**Standard for Policy Topic 1: Operations Security**

| **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. *Operations Security Controls and Requirements……………….*
6. *[[1]](#footnote-0)Revision History…………………………………………………………………………………….*

**1 Introduction**

The purpose of this document is to record [Company]’s operations security policy, requirements and the responsibilities for implementation. Operations Security covers important security practices including protection against malware (e.g. anti-virus software), information backups, event logging, and clock synchronization.

**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 Policy document.

**5 Operations Security Controls and Requirements**

| **Policy Category 1.1** |
| --- |

| **Operational Procedures and Responsibilities** |
| --- |
| [Company] Business Groups and Functions must ensure correct and secure operations of information processing facilities, business data centers, labs and development environments. |
| **Policy Category 1.1 Controls**   * 1.1.1 Documenting Operating Procedures * 1.1.2 Change Management * 1.1.3 Capacity Management * 1.1.4 Separation of Development, Testing and Operation Environments |

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

| Control 1.1.1 |
| --- |

| **Documenting Operating Procedures** |
| --- |
| Operating procedures must be documented and made available to HP employees an other workers who need them. |

**1.1.1.1 Operating Procedures Development**

**1.1.1.2 Implementing Operating Procedures**

**1.1.1.3 Secure Configurations Procedures**

**1.1.1.4 Implementing Secure Configurations**

| Control 1.1.2 |
| --- |

| **Change Management** |
| --- |
| Changes to any [Company] business processes, information processing facilities, business data centers, development environments and systems that affect information security must be controlled. |

**1.1.2.1 Change Control Board**

**1.1.2.2 CCB Frequency and Format**

**1.1.2.3 Testing Technical Changes**

**1.1.2.4 User Functional Testing**

**1.1.2.5 Fall-back Procedures**

**1.1.2.6 Compliance Review for Major Technical Changes**

**1.1.2.7 Compliance Review for Emergency Changes**

| **Policy Category 1.2** |
| --- |

**Policy Category 3.1**

| **Protections from Malware and Vulnerabilities** |
| --- |
| [Insert description of Policy Category] |
| **Policy Category 1.2 Controls**   * 1.2.1 Controls Against Malware and Vulnerabilities |

| Control 1.2.1 |
| --- |

| **Controls Against Malware and Vulnerabilities** |
| --- |
| Detection, prevention and recovery controls to protect against malware and vulnerabilities must be implemented and combined with appropriate user awareness. |

**1.2.1.1 Malware and Vulnerability Management**

**1.2.1.2 Centralized Malware Protection**

**1.2.1.3 Firewalls**

**1.2.1.4 Network Intrusion Detection Systems**

| **Policy Category 1.3** |
| --- |

| **Logging and Monitoring** |
| --- |
| [Company] Business Groups and Functions must monitor information assets under their responsibility and record all information security events. |
| **Policy Category 1.3 Controls**   * 1.3.1 Event Logging * 1.3.2 Protection of Log Information * 1.3.3 Administrator and Operator Logs * 1.3.4 Clock Synchronization |

| Control 1.3.1 |
| --- |

| **Event Logging** |
| --- |
| Event logs recording user activities, exceptions, faults, and information security events must be produced, kept, and regularly reviewed. |

| Control 1.3.2 |
| --- |

| **Protection of Log Information** |
| --- |
| Logging facilities and log information must be protected against tampering and unauthorized access. |

| Control 1.3.3 |
| --- |

| **Administrator and Operator Logs** |
| --- |
| System administrator and system operator activities must be logged. The logs must be protected and regularly reviewed. |

| Control 1.3.4 |
| --- |

| **Clock Synchronization** |
| --- |
| The clocks of relevant information processing systems with a [Company] or security domain must be synchronized to a single reference time source. |

| **Policy Category 1.4** |
| --- |

| **Technical Vulnerability Management** |
| --- |
| [Company] must prevent exploitation of technical vulnerabilities by establishing a method to obtain awareness of known vulnerabilities affecting [Company] systems and network devices, control introduction of new vulnerabilities, scan for existing vulnerabilities, and evaluate appropriate measures to reduce risk - up to and including disconnecting vulnerable machines  after notice. |
| **Policy Category 1.4 Controls**   * 1.4.1 Management of Technical Vulnerabilities * 1.4.2 Restriction of Software Installation |

| Control 1.4.1 |
| --- |

| **Management of Technical Vulnerabilities** |
| --- |
| Information about technical vulnerabilities of information systems being used must be obtained in a timely fashion. [Company] Information Technology must ensure [Company]’s exposure to such vulnerabilities is evaluated and take appropriate measures to address the associated risks. |

**1.4.1.1 Identification of Vulnerabilities**

**1.4.1.2 Security and Patch Management**

**1.4.1.3 Vulnerability Categories and Timelines**

[Company] Information technology and other infrastructure owners must ensure that system components and software are protected from known vulnerabilities by installing applicable vendor supplied security patches, and critical security patches must be applied within one month of their release.

[Company] Cybersecurity must ensure technical vulnerabilities, including vendor supplied patches, are remediated following the timeline below:

* Emergency - 24-48 hours from when remediation/patch is available
* Critical - 30 calendar days
* High - 30 calendar days
* Medium - 45 calendar days
* Low - 60 calendar days

Vulnerabilities are classified based on the vendor classifications or CVSS score bracket.

**6 Revision History**

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

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