**Cryptographic Control**

**Doc A10**

**Version: 1.0**

Publication Date: January 2019

Current Status: Published

Author(s): Michael Woolard

Reviewed By: Michael Woolard

**Table of Contents**

1 Cryptographic Controls 3

1.1 Scope 3

1.2 Responsibilities 3

2 Level of Cryptography 3

2.1 Best Practices 3

3 Procedure 3

3.1 Laptop Computers 3

3.2 E-mail 3

3.3 USB Flash Drives 3

3.4 Remote Access 4

3.5 Inter-office Network 4

3.6 FTP 4

3.7 Smart Phones 4

3.8 Websites 4

3.9 Databases 4

3.10 Cryptographic Key management 4

3.11 Regulations for cryptography 5

4 Document Control and Approval 6

4.1 Distribution 6

4.2 Version Information 6

# Cryptographic Controls

## Scope

This procedure relates to how Wacky Widget applies cryptographic controls to items / assets within its scope.

## Responsibilities

The Risk and Compliance Team is responsible for defining the cryptography in place. The Technology teams are responsible for technical deployment of the measures. All employees, contractors and third parties have responsibilities to comply with these procedures.

# Level of Cryptography

## Best Practices

* Password Hashing: PBKDF2, Scrypt, Bcrypt
* Key exchange: Diffie–Hellman key exchange with minimum 2048 bits
* Message Integrity: HMAC-SHA2, MD5
* Message Hash: SHA2 256 bits
* Asymmetric encryption: RSA 2048 bits
* Symmetric-key algorithm: AES 256 bits

Reference REC A10

# Procedure

## Laptop Computers

All laptop computer hard-drives must be encrypted using a full disk encryption tool.

## E-mail

E-mail encryption is required when using e-mail to exchange company secret, confidential, or personally identifiable data, where no alternative secure transmission methods are available.

## USB Flash Drives

USB flash drives must be encrypted if they are taken from the office and contain any company data other than that classified as Public or Sensitive. USB flash drives can remain unencrypted if they are retained within a single Company office location.

## Remote Access

Remote data and network access is only permitted using encrypted VPN over the Internet.

## Inter-office Network

The Company offices must be connected via secure point to point connections.

## FTP

The Company allows the use of both unencrypted FTP (FTP) and encrypted FTP (sFTP). It is the responsibility of the person initiating the transfer to ensure that they are using a method that will protect the data being sent in line with the Information Classification Policy.

## Smart Phones

Company data must only be stored on devices where appropriate business and technical approval has been given and the data is encrypted using a company approved method.

## Websites

Website applications, in any environment, accessible over the internet or other insecure networks are secured by TLS. Any exceptions to this policy must be authorized by the Risk and Compliance Manager.

## Databases

Databases (or specific fields within databases) are encrypted based on the contained information classification requirements. Any exceptions to this policy must be authorized by the CTO.

## Cryptographic Key management

Cryptographic keys are kept securely by the relevant technical team.

Passwords for certificate keys are secured with access restrictions in place.

When an employee who has access to Cryptographic keys protecting restricted data leaves the organization, private keys and associated certificates must be replaced.

The same Cryptographic key should not be installed on multiple hosts, except for clustered and load-balanced services. Where certificates are shared or span across multiple hosts, the security requirements of the most sensitive member prevail.

The same Cryptographic key and certificate should only be used with one set of restricted data (e.g., website, ssh, etc.), to reduce the risk of compromise across multiple data sets.

**Certificate Renewal**

Keys must be regenerated, and certificates re-signed, when renewing a certificate.

Certificates must be renewed after no more than three years.

**Revoking Certificates**

Certificates must be revoked when one or more of the following occur:

* A Cryptographic key has been compromised.
* The service is being retired or decommissioned.
* When the Cryptographic key is no longer in use.
* When the password to the key has been exposed to unauthorized persons

**Self-Signed Certificates**

Systems only reachable via trusted networks may use self-signed certificates

Self-signed certificates outside of trusted networks are allowed as an exception only where authorized by the CTO.

**Backup and storage of cryptographic keys**

All cryptographic keys are backed up and retained in a secure location of-site

## Regulations for cryptography

All cryptographic tools used are compliant with all relevant laws and regulations related to cryptography.

# Document Control and Approval

The Chief Information Security Officer is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff and is the published version.

Signature: Executive Manager Signature Date: 01.01.2019

## Distribution

|  |  |
| --- | --- |
| **Name** | **Role** |
| *Intranet* | *Distribution to all staff* |

## Version Information

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author(s)** | **Details** |
| 0.1 | 11/28/18 | M.Woolard | First draft |
| 0.2 | 12/07/18 | M.Woolard | Second draft |
| 1.0 | 01/01/19 | M.Woolard | First published |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 