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

Here's a sample **Key Management Policy** that follows security best practices. This can be adapted for organizational use across industries such as finance, healthcare, or technology:

**Key Management Policy**

**1. Purpose**  
The purpose of this policy is to establish guidelines for the secure generation, distribution, storage, use, rotation, and destruction of cryptographic keys used to protect sensitive information within the organization.

**2. Scope**  
This policy applies to all employees, contractors, vendors, and systems that manage or utilize cryptographic keys for any purpose, including encryption, decryption, digital signatures, and authentication.

**3. Roles and Responsibilities**

* **Key Custodian**: Responsible for the secure handling of cryptographic keys.
* **Information Security Officer (ISO)**: Oversees key management operations and audits compliance.
* **System Administrators**: Ensure systems comply with key management policies.

**4. Key Generation**

* Keys must be generated using approved cryptographic algorithms and secure key generation methods (e.g., FIPS 140-3 compliant modules).
* Random number generators used for key generation must meet NIST standards.

**5. Key Distribution**

* Keys must be distributed over secure channels (e.g., TLS, SSH, encrypted email).
* Public keys may be distributed openly; private/symmetric keys must be transferred securely to authorized entities only.

**6. Key Storage**

* Private and symmetric keys must be stored in encrypted form using hardware security modules (HSMs), trusted platform modules (TPMs), or other secure environments.
* Access to stored keys must be restricted to authorized personnel based on the principle of least privilege.

**7. Key Usage**

* Keys must be used solely for their intended purposes.
* Use of deprecated or weak algorithms (e.g., MD5, SHA-1, 1024-bit RSA) is strictly prohibited.

**8. Key Rotation and Expiration**

* Keys must have a defined lifespan and be rotated regularly (e.g., annually or upon compromise).
* Automated systems should enforce key expiration and renewal alerts.

**9. Key Revocation and Destruction**

* Keys must be revoked immediately upon suspicion or confirmation of compromise.
* Keys must be destroyed securely (e.g., cryptographic erasure) when no longer needed.

**10. Audit and Logging**

* All key lifecycle operations (creation, use, rotation, deletion) must be logged.
* Logs must be protected from unauthorized access and retained in accordance with data retention policies.

**11. Compliance and Review**

* Regular audits must be conducted to ensure compliance with this policy.
* The policy must be reviewed and updated at least annually or upon changes in legal, regulatory, or operational requirements.