Version 1.0

Date: 10/5/2019

# Encryption Policy Template

## 1. 0 Purpose

To provide our members a template that can be modified for your company's use in developing an Enterprise Encryption Policy. This policy template and the procedures it encompasses are to ensure the confidentiality and integrity of your company's information through the implementation of cryptographic controls.

## 2.0 Scope

Define the scope covered in the policy. Our recommendations for this section are delineated below.

This policy covers all of our company's information, systems, networks, and other information assets to ensure adequate controls are in place to ensure the confidentiality, integrity and availability of our data. These critical assets must be managed and controlled to protect our company from loss due to misuse, disclosure, fraud, or destruction.

This policy applies to all company employees, temporary employees, contractors, consultants, vendors, service providers, partners, affiliates, third parties or any other person or entity authorized to utilize our information resources. This includes all information systems, hardware, software, data, media, and paper files at our company and any approved third-party facilities. This policy also pertains to all systems, networks, and users connected to our company resources through any means, including but not limited to: local access, leased lines, wireless access points, or any other telecommunications device, through either private or public networks. It also applies to all third-party local and remote connections as well as non-company assets involved in the storage, processing, or transmission of company's information or data.

## 3.0 Policy

A. Cryptographic Controls - this section covers the use of cryptography to encrypt sensitive data. The recommended text includes:

Cryptographic controls must be utilized for sensitive information classified by our company as {PROTECTED} or {RESTRICTED} including, but not limited to: Personally Identifiable Information (PII), Protected Health Information (PHI), credit card numbers, passwords, intellectual property (define), budget or contract proposals, legal correspondence and research and development information. (Define your list of critical data). All encryption mechanisms utilized by our company must be authorized by the appropriate authority.

Users must not attempt to utilize any form of cryptography, including, but not limited to, encryption, digital signatures, and digital certificates, which has not been approved and installed/implemented by

© 2019 National Cybersecurity Society. All Rights Reserved.

our designated representative (maybe an outside consultant, define who this is). The use of all encryption mechanisms must meet relevant regulatory and legal requirements, including any import/export requirements and use of cryptography in other countries. Define the recommended encryption methods - such as AES-128, RSA, Bitlocker, or ECC.

B. Key Management (if applicable) - Define the scope of your key management system. Suggested text includes:

All encryption keys must be managed using a commercially available key management system. The key management system must ensure that all encryption keys are secured and there is limited access to company personnel. Master keys and privileged access to the key management system must be granted to at least two administrators. Keys generated by the key management system must not be easily discernible and easy to guess. When keys are transmitted to third party users, the encryption key must be transmitted over a different communication channel than the data that has been encrypted. All key recovery operations must be authorized and all activities must be logged by the key management system. All logged activities must be periodically reviewed (state how often and by whom) of the company.

C. Network Encryption - Define how transmission of sensitive data is handled. Suggested text follows.

All sensitive information classified by our company as PROTECTED or RESTRICTED including, but not limited to, PII, PHI, credit card numbers, passwords, and research and development information, must be encrypted when transmitted outside of our company. This includes transmission of information via email or other communication channels. Remote management activities for our company, such as contractors accessing our network remotely, must consistently employ session encryption. Define remote access procedures such as using VPN to access corporate systems while teleworking.

D. Hard Disk Encryption - Define how sensitive data is encrypted at rest. Suggested text follows.

All sensitive information classified by our company as PROTECTED or RESTRICTED including, but not limited to PII, PHI, credit card numbers, and passwords, must be encrypted. When feasible, hardware encryption must be utilized over software encryption. It is our company's policy to use laptops and desktops that have encrypted hard drives - or use Apple's FileVault - a built-in disk encryption feature.

## 4.0 Roles and Responsibilities

A. Responsible Parties. Define roles and responsibilities in this section, sample text below.

Our company's leadership and management team are responsible for maintaining and enforcing the policies, standards and guidelines established within this document. Employees, contractors, vendors, service providers, partners, affiliates, and third parties are responsible for ensuring all actions are in accordance with our management policies and objectives.

© 2019 National Cybersecurity Society. All Rights Reserved.

All users are required to sign our company's Acceptable Use Policy and acknowledge they understand and will abide by the standards and individual responsibilities it defines. All changes to the Acceptable Use Policy are communicated to all staff, contractors and other third parties in a timely fashion.

B. Ownership

All IT policies, standards, and guidelines are owned, established and managed by the CIO (or equivalent authority) within our company.

C. Communication

All policies, standards and guidelines are available for reference to all company users. The availability of this program will also be communicated to all users annually.

D. Policy Review and Maintenance

This document will be updated upon any material change to the company and its employees in timely fashion.

## 5.0 Compliance

All users must comply with our company's corporate policies. Any user found to be abusing the privilege of using our corporate assets and access to business systems, or not in compliance with any of these policies, may be subject to disciplinary action, up to and including termination of employment.

## 6.0 Applicability

A. This policy is applicable to all company employees working both on site and remotely.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
**web@thencss.org** or visit us at the link below.

© 2019 National Cybersecurity Society. All Rights Reserved.