**Standard for Policy Topic 2: Cryptography**

| **Owner** | [Insert Owner] |
| --- | --- |
| **Responsible Group** | [Company Name] Governance Team |
| **Revision Date** | 24-Mar-2023 |
| **Abstract** | This Standard provides management support for system acquisition, software development, and maintenance that ensures information security is integrated across the entire information systems lifecycle. |
| **Applicability** | This Standard is applicable to [Company Name] employees, other workers, Business Groups, Global Functions, and other relevant [Company name] groups that have been specifically assigned a responsibility in this document. |
| **Status** | Effective as of : 24-Mar-2023 |

**Table of Contents**

1. *Introduction………………………………………………………………………………………….*
2. *Compliance Program…………………………………………………………………………….*
3. *Communication…………………………………………………………………………………….*
4. *Definitions…………………………………………………………………………………………….*
5. *Cryptography Controls and Requirements……………….*
6. *[[1]](#footnote-0)Revision History…………………………………………………………………………………….*

**1 Introduction**

The purpose of this document is to record [Company]’s standard that covers the technique in place to protect the confidentiality, authenticity, and integrity of data.

**2 Compliance Program**

[Insert Company name] Business Groups are required to read this Standard in its entirety and apply it as directed within the Standard.

**3 Communications**

[Insert information on how this information is communicated to company employees]

**4 Definitions**

Relevant definitions for this Standard are included in the table below.

| Term | Definition |
| --- | --- |
| Cryptography | The discipline that embodies principles, means, and methods to transform data in order to hide information content, prevent undetected modification, and/or prevent unauthorized use. |
| Encryption | The process, approved by [Company], by which data is converted into private code to ensure secure transmission or storage. |
| [Insert other relevant terms specific to company procedure] |  |

**5 Cryptography Controls and Requirements**

| **Policy Category 2.1** |
| --- |

| **Compliance with Legal and Contractual Agreements** |
| --- |
| [Company] Cybersecurity must develop and implement methods of information and key protection to ensure proper and effective use of cryptography. All [Company] Business Groups and Functions must implement appropriate cryptography controls as defined by [Company] Cybersecurity. |
| **Policy Category 2.1 Controls**   * 2.1.1 Policy on the Use of Cryptographic Controls * 2.1.2 Key Management |

**Note: Each control identified in each Policy Category table will be detailed as below.**

| Control 2.1.1 |
| --- |

| **Policy on the Use of Cryptographic Control** |
| --- |
| [Company] Cybersecurity must develop and implement a policy on the use of cryptographic controls for the protection of information. Strong cryptography must be used in every case where sensitive data is involved. |

**2.1.1.1 Cryptography Uses**

**2.1.1.2 Implementing Cryptography**

**2.1.1.3 Encryption for Users**

**2.1.1.4 User Encryption of PII and Customer Data**

**2.1.1.5 User of Transport Layer Security (TLS)**

| Control 2.1.2 |
| --- |

| **Key Management** |
| --- |
| [Company] Cybersecurity must develop and implement a policy on the use, protection, and lifetime of cryptographic keys. |

**2.1.2.1 Key Ownership**

**2.1.2.2 Key Backup and Recovery**

**2.1.2.3 Key Changes, Expiration and Renewals**

**2.1.2.4 Key Access for Evidence**

**2.1.2.5 Private Key Strength and Generation**

**2.1.2.6 Key Management**

**6 Revision History**

| **Revision Date** | **Description of change** | **Revision Authority POC** |
| --- | --- | --- |
|  |  |  |

1. Internal Use Only [↑](#footnote-ref-0)