**Encryption Policy**

Prepared By

**IT Security**

**VERSION: 1.0**

All rights reserved. This document is a proprietary product of Menara Organization and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission from Menara Organization, is strictly prohibited. Any printed copy of this document is uncontrolled

**CHANGE HISTORY**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Date** | **Summary of changes** | **Author/Editor** | **Pages affected** | **Remark** |
| 1.0 |  |  |  |  |  |
|  |  |  |  |  |  |

**Table of Contents**

**PURPOSE 4**

**SCOPE 4**

***POLICY* 4**

**ENFORCEMENT 9**

1. **PURPOSE**

The purpose of this document is to assure interoperability and consistency across the Organization Group. It provides the standards to which encryption systems must comply, specifying algorithms and parameters to be used. To assure interoperability and reduce life cycle costs, standard products should be selected for Organization Group use. Additionally, this document provides direction to ensure that the regulations are followed.

1. **SCOPE**

Primary audiences for this document are individuals’ assigned ownership of data, and asset owners and asset custodians assigned operational and maintenance responsibility for an encryption system.

1. ***POLICY***
	1. **Data Classification**
		1. **Category I (C-1) – General/Unrestricted:** This information is targeted for general public use. Examples include Internet website contents for general viewing and press releases.
		2. **Category II (C-2) – General/Restricted:** Information not generally available to parties outside Organization Group, such as directory listings, minutes from non-confidential meetings, and internal (Intranet) websites. Public disclosure of this information would cause minimal trouble or embarrassment to the Group. This category should be the default data classification category.
		3. **Category III (C-3) – Classified/Unrestricted:** This information is considered private and should be guarded from disclosure. However, public disclosure of this information due to a system compromise generally does not result in financial fraud or violation of law. Examples might include intellectual property information, private directory listings, and contract negotiations.
		4. **Category IV (C-4) – Classified/Restricted:** Any disclosure of this information, intentional or otherwise, may directly contribute to financial fraud and/or violate the law. Examples include customer credit card numbers, customer details, and might include financial institution account numbers.
		5. Refer to Classification of Organization Internal Information/Data SPI for further details.
	2. **Use of Encryption**

The use of encryption is to apply the technology to protect high value information assets by minimizing various risks, to comply with legal or regulatory requirements, and to protect Organization Group’s reputation.

The requirements specified below are the minimum requirements. Asset owners should be aware of the benefits of the use of encryption and weigh those benefits against costs to determine other appropriate applications of the technology.

* + 1. **Encrypted Data Storage**
			1. Data storage shall be encrypted when under the following conditions:
				1. Data stored outside the security perimeter of the Organization group network classified with a confidentiality level of Confidential (C-3) or higher.
				2. Data classified with a confidentiality level of Secret (C-4).
			2. ***Organization IT*** Risk ***Management Framework*** shall ***apply to*** consider encrypted storage of data classified with a confidentiality level of Confidential (C-3) or higher stored within the Group network.
			3. All other data stored in the Group computer may be encrypted at the discretion of the asset’s owner.
		2. **Encryption of Electronic Mail Messages and Attachments**
			1. Transmission of electronic mail for delivery within Organization Group that includes information classified with a confidentiality level of Confidential (C-3) or higher either in the body of the message or in an attachment shall be protected by encryption. A comprehensive solution enabling delivery of secure e-mail to addresses outside Organization Group is desired but not mandatory.
		3. **Encryption of Data and Information in Transit**
			1. All data transmissions that leave the control or management of Organization Group, except information classified with a confidentiality level of Public only (C-1) data transmissions and electronic mail addressed for an external recipient, shall be encrypted.
			2. Application system transmits information classified as Confidential (C-3) shall not be on clear text.
			3. Application system transmits information classified as Secret (C-4) shall be encrypted from point of entry to point of delivery.
			4. Application risk assessments shall address failure to provide such measures and provide alternatives to mitigate the associated risk.
		4. **Encryption of Information Used for Authentication**
			1. Information used for authentication of user identity provides a unique set of protection requirements. It shall comply with the following:
				1. Authentication information shall be transmitted in an unintelligible form or sender-to-recipient encrypted for transmission.
				2. The information shall be stored in a form that the contents of the information cannot be easily determined. E.g. one-way encrypted or as hash fragments.
				3. Encrypted authentication information should use one-way cryptography wherever it is feasible.
		5. **Use of Secure Hash**
			1. Asset owners may elect to use secure hash as an integrity mechanism for files, messages, or transmission.
			2. Industry standards or proven secure hash algorithm shall be used to verify the data integrity.
	1. **Encryption Key Management**
		+ 1. All keys (symmetric and asymmetric key) must be kept secret throughout their lifecycles; otherwise the protection properties of the encryption technology are invalidated.
			2. Encryption algorithms and keys must be sufficiently strong that they withstand crypt-analysis, including guessing and brute force attacks within a satisfactory period of attack.
			3. The method of distributing and storing secret keys must be sufficiently strong that the key cannot be compromised during distribution or storage.
			4. Key management procedure must be endorsed by Organization IT Security and reviewed by Audit.
		1. **Classification of Keys**
			1. Encryption keys shall be classified minimally with a confidentiality level of Restricted (C-2) or at the same level as the highest level of data to be encrypted using the key.
			2. Key shall retain their classification, i.e., they cannot be downgraded, throughout their lifecycle.
			3. The asset owner of the encryption system shall assign the integrity and availability classification of symmetric or asymmetric encryption keys.
			4. The asset owner shall independently consider the integrity and availability requirements for both secret and public asymmetric keys.
		2. **Key Initialization Including Seed Keys**
			1. Key initialization is a critical process that must be endorsed by Organization IT Security and reviewed by Audit.
			2. Procedures for the initialization of an encryption device with a human-readable key shall require that the key be divided into at least two segments, which each key segment known to a single individual who shall enter that key segment to initialize the device.
		3. **Use of Automated Key Management Systems**
			1. Key management systems that automatically and securely generate and distribute new keys shall be used for all encryption technologies employed within Organization Group.
			2. If an automated key management system is not in use, standard operating procedures shall define one or more acceptable secure methods for distribution or exchange of keys. The standard operating procedures must be endorsed by Organization IT Security and reviewed by Audit
			3. In no case shall an encryption key be distributed or exchanged during a telephone conversation, in an e-mail message, by non-encrypted fax, or by any other method than the secure methods authorized by the standard operating procedures.
		4. **Key Storage and Data Scavenging**
			1. Keys may be stored on the device’s hard disk, in memory, on a variety of peripheral devices or tokens.
			2. Risk Assessments shall specifically address the risk to the key associated with data scavenging based on the method of storage, the classification level of the information encrypted/decrypted using the key, and the life of the key.
		5. **Key Length**
			1. Key length may be fixed or variable depending on the encryption algorithm. The minimal encryption key length is 56 bits, however stronger key length is recommended.
			2. The key length requirements will be reviewed annually and upgraded as technology allows.
		6. **Key Life**
			1. Every key should have a defined lifetime based on the function of the key and the risks associated. It is recommended to recycle the key yearly. Any key lifetime beyond one year period has to be approved by Organization IT Security.
		7. **Key Archiving and Key Escrow**
1. Asset owner shall determine the need for key archiving to enable decryption of information encrypted with secret keys.
	1. **Encryption Algorithm Standards**
		* 1. The algorithm standards shall be based on international standards on encryption and the guidance of international institutes, governments, and regulators.
			2. The encryption algorithm will be reviewed annually and upgraded as technology allows.
			3. The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by Organization IT Security.
	2. **Ownership of Encryption Systems**
		* 1. Each encryption and key management system in use within Organization Group shall have an assigned asset owner.
			2. A custodian may be assigned operational and maintenance responsibilities for the encryption system.
			3. The asset owner shall address appropriate segregation of duties based on strict requirements for key protection and minimization of risk arising from granting excessive privileges to any individual.
			4. The asset owner shall provide standard operating procedures and guidelines for all aspects of encryption and key management, operations, and maintenance.
	3. **Logging of Key Management Activities**
		* 1. Logs shall be maintained for security-relevant activities, including: -
				1. Installation of keys
				2. Out of cycle change of keys
				3. Problems and exceptions
				4. Physical access to encryption equipment
			2. The logs shall include the individual or individuals involved the date and time, and the action performed.
			3. Log shall be retained for at least one calendar year.
	4. **Security Incidents Involving Key Compromise**
		* 1. Standard operating procedures for emergency replacement of encryption keys shall be developed and endorsed by IT Security for each encryption system in use within Organization Group.
			2. IT Security, ISD and Audit must be notified when the encryption key is compromised.
	5. **Hardware Maintenance**
		* 1. Standard operating procedures shall be developed to cover the secure delivery of the device to the vendor facility and return to the Organization Group facility. It must also include the procedure for admission and monitoring of the vendor personnel to do hardware maintenance.
			2. The procedures shall address continuous protection of keys associated with the hardware on-site and shall ensure that the keys are removed prior to shipment of encryption device to a vendor facility.
	6. **Disposal of Specialized Encryption Hardware**
		* 1. Unused specialized encryption hardware must be destroyed and disposed.
			2. Standard operating procedures for the disposal of specialized encryption hardware shall specifically address removal and destruction of encryption keys stored in the device.
	7. **Disposal of Keys**
		* 1. Keys that are no longer used or keys that have been replaced with new keys are to be destroyed.
			2. Standard operating procedures for disposal of keys shall specifically address removal and destruction of encryption keys.
	8. **Procedural Requirements**
		* 1. The Standard Operating Procedures and guidelines shall address at least the implementation of the requirements stated in this document.
			2. The following shall be developed and maintained to support consistent, reliable implementation of this ***policy***: -
				1. Encryption component installation and management procedures.
				2. Encryption component maintenance procedures.
				3. Encryption component disposal procedures.
				4. Key management procedures.
				5. Procedures for the distribution/exchange of keys.
				6. Security incident response procedures that address compromise of encryption keys.
				7. Software release processing procedures related to an encryption component.
2. **ENFORCEMENT**

# *All staffs are required to comply with this security policy and its appendices. Disciplinary actions including termination may be taken against any Organization staffs who fail to comply with the Organization’s security policies, or circumvent/violate any security systems and/or protection mechanisms.*

# *Staff having knowledge of personal misuse or malpractice of IT Systems must report immediately to management and IT Security.*

* 1. ***Organization’s staff must ensure that Organization’s contractors and others parties authorized by the Organization using its internal computer systems, comply with this policy.***
	2. ***Where the role of the service provider is outsourced to a vendor, the outsourced vendor should ensure compliance with this policy.***