Generate a policy for key management.

Here's a comprehensive **Key Management Policy** designed to establish secure practices for the generation, distribution, use, storage, rotation, and disposal of cryptographic keys. This can be adapted for use in enterprise, government, or regulated environments.

**Key Management Policy**

**1. Purpose**  
This policy establishes the requirements for secure management of cryptographic keys used to protect data integrity, confidentiality, and authenticity across all systems, applications, and networks.

**2. Scope**  
This policy applies to all employees, contractors, vendors, and systems that use or manage cryptographic keys within the organization.

**3. Policy Statement**

**3.1 Key Generation**

* Keys must be generated using industry-standard algorithms (e.g., RSA, ECC, AES) and meet minimum strength requirements:
  + AES: 256 bits
  + RSA: 2048 bits (minimum), 3072 bits preferred
  + ECC: secp256r1 (P-256) or higher
* Keys must be generated in a secure environment, preferably using a FIPS 140-2 Level 3 or higher Hardware Security Module (HSM).

**3.2 Key Distribution**

* Keys must be distributed securely using secure channels (e.g., TLS, SFTP, SSH).
* Keys must never be transmitted in plaintext.
* Public keys can be freely distributed but must be signed by a trusted Certificate Authority (CA) when applicable.

**3.3 Key Storage**

* Private and symmetric keys must be stored in encrypted form using strong encryption mechanisms.
* Keys must be stored in secure containers such as HSMs, Key Management Systems (KMS), or encrypted databases.
* Access to stored keys must be restricted based on the principle of least privilege.

**3.4 Key Usage**

* Keys must only be used for their intended purposes (e.g., encryption, signing).
* Systems must enforce key separation policies (e.g., one key per purpose).
* Logging and auditing must be enabled for all key usage.

**3.5 Key Rotation**

* Keys must be rotated periodically based on risk and regulatory requirements:
  + Symmetric keys: at least annually or upon compromise
  + Asymmetric keys: every 2–3 years or as required by policy
* Rotation procedures must ensure continuity of service without exposing keys.

**3.6 Key Revocation and Expiry**

* Expired or revoked keys must be removed from active use.
* Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP) must be used for real-time status validation.

**3.7 Key Disposal**

* Keys that are no longer needed must be securely destroyed using approved methods (e.g., zeroization, crypto-erase).
* Destruction must be logged and verified by a designated security officer.

**4. Roles and Responsibilities**

* **CISO/Security Team**: Define policies, conduct audits, ensure compliance.
* **IT Operations**: Implement and maintain secure key management infrastructure.
* **Developers/Engineers**: Use keys appropriately and report anomalies.
* **Auditors**: Periodically review key management processes.

**5. Compliance and Audit**

* Regular audits must be performed to ensure adherence to this policy.
* Non-compliance must be reported to the Information Security team and may result in disciplinary action.

**6. Exceptions**

* Exceptions to this policy must be documented and approved by the CISO or an authorized delegate.

**7. Review and Updates**

* This policy must be reviewed at least annually and updated as necessary to reflect changes in regulatory, business, or technology requirements.