Desktop – Laptop Configuration Standard

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: Internal*

**Internal INFORMATION**

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX.

Table of Contents

1. Introduction 4

1.1 Document Definition 4

1.2 Objective 4

1.3 Scope 4

1.3.1 Applicability to employees 4

1.3.1 Applicability to External Parties 4

1.3.2 Applicability to Assets 4

1.4 Industry Configuration Standards 4

1.5 Related Documents / References 4

2. Standard Statements 5

2.1 Minimum Hardware Configuration Standards for Computers 5

2.2 Assured Data at rest 6

2.3 Authentication 6

2.4 Secure Boot 6

2.5 Platform Integrity and Application Sandboxing 7

2.6 Application Whitelisting 7

2.7 Malicious Code 7

2.8 Security Policy Enforcement 7

2.9 External Interface protection 8

2.10 Device Policy Update 8

2.11 Event Collection for Enterprise analysis 8

2.12 Incident Response 9

2.13 Device Sanitisation and re-provisioning 9

2.14 Wi-Fi 9

2.15 Browsers 10

2.16 Assured Data in Transit 10

3. Standard Compliance & Enforcement 11

3.1 Compliance Measures 11

3.2 Enforcement 11

4. Exception Process / Glossary 12

4.1 Exception Process 12

4.2 Glossary / Acronyms 12

5. Document Management 13

5.1 Document Revision Log 13

5.2 Document Ownership 13

5.3 Document Coordinator 13

5.4 Document Approvers 13

5.5 Distribution 13

# Introduction

## Document Definition

This document is a Standard.

For a full description of document types, see XXXX-POL-ALL-001 - Information Security Policy Framework.

## Objective

This Standard provides the list of controls that are required to secure laptop and desktop operating system deployment and realise an approved level of security and hardware requirements. It provides a list of security controls to protect these assets where it is used to provide application access

## Scope

### Applicability to employees

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This Standard applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant Standard statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This Standard applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Industry Configuration Standards

* Centre for Internet Security (CIS): http://www.cisecurity.org/

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*

# Standard Statements

## Minimum Hardware Configuration Standards for Computers

**Laptop Computers**

Minimum Configuration:

Processor (CPU): Intel Core i5 (sixth generation or newer) or equivalent

Operating System: Microsoft Windows 10 Professional x64

Memory: 8 GB RAM

Storage: 500 GB internal storage drive

Monitor/Display: 14" LCD monitor, resolution of 1600 x 900 or better.

Network Adapter: 802.11ac 2.4/5 GHz wireless adapter

Other: Internal or external Webcam, lock, carrying case, external hard drive for backups

**Desktop Computers**

Minimum Configuration:

Processor (CPU): Intel Core i5 (sixth generation or newer) or equivalent

Operating System: Microsoft Windows 10 Professional x64

Memory: 8 GB RAM

Storage: 512 GB internal Solid-State Drive (SSD) or 1 TB internal HDD

Sustainability: EPEAT Silver rating (preferably EPEAT Gold)

Monitor/Display: 24" LCD monitor

Network Adaptor: 802.11ac 2.4/5 GHz wireless adapter

Other: Webcam, lock, external drive for backups

## Assured Data at rest

|  |  |
| --- | --- |
| **S/N** | **Security Control Requirement** |
| 2.1. | Data stored on the desktop MUST be satisfactorily prevented from unauthourised access |
| 2.2. | Measures must be put in place to ensure data stored on shared folders are only accessed on a need to know basis |

## Authentication

|  |  |
| --- | --- |
| **S/N** | **Security Control Requirement** |
| 3.1. | Each of the three types of authentication described MUST be implemented:   * User to desktop: Authenticating to the device in line with XXXX authentication policy, the user is only granted access to the desktop after successfully authenticating to the desktop. * User to service: The user is only able to access enterprise services after successfully authenticating to the service, via their desktop/laptop. Access via remote services requires successfully authenticating to the service, via authourised device types. * Device to service: Only XXXX authourised devices can authenticate to the enterprise to be granted access. |
| 3.2. | All default passwords MUST be changed and password configuration parameter options set in accordance with XXXX User Access Control Policy. |
| 3.3. | System administration privileged accounts MUST only be used on devices deployed to perform administrative function. Such privileged user accounts with administrative privileges MUST deploy strong authentication including a second factor to authenticate to the platform at both logon and unlock time |

## Secure Boot

|  |  |
| --- | --- |
| **S/N** | **Security Control Requirement** |
| 4.1. | An unauthourised entity MUST not be able to modify the boot process of a device, and any attempt to do so MUST be detected, where suitable mechanisms exist. |
| 4.2. | Due to the platform specific vendor protection methods available, a risk assessment  of the vendor secure boot implementation guidance MUST confirm if the platform meets XXXX protective security requirements. |
| 4.3. | Users MUST be educated to recognise and report where suspicion is that the boot process has been compromised. |

## Platform Integrity and Application Sandboxing

|  |  |
| --- | --- |
| **S/N** | **Security Control Requirement** |
| 5.1. | The desktop can continue to operate securely despite potential compromise of an application or component within the platform and there MUST be the ability to restrict the capabilities of applications on the desktop, where configuration allows. |
| 5.2. | Robust hardening of operating system, access controls and file permissions must meet application sandbox requirements. |

## Application Whitelisting

|  |  |
| --- | --- |
| **S/N** | **Security Control Requirement** |
| 6.1. | A whitelist of authourised applications MUST be defined and maintained, constrained to allow only authourised applications to run on devices to reduce the ability for malicious code to execute. |
| 6.2. | Arbitrary application installation by users MUST not be allowed. |
| 6.3. | Authourised application deployment MUST only be performed by an administrator using a trusted mechanism. |

## Malicious Code

|  |  |
| --- | --- |
| **S/N** | **Security Control Requirement** |
| 1. | All device operating systems MUST implement capability to detect, isolate and defeat malicious code which becomes present on the device.  The selection of appropriate countermeasures to be informed by a per platform risk assessment selection. This MUST include platform specific recommendations for Malware Threat countermeasures and in combination include:-   * Anti-malware tools; * Behavioural monitoring of applications and platform; * File and URL reputation. |
| 2. | There MUST be an agreed anti-malware solution deployed on the desktop endpoint  that deploys established product(s) |
| 3. | Current operating system patch and software version MUST be installed and maintained throughout lifecycle of the devices |
| 4. | Content-based attacks MUST be filtered by scanning capabilities in the organisation. |

## Security Policy Enforcement

|  |  |
| --- | --- |
| **S/N** | **Security Control Requirement** |
| 8.1. | Platform specific security policies MUST be agreed at desktop/laptop device selection then robustly implemented across the Enterprise platform to technically enforce Security Group policy, where possible. |
| 8.2. | Only privileged users with specific change control authourisation MUST be able to override or modify Security Group Policy. |
| 8.3. | Security policies MUST be enforced. A combination of operating system and third- party product configuration specific to the platform can meet this requirement. |
| 8.4. | Mobile Device Management (MDM) profiles MUST be marked as non-removable so the user cannot remove them and alter their configuration. |

## External Interface protection

|  |  |
| --- | --- |
| **S/N** | **Security Control Requirement** |
| 9.1. | The laptop/desktop MUST be able to restrict the set of ports available and MUST be hardened and robust to malicious attack. |
| 9.2. | Network interface protection MUST include a host based firewall configured to prevent inbound initiated network connections to the device and limiting outbound connection to XXXX approved IPSec, on the required ports, where external connection is required. |
| 9.3. | Physical and wireless interfaces MUST only allow a whitelist of authourised peripherals or peripheral classes to connect and communicate with the laptop/desktop, additionally connection MUST only be using specific protocols. Subject to risk assessment, interface configuration MUST block unauthourised external devices e.g. USB removable media or configured to read-only, to limit data import and export where business requirements exist. |
| 9.4. | Direct Memory Access (DMA) MUST be restricted from external interfaces. Where  the OS platform does not control access via DMA it is advisable to procure hardware which does not have external DMA interfaces present. |
| 9.5. | All exports to the Internet MUST be authourised and traceable to a user. |

## Device Policy Update

|  |  |
| --- | --- |
| **S/N** | **Security Control Requirement** |
| 10.1. | The Enterprise solution (whether that on premise or in Cloud) MUST be able to issue  security updates and remotely validate the patch level of all authourised laptop/desktop endpoint device types across the entire XXXX. |
| 10.2. | The appropriate version/patches for the OS MUST be downloaded and installed in accordance with XXXX patching policy. |
| 10.3. | There MUST be controls implemented to audit, monitor and as functionally available  per laptop/desktop device specifics, enforce updates of the OS platform, system firmware and any appropriate applications. |

## Event Collection for Enterprise analysis

|  |  |
| --- | --- |
| **S/N** | **Security Control Requirement** |
| 11.1. | The Enterprise solution (whether that on premise or in Cloud) MUST be able to report security-critical events to XXXX Enterprise SOC audit and monitoring service for all  authourised laptop/desktop device types and services. |
| 11.2. | Security critical events which can **only** be collected from the desktop are required to be logged as collecting audit events from enterprise services is preferred where possible and duplication of event collection should be avoided. Desktop logging includes (not an exhaustive list) e.g.:-   * User log in and log out * Local security alerts from third party tools or platform components such as alerts from anti-malware, host based firewall, platform integrity checks which fail. |
| 11.3. | Event collections MUST be implemented using an appropriate assessed solution. User MUST be prevented from log tampering and the Integrity of the reporting service protected. Risk assessment MUST be used to determine the requirement for  viewing both locally and remotely. |
| 11.4. | Accurate time stamps are required for audit and time on devices should be maintained through an NTP hierarchy with links to common XXXX time services. |

## Incident Response

|  |  |
| --- | --- |
| **S/N** | **Security Control Requirement** |
| 12.1. | XXXX laptop/desktop devices MUST have configurable capability to support the XXXX’s Enterprise incident handling and response plans.  Appropriate laptop/desktop functionality includes:-  Desktop to be locked, wiped, and configured remotely;  Sending a wipe command to the desktop and revoking credentials;  Remote function to destroy encryption key material or using secure erase functions if the device is present |
| 12.2. | The enterprise MUST revoke user credentials and / or access to XXXX network by  revoking both the remote connection client and any other enterprise services certificate e.g. e-mail that are stored on the desktop whenever a compromise is suspected. |

## Device Sanitisation and re-provisioning

|  |  |
| --- | --- |
| **S/N** | **Security Control Requirement** |
| 13.1. | Where deploying or redeploying XXXX endpoint devices within a XXXX Security management boundary domain, platform specific guidance MUST be defined under risk assessment agreement to restore a misconfigured or potentially compromised device to a known-good state using native functionality. Scenarios include:-   * Sanitising device believed to be compromised with malware; * Preparing a device which has not previously been managed; * Reissuing device to a different user in the same security environment. |

## Wi-Fi

|  |  |
| --- | --- |
| **S/N** | **Security Control Requirement** |
| 14.1. | Captive Portals  XXXX laptop/desktop devices MUST be configured to maintain always-on XXXX proxy when not connected to the XXXX LAN Infrastructure and Internet is available. A risk assessment is therefore mandatory to avoid threats that captive portal Wi-Fi hot spots introduce from a connection outside of XXXX management domain. |

## Browsers

|  |  |
| --- | --- |
| **S/N** | **Security Control Requirement** |
| 15.1. | XXXX laptop/desktop devices MUST deploy a mature and secure browser product that is in support and maintains a hardened build that takes advantage of the native security features of the underlying platform and remains compliant with XXXX patch policy. |

## Assured Data in Transit

|  |  |
| --- | --- |
| **S/N** | **Security Control Requirement** |
| 16.1. | Data MUST be protected as it transits between the Desktop and any connecting service(s). |
| 16.2. | All network data from the desktop MUST be routed over an agreed secure enterprise VPN when working remotely. Using an assured VPN protects Confidentiality and Integrity of the traffic. |
| 16.3. | Where certificates provide user or machine credentials, they MUST be used, and these credentials should bind to the device’s hardware. |

# Standard Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Standard can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Standard. The following list is not exhaustive, and all example evidence types may not be required to validate compliance.

Evidence of compliance can be presented in hard copy or electronic format.

|  |  |
| --- | --- |
| **Criteria** | **Example Evidence** |
| Review the settings on sample of desktops and laptops | * Confirm if the devices are configured in line with this standard |

## Enforcement

All staff of XXXX must comply with all Information Security Standards. Failure to comply with these standards may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Exception Process / Glossary

## Exception Process

Non-compliance with the Standard statements described in this document must be reviewed and approved in accordance with the Exception Process defined in *XXXX-POL-ALL-001 - Information Security Policy Framework.*

## Glossary / Acronyms

|  |  |
| --- | --- |
| DMA | Direct Memory Access |
| IPsec | Internet Protocol Security |
| MDM | Mobile Device Management |
| NTP | Network Time Protocol |
| TPM | Trusted Platform Module |
| USB | Universal Serial Bus |
| VPN | Virtual Private Network |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |

## Document Ownership

This Standard is owned by the YYYY

## Document Coordinator

This Standard is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |

## Distribution

* *Information Security*
* *IT Department*