Microlink Cryptographic Control Policy

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | Date | Amended By | Summary of Change | File Location | Approved by/ Date |
| V1 | 22/06/2020 | David Henderson | Initial draft | SharePoint IT Site |  |
| V2 | 15/12/2021 | David Henderson | Included version control within document and reviewed. | SharePoint IT Site |  |
| V2.1 | 30/09/2022 | D Henderson | Added inline document owner | SharePoint | Michael Moore Legal Counsel  |
| V2.2 | 09/01/2023 | D Henderson | Incorporated requirements from ISMS IT Ops manual  | SharePoint | Michael Moore Legal Counsel |
| V3 | 19/11/2024 | D Henderson | Inclusion of key compromise policy | SharePoint | Exec |
| V3.1 | 21/11/2024 | D Henderson | Inclusion of mandatory key disclosure | SharePoint | Exec |
| V3.2 | 26/11/2024 | D Henderson | Inclusion of point 8.8 Cryptographic key rotations | SharePoint | Exec |

**Document Owner IT**

# Introduction

This policy defines the controls that are required and related procedures for various areas where encryption and cryptographic technologies are used.

# Scope

Controls that implement cryptographic technologies can be used to accomplish various security objectives:

Confidentiality: Encrypting data to protect sensitive or critical information. Encryption can be used with stored data, at rest or data that is being transmitted, in motion.

Integrity: Using digital signatures certificates to ensure authenticity of stored or transmitted sensitive or critical information.

Non-repudiation: using cryptographic techniques to provide evidence of an action or event.

Authentication: Using cryptographic techniques to authenticate users or systems that require transacting with resources.

# Overview

The purpose of this policy is to identify where cryptographic controls are used and how they should be managed.

Identifying areas where and how cryptographic technology should be used is vital to running a secure and safe environment for client, and Microlink data. It is also recommended as best practice in ISO 27002. However correct management of cryptographic keys such as password, encryption/decryption keys authentications tokens (smartcards) etc is critical.

Miss managing encryption and cryptographic technology can introduce a false sense of security which in turn can increase risk to the business.

This policy aims to clarify how encryption and cryptographic controls should be correctly managed.

# Definitions

For the purposes of this document the following definitions are made

**Cryptography:** a method of storing and transmitting data in a form that only those it is intended for can read and process.

**Encryption**: the process of converting data from plain text to a form that is not readable to unauthorized parties, known as cipher-text.

**Key:** the input that controls the process of encryption and decryption. There are both secret and public keys used in cryptography.

**Digital Certificate**: An electronic document that is used to verify the identity of the certificate holder when conducting electronic transactions. SSL certificates are a common example that have identifying data about a server on the Internet as well as the owning authority’s public encryption key.

**Digital Signature Certificate**: a type of digital certificate that proves that the sender of a message or owner of a document is authentic, and the integrity of the message or document is intact. A digital signature certificate uses asymmetric cryptography and is not a scanned version of someone’s handwritten signature or a computer-generated handwritten signature (a.k.a. an electronic signature).

**Asymmetric Keys**: A type of cryptographic key that uses key pairs, usually a public and private key pair where the Public half and Private half differ and are used for authenticating and/or establishing a secure connection. Examples can be TLS certificate, SSH keys, document or data signing.

# Use of Cryptographic controls

* 1. Approved encryption methods for data at rest
		1. Endpoints that handle or process sensitive or critical data must use AD managed BitLocker with a minimum of AES-256 with TDM modules.
		2. Mobile and laptop devices permitted for remote use should be further secured with a pre-boot security PIN/passphrase
		3. Self-Encrypting drives implementing minimum of AES-256 for server deployments that store or process Sensitive or Critical data.
		4. Where permitted, removable media should be encrypted with BitLocker To Go with a minimum of AES-256.
	2. Approved encryption methods for data in motion
		1. Sensitive and critical information is required to be transferred via a secure method or channel. A Secure channel is an encrypted network connection.
		2. Encryption is built into various application such as web-browser Remote desktop sessions etc. The user should be aware any connection they use to transmit sensitive or critical data and should ensure that encryption is enabled for those applications.
		3. Ciphers and algorithms implemented must not be considered “Weak”
		4. Where possible cryptographic keys are issues and stored within the local Certificate authority system.
* Such as;
* Smartcard
* Internal only systems

# Encryption is required when.

* 1. Accessing sensitive or critical information via web application. (ensure the HTTPS lock is visible)
	2. When remotely accessing any virtual desktop environments eg citrix, RDP etc.
	3. Inter system communication such as API calls SQL queries are made. (ensure SSL is used)
	4. When any privileged access to network or server equipment is required. Ie SSH, web interfaces etc
	5. Microlink webservers that are accessed via public networks and support SSL must have a valid certificate installed.

# Encryption when using Email.

* 1. Sending sensitive or critical data without any addition form cryptographic control is prohibited. Even where TLS is enforced.
	2. Exact handling procedures differ per client, please review your local handling procedures for specific requirements.

# Management of cryptographic keys and certificates.

* 1. All cryptographic keys used to encrypt endpoints using BitLocker must have their Recovery key stored in Active directory.
	2. All certificates’ issues by a 3rd party certificate authority must be:
		1. If required to be temporarily or permanently Stored this should be in the IT secure KeePass (if generated off device)
		2. Be protected by a passphrase or AD credentials/groups.
		3. Never left un-protected/ unlocked.
		4. Revocation procedures per CA should be documented.
		5. All cryptographic keys must be recorded to ensure any legal obligations can be fulfilled.
		6. Keys used for Infrastructure such as disc encryption, securing SSH, etc should be recorded in the IT Secure KeePass
		7. Keys used for encrypting end user data, such as passworded ZIP files should be recorded in the end users record.
		8. Private Keys should not, at any time, be stored with the encrypted media.
	3. Unique cryptographic keys should be used per client where possible.
	4. Access to cryptographic key should be limited on a “need to know” basis and restricted to as few personnel as possible.
	5. Cryptographic keys should be destroyed at the end of their service life or when the data they protect is no longer needed.
	6. Cryptographic Keys must be rotated regularly, at least annually, where used to encrypt customer data.

# Disposal of cryptographic keys

Cryptographic keys should be destroyed at the end of their service life or when the data they protect is no longer needed.

* 1. This includes wiping TPM modules.
	2. Deleting communal keys in self encrypting drive systems (DAS and SAN)
	3. Transparent data encryptions keys for databases.
	4. Certificates on smart cards.
	5. Monitoring of cryptographic keys
	6. SSL certificates should be monitored via the SSL monitoring dashboard.

# Secure Key Generation

* 1. **Symmetric keys**
		1. Use Randomization techniques to create an unpredictable and strong key
		2. Use long key – Keys should be a minimum of 15 characters.
		3. Keys should be suitably random and unique
		4. Where available use hardware cryptographic module over software modules.
		5. Be generated on a secured microlink controlled device.
	2. **Asymmetric keys**
		1. Private Keys should be generated on device where possible (example: generating a Certificate signing request)
		2. If not possible from onboard the device, it should, at minimum, be generated on a secured microlink controlled device.

# Secure Key Exchange

* 1. **Symmetric Keys**
		1. Keys should be exchanged using a secure channel
		2. Keys should use a separate channel from data transfer where the key is used to encrypt the data.
	2. **Asymmetric Keys**
		1. If a key is not generated on the device using it – it should be securely transported on the device.

# Key compromise plan

# Asymmetric Key

* + 1. **Assessment**
		2. **Immediate Assessment:** Once a compromise is suspected, the extent of the breach should be identified. Determine which keys are affected and the potential impact.
		3. **Containment**
			1. **Revoke compromised** **keys** Revoke the compromised keys from all systems and services to prevent their use.
			2. **Revoke compromised keys:** Where keys were issued by a Certificate authority contact the authority to have them revoked.
			3. **Where used on 3rd party system** (ie FTP or SSH access) inform 3rd party to revoke/stop use of that key until further notice
		4. **Notification**
			1. **Internal Notification**: Inform relevant internal stakeholders by logging the incident in the incident management system.
			2. **External notification:** Identify External stakeholders that this may impact such as partners customers if their data or service are impacted. Pass this information onto incident team via the incident ticket raised.
		5. **System process and review:**
			1. **Audit and review:**  Conduct a thorough audit of the affected systems and processes to identify vulnerabilities that led to the compromise. Update the incident ticket with findings
			2. **Update security measures:**  identify and implement additional security measures to prevent future compromises, examples: enhanced monitoring, stricter access controls, improved patch management and more regular key rotation.
		6. **Key Replacement:**
			1. **Generate new Keys** Generate new asymmetric key pairs/Certificates etc to replace the compromised ones.
			2. **Distribute new Keys:** Securely distribute the new keys to all relevant parties and systems if not generated on system.
		7. **Post incident analysis**
			1. **Root cause analysis**: a root cause analysis should conduct to understand how the compromise occurred. Any further controls can be identified and applied to other systems that are potential effected, employee training can be identified if a procedure failure cause the compromise.

# Symmetric Key

* 1. **Assessment**
		1. **Immediate Assessment:** Once a compromise is suspected, the extent of the breach should be identified. Determine which keys are affected and the potential impact.
	2. **Containment**
		1. **Revoke compromised** **keys** Revoke the compromised keys from all systems and services to prevent their use.
		2. **Request 3rd party to cease operation of the compromised key until further notice.**
	3. **Notification**
		1. **Internal Notification**: Inform relevant internal stakeholders by logging the incident in the incident management system.
		2. **External notification:** Identify External stakeholders that this may impact such as partners customers if their data or service are impacted. Pass this information onto incident team via the incident ticket raised.
	4. **System process and review:**
		1. **Audit and review:**  Conduct a thorough audit of the affected systems and processes to identify vulnerabilities that led to the compromise. Update the incident ticket with findings
		2. **Update security measures:**  identify and implement additional security measures to prevent future compromises, examples: enhanced monitoring, stricter access controls, improved patch management and more regular key rotation.
	5. **Key Replacement**
		1. **Generate New Keys**: Create new symmetric keys to replace the compromised ones. Do this following Key generation policy
		2. **Distribute New Keys**: Securely distribute the new keys to all necessary parties and systems.
		3. **Data Encryption**: Symmetric keys are typically used for data at rest encryption, where this is the case, data encrypted with compromised keys should be decrypted and re-encrypted with new keys, on a microlink controlled secure environment/device.
	6. **Post incident analysis**
		1. **Root cause analysis**: a root cause analysis should conduct to understand how the compromise occurred. Any further controls can be identified and applied to other systems that are potential effected, employee training can be identified if a procedure failure cause the compromise.

# Mandatory Key Disclosure

* 1. **Employee responsibilities**
		1. **Any employee that generates a cryptographic key for data at rest**, must,
		2. disclose the details of that private key to the IT department, or
		3. store them in the company’s approved key vault,
		4. Store them on the customers record,
		in order to allow Microlink PC to comply with any local laws.
	2. **Compliance with local laws**
		1. **Under the Regulation of investigatory Powers Act** (RIPA) section 49 we may be required to provide decryption or private keys. This will only carried out with;
			1. **Approval** from a member of the Executive **and**
			2. **On production of a warrant** or other court order issued by the relevant judicial authority.
		2. Any requests for key disclosure should be **logged in the incident management system**
		3. **The key should be considered compromised**, and the key should be replaced. (providing that doing so does not conflict with the company’s obligations section 49 of RIPA or the terms of any warrant or order served upon the company.