**Standard for Policy Topic 3: System Software Development Life Cycle**

| **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. *System Software Development Life Cycle Controls and Requirements……………….*
6. *[[1]](#footnote-0)Revision History…………………………………………………………………………………….*

**1 Introduction**

The purpose of this document is to record [Company]’s system software development lifecycle (SDLC) policy, requirements and the responsibilities for implementation. A SDLC emphasizes decision processes that influence system cost and usefulness. These decisions must be based on full consideration of business process, functionality requirements, and economic and technical feasibility in order to produce an effective system.

**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 |
| --- | --- |
| SDLC | An abbreviation for Software Development Lifecycle. The process that [insert company name] development teams use to design and build high quality software. |
| [Insert other relevant terms specific to company procedure] |  |

**5 Software Development Life Cycle Controls and Requirements**

| **Policy Category 3.1** |
| --- |

| **Security in Development and Support Processes** |
| --- |
| [Company] Business Groups and Functions that perform software development must perform work in a secure development environment and adhere to a set of change control procedures and secure engineering principles. |
| **Policy Category 10.2 Controls**   * 3.1.1 Secure Development Policy * 3.1.2 System Change Control Procedures * 3.1.3 Technical Review of Applications after Operating Platform Changes * 3.1.4 Restrictions on Changes to Software Packages * 3.1.5 Secure System Engineering Principles * 3.1.6 Secure Development Environment * 3.1.7 System Security Testing * 3.1.8 System Acceptance Testing |

Example:

| Control 3.1.1 |
| --- |

| **Secure Development Policy** |
| --- |
| [Company] Information Technology and/or Cybersecurity must establish and implement rules for the development of [Company] software and systems. |

**3.1.1.1 System Development Lifecycle (SDLC)**

[Company] Information Technology and other IT infrastructure owners are responsible for adopting, implementing, and requiring compliance with an SDLC process and workflow. The SDLC must define initiation, development.acquisition, implementation, operations, and disposal requirements. SDLC must be used for both new developments and code reuse scenarios.

**3.1.1.2 SDLC Protocols**

**3.1.1.3 Threat Modeling**

**3.1.1.4 Security Control Evaluation**

**3.1.1.5 Secure Development & Hosting Requirements**

**Note: Each control identified in the Policy Category table will be detailed as above.**

| **Policy Category 3.2** |
| --- |

**Policy Category 3.1**

| **Test Data** |
| --- |
| [Company] Business Groups and Functions must identify, label, and appropriately protect any tst data collected. |
| **Policy Category 3.2 Controls**   * 3.2.1 Protection of Test Data |

| Control 3.1.2 |
| --- |

| **System Change Control Procedures** |
| --- |
| [Company] Information Technology and/or Cybersecurity must control changes to systems within the development lifecycle through formal change control procedures. |

**3.1.2.1 Formal Change Control Process**

**3.1.2.2 Change Approvals**

**3.1.2.3 Identifying Second Order Updates**

**3.1.2.4 Update Restrictions**

| Control 3.1.3 |
| --- |

| **Technical Review of Applications After Operating Platform Changes** |
| --- |
| [Company] Information Technology must review and test business critical applications when operating platforms are changed. This is to ensure there is no adverse impact on organizational operations or security. |

**3.1.3.1 Technical Review Process**

| Control 3.1.4 |
| --- |

| **Restrictions on Changes to Software Packages** |
| --- |
| [Company] Information Technology must define protocols for modifications to software packages, limiting updates to only necessary changes. [Company] Information Technology must strictly control all software changes and updates. |

**3.1.4.1 Software Restrictions**

**3.1.4.2 Change Management Process**

| **Policy Category 3.3** |
| --- |

| **Security Requirements of Information Systems** |
| --- |
| [Company] Business Groups and Functions must identify, label, and appropriately protect any tst data collected. |
| **Policy Category 3.2 Controls**   * 3.2.1 Protection of Test Data |

| Control 3.3.1 |
| --- |

| **Protection of Test Data** |
| --- |
| [Company] Information Technology must ensure that test data is carefully selected, protected, and controlled. |

**3.3.1.1 Test Data Collection Protocols**

**3.3.1.2 Test Data Classification**

**6 Revision History**

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

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