COMPANY policy template instructions

This COMPANY policy template represents a complete, compliance-ready policy with placeholders for company specific text. Each policy section represents a policy-specific topic that you should consider and/or modify to match your company’s practices.

For each policy section

* Consider if this section and its corresponding risks applies to you. If it does not, remove it and/or replace it with your organization’s corresponding practices.
* Replace any highlighted text in angled brackets < > with your own language
* Rewrite the policy language such that it reflects the practices of your organization

Policy completion checklist

1. Use Find to make sure that all text in angled brackets is replaced
2. Proofread your policy for spelling and grammar mistakes
3. Confirm that the policy’s content reflects your organizations practices
4. Add any company-specific letterhead, branding, and formatting
5. Remove this instructions page
6. Export this document as PDF — File > Save As > Change “File Format” to PDF
7. Upload the PDF to COMPANY at https://app.COMPANY.com/policies

More questions?

A good rule-of-thumb is to keep your language high enough level such that it stays representative for at least a year. If you have more questions about how to use this template, please reach out to support@COMPANY.com or your auditor for additional guidance.

# Cryptography Policy

Policy Owner: <Policy owner>

Effective Date: <Effective date>

# Purpose

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information. This policy establishes requirements for the use and protection of cryptographic keys and cryptographic methods throughout the entire encryption lifecycle.

# Scope

All information systems developed and/or controlled by <Company Name> which store or transmit confidential data.

# Policy

<Company Name> shall evaluate the risks inherent in processing and storing data, and shall implement cryptographic controls to mitigate those risks where deemed appropriate. Where encryption is in use, strong cryptography with associated key management processes and procedures shall be implemented and documented. All encryption shall be performed in accordance with industry standards, including NIST SP 800-57.

Customer or confidential company data must utilize strong ciphers and configurations in accordance with vendor recommendations and industry best practices including NIST when stored or transferred over a public network.

# Key Management

Access to keys and secrets shall be tightly controlled in accordance with the Access Control Policy.

The following table includes the recommended usage for cryptographic keys:

| **Domain** | **Key Type** | **Algorithm** | **Key Length** | **Max Expiration** |
| --- | --- | --- | --- | --- |
| Web Certificate | RSA or ECC with SHA2+ signature | RSA or ECC with SHA2+ signature | 2048 bit or greater/RSA, 256bit or greater/ECC | Up to 1 year |
| Web Cipher (TLS) | Asymmetric Encryption | Ciphers of B or greater grade on SSL Labs Rating | Varies | N/A |
| Confidential Data at Rest | Symmetric Encryption | AES | 256 bit | 1 Year |
| Passwords | One-way Hash | Bcrypt, PBKDF2, or scrypt, Argon2 | 256 bit+10K Stretch. Include unique cryptographic salt+pepper | N/A |
| Endpoint Storage (SSD/HDD) | Symmetric Encryption | AES | 128 or 256 bit | N/A |

# Exceptions

Requests for an exception to this policy must be submitted to the <approver of requests for an exception to this policy, e.g., IT Manager> for approval.

A documented exception is required prior to moving, copying, or storing customer or company confidential data on any media or removable device; all portable devices and removable media containing sensitive data must be encrypted using approved standards and mechanisms.

# Violations & Enforcement

Any known violations of this policy should be reported to the <recipient of reports of violations of this policy, e.g., IT Manager>. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

| **Version** | **Date** | **Description** | **Author** | **Approved by** |
| --- | --- | --- | --- | --- |
| <1.0> | <29-Apr-2020> | <First Version> | <OWNER> | <APPROVER> |
|  |  |  |  |  |