitoring of key access and usage
* Automated alerting for suspicious activities
* Regular access log reviews and analysis

**7. Incident Response**

**7.1 Key Compromise**

* Immediate incident response procedures for suspected key compromise
* Emergency key rotation and revocation capabilities
* Communication protocols for stakeholder notification
* Post-incident analysis and remediation procedures

**7.2 Business Continuity**

* Disaster recovery procedures for key management systems
* Business continuity planning for key-dependent systems
* Regular testing of recovery procedures

**8. Compliance and Audit**

**8.1 Regular Audits**

* Annual comprehensive key management audits
* Quarterly key inventory and usage reviews
* Monthly access control reviews

**8.2 Compliance Monitoring**

* Continuous monitoring of key management policy compliance
* Regular vulnerability assessments of key management infrastructure
* Compliance reporting to management and regulatory bodies

**8.3 Documentation**

* Maintenance of comprehensive key management documentation
* Regular updates to procedures and standards
* Training materials and user guides

**9. Training and Awareness**

**9.1 Personnel Training**

* Initial key management training for all relevant personnel
* Annual refresher training programs
* Specialized training for key management administrators
* Security awareness programs highlighting key management importance

**9.2 Competency Requirements**

* Certification requirements for key management personnel
* Regular competency assessments
* Professional development opportunities

**10. Third-Party Management**

**10.1 Vendor Requirements**

* Due diligence requirements for key management service providers
* Contractual security requirements for third-party key handling
* Regular security assessments of third-party providers

**10.2 Cloud Services**

* Specific requirements for cloud-based key management services
* Data residency and sovereignty considerations
* Encryption key ownership and control requirements

**11. Policy Enforcement**

**11.1 Violations**

* Clear consequences for key management policy violations
* Investigation procedures for security incidents
* Disciplinary actions for non-compliance

**11.2 Exceptions**

* Formal exception request and approval process
* Risk assessment requirements for policy exceptions
* Regular review of approved exceptions

**12. Policy Review and Updates**

This policy will be reviewed annually or following significant security incidents, regulatory changes, or technological developments. Updates require approval from the CISO and relevant stakeholders.

**Effective Date:** [Insert Date]  
**Review Date:** [Insert Date]  
**Policy Owner:** Chief Information Security Officer  
**Version:** 1.0