Security Standard – Desktop Operating System (SS-010)

Chief Security Office

Date: March 2020

Department for Work & Pensions

1. Revision History

Version	Author	Description	Date
0.0a		First Draft	09/05/17
0.0b		Amended to include team feedback	31/05/17
0.0c		Amended to include SME feedback	02/07/17
0.0d		Amended to include Domain Architect feedback	23/08/17
1.0		First published version	18/09/2017
1.1		Version for external publication	30/03/2020

2. Distribution

Version	Role/Area	Role	Date
0.0a		Project Team & Security Architecture	09/05/17
0.0b		SME	05/06/17
0.0c		Domain Architects	07/08/17
0.0d		Chief Security Officer	24/08/17
1.0		First published version	18/09/2017

3. Approval History

Version	Approver Title	Role	Date
1.0		Chief Security Officer	18/09/2017
1.1		Chief Security Officer	30/03/2020

This document will be reviewed for continued completeness, relevancy and accuracy within 1 year of being granted "final" status, and at yearly intervals thereafter.

Contents

4. Introduction

4.1. This Desktop Operating System Security Standard provides the list of controls that are required to secure desktop operating system deployments to an Authority approved level of security. It provides a list of security controls to protect OFFICIAL assets where the desktop is used to provide application access. Compliant implementation will minimise the risk from physical and logical known threats to an acceptable level for Authority assets operating at OFFICIAL.

5. Purpose

5.1. The purpose of this document is to enable teams to work to a defined set of security requirements which enable solutions to be developed, deployed and managed to Authority security standards, which are based upon international best practice for Desktop Operating System deployments.

5.2. Secondly, this standard provides a means to conduct compliance based technical security audits.

6. Exceptions

6.1. Any exceptions to the application of this standard or where controls cannot be adhered to MUST be presented to the Authority where appropriate. This MUST be carried out prior to deployment and managed through the design caveats or exception process.

6.2. Such exception requests may invoke the Risk Management process in order to clarify the potential impact of any deviation to the configuration detailed in this standard.

6.3. Exceptions to this standard MUST be maintained on a risk register for accountability, traceability and security governance reporting to the Authority.

7. Audience

7.1. This standard is intended for Suppliers, Desktop and Database Administrators, Developers, security groups, and also IT staff such as Security Compliance Teams, involved in securing environments for Authority systems and applications.

8. Scope

8.1. This standard covers systems handling data within the OFFICIAL tier of the Government Security Classification Policy (GSCP). All Supplier desktop system end point implementations falling within this category are subject to the requirements specified. This applies to new and existing installations.

8.2. The security control requirements laid out in this standard are product agnostic and applicable for all Desktop Operating systems both physical and virtual that are provisioned to handle Authority data.

8.3. In the event of uncertainty on the controls laid out in this standard please contact the Authority for guidance and support on items which require clarification.

9. Security Controls Assurance

9.1. Controls presented in this standard or referred to via this standard MUST be subjected to a formalised IT Health Check penetration test to provide evidence of adequacy and effectiveness of implementation before deployment to production. Note the scope of ITHC including vulnerability scan will be proportionate to the scope of solution change. The frequency of retesting to be determined by risk assessment e.g. changes in deployment reconfiguration.

10. Technical Security Control Requirements

In this document the term MUST in upper case is used to indicate an absolute requirement. Failure to meet these requirements will require a formal exemption (see section [6. Exceptions] above).

10.1. Assured Data in Transit

Reference	Security Control Requirement
10.1.1.	Data MUST be protected as it transits between the Desktop and any connecting service(s).
10.1.2.	An assured IPsec client MUST be implemented. Validation to Foundation grade is strongly recommended. This is to support the IPsec VPN for Remote Working Software Client with security characteristics configured in accordance with the PSN End State IPsec profile.
10.1.3.	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.
10.1.4.	An assured firewall solution MUST be used in compliance with SS-013 Firewall Security Standard, configured to block outbound traffic when the VPN is not active.

Reference	Security Control Requirement
10.1.5.	Where certificates provide user or machine credentials, they MUST be used and these credentials should bind to the device's hardware.

10.2. Assured data at rest

Reference	Security Control Requirement
10.2.1.	Data stored on the desktop MUST be satisfactorily encrypted when the desktop is in its rest state. For always on devices, this is when the device is locked. Assurance of this function is necessary that takes into account NCSC End User Device Security Principles and SS-007 Use of Cryptography Security Standard.
10.2.2.	The desktop MUST be configured to provide full volume encryption using an assured data-at- rest encryption product
10.2.3.	A Trusted Platform Module (TPM) can be used in place of a token where the deployment environment risks allow, making the user's experience smooth whilst providing a similar degree of cryptographic strength to the Smart Token method.

10.3. Authentication

Reference	Security Control Requirement
10.3.1.	Each of the three types of authentication described MUST be implemented: • User to desktop: Authenticating to the device in line with SS-001 Access and Authentication Controls security standard, 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. Access via remote services requires successfully authenticating to the service, via authorised device types. • Desktop to service: Only Authority authorised desktops which can authenticate to the enterprise can be granted access.
10.3.2.	There MUST be authentication to both the encryption product i.e. to access the encrypted drive and the OS platform.
10.3.3.	All default passwords MUST be changed and password configuration parameter options set in accordance with SS-001pt1 Access and Authentication Controls Security Standard.
10.3.4.	Use of Biometric authentication factors MUST be subject to risk assessment to determine authentication strength.
10.3.5.	System administration privileged accounts MUST only be used on desktops 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 in compliance with SS-001 pt2 Access and Authentication Controls Security Standard.

10.4. Secure Boot

Reference	Security Control Requirement
10.4.1.	An unauthorised entity MUST not be able to modify the boot process of a desktop, and any attempt to do so MUST be detected, where suitable mechanisms exist.
10.4.2.	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 the Authority's protective security requirements.
10.4.3.	Users MUST be educated to recognise and report where suspicion is that the boot process has been compromised.

10.5. Platform Integrity and Application Sandboxing

Reference	Security Control Requirement
10.5.1.	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.
10.5.2.	Robust hardening of operating system, access controls and file permissions will meet application sandbox requirements when fully implemented. The recommended platform specific guidance selected MUST be implemented accordingly.

10.6. Application Whitelisting

Reference	Security Control Requirement
10.6.1.	A whitelist of authorised applications MUST be defined and maintained, constraining to allow only authorised applications to run on the desktop to reduce the ability for malicious code to execute.
10.6.2.	Arbitrary application installation by users MUST not be allowed.
10.6.3.	Authorised application deployment MUST only be performed by an administrator using a trusted mechanism.

10.7. Malicious Code

Reference	Security Control Requirement
10.7.1.	All Desktop 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.
10.7.2.	There MUST be an agreed anti-malware solution deployed on the desktop endpoint that deploys established product(s) (SS-015 Malware Protection Security Standard)
10.7.3.	Desktop patch and software version (N / N-1) MUST be installed and maintained throughout lifecycle.
10.7.4.	Content-based attacks MUST be filtered by scanning capabilities in the organisation.

10.8. Security Policy Enforcement

Reference	Security Control Requirement
10.8.1.	Platform specific security policies MUST be agreed at desktop device selection then robustly implemented across the Enterprise platform to technically enforce Security Group policy, where possible.
10.8.2.	Only privileged users with specific change control authorisation MUST be able to override or modify Security Group Policy.
10.8.3.	Security policies MUST be enforced. A combination of operating system and Supplier product configuration specific to the platform can meet requirements.
10.8.4.	Mobile Device Management (MDM) profiles MUST be marked as non-removable so the user cannot remove them and alter their configuration.

10.9. External Interface protection

Reference	Security Control Requirement
10.9.1.	The desktop MUST be able to constrain the set of ports available and MUST be hardened and robust to malicious attack.

Reference	Security Control Requirement
10.9.2.	Network interface protection MUST include a host based firewall configured to prevent inbound initiated network connections to the device and limiting outbound connection to the Authority's IPsec VPN gateway only, on the required ports, where external connection is required.
10.9.3.	Physical and wireless interfaces MUST only allow a whitelist of authorised peripherals or peripheral classes to connect and communicate with the desktop, additionally connection MUST only be using specific protocols. Subject to risk assessment, interface configuration MUST block unauthorised external devices e.g. USB removable media or configured to read-only, to limit data import and export where business requirements exist.
10.9.4.	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.
10.9.5.	All exports to the Internet MUST be authorised by and traceable to a user.

10.10. Device Policy Update

Reference	Security Control Requirement
10.10.1.	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 authorised desktop endpoint device types across the entire estate.
10.10.2.	The appropriate version/patches for the OS MUST be downloaded and installed in accordance with SS-033 Patching Security Standard.
10.10.3.	There MUST be controls implemented to audit, monitor and as functionally available per desktop device specific, enforce updates of the OS platform, system firmware and any appropriate applications.

10.11. Event Collection for Enterprise analysis

Reference	Security Control Requirement
10.11.1.	The Enterprise solution (whether that on premise or in Cloud) MUST be able to report security-critical events to an Enterprise SOC audit and monitoring service for all authorised desktop device types and services. (SS-012 Protective Monitoring Security Standard)
10.11.2.	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 Supplier tools or platform components such as alerts from anti-malware, host based firewall, platform integrity checks which fail.
10.11.3.	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.
10.11.4.	Accurate time stamps are required for audit and time on devices should be maintained through an NTP hierarchy which chains to common Authority time services.

10.12. Incident Response

Reference	Security Control Requirement
10.12.1.	Supplier desktop devices MUST have configurable capability to support incident handling and response plans. Appropriate 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
10.12.2.	The enterprise MUST revoke user credentials and / or access to the Authority network by revoking both the VPN client any other enterprise services certificate e.g. e-mail that are stored on the desktop whenever a compromise is suspected.

10.13. Desktop device Sanitisation and re-provisioning

Reference	Security Control Requirement
10.13.1.	Data sanitisation methods available currently may not result in the secure erasure of data, which results in a principle security concern for OFFICIAL Tier information. HMG IA Standard No. 5 (IS5) MUST be applied before end points containing Authority data are released outside the Authority's Security management boundary domain to confirm whether whole disc encryption supports safe disposal compliance.
10.13.2.	Where deploying or redeploying endpoint devices within an Authority 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.

10.14. Browsers

Reference	Security Control Requirement
10.14.1.	Supplier desktop devices MUST deploy a mature and secure browser product that is in support and maintains a hardened build that keeps takes advantage of the native security features of the underlying platform and remains compliant with SS-033 Patching Security Standard.

11. Compliance

Compliance with this standard MUST occur as follows:

Compliance	Due Date
On-going	From the first day of approval
Retrospective	Within 6 months of the approval of the standard.

12. Accessibility

No user interfaces are included in this standard and accessibility is not applicable as part of this standard. However, it is deemed that Suppliers implementing this standard are obliged to incorporate accessibility functions where necessary.

13. Security Standards Reference List

Document Name	Location	Version
SS-007 Use of cryptography Security Standard.		
SS-012 Protective Monitoring Security Standard		
SS-013 Firewall Security Standard		
SS-015 Malware Protection Security Standard		

14. Definition of Terms

Captive portal	A web page that the user of a public-access network is obliged to view and interact with before access is granted.
Cryptographic Items	All logical and physical items used to achieve confidentiality, integrity, non-repudiation and accountability; including, but not limited to: devices, products, systems, key variables and code systems.
Cryptographic Key Material	Any parameter passed to an encryption cipher which influences the output of the algorithm (with the exception of the message itself).
Data sanitisation	The process of deliberately, permanently, and irreversibly removing or destroying the data stored on a memory device.
Firewall	Type of security barrier placed between network environments consisting of a dedicated device or a composite of several components and techniques through which all traffic from one network environment traverses to another, and vice versa, and only authorised traffic, as defined by the local security policy, is allowed to pass.
Malware	Malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability.
Security Group Policy	Provides centralized management and configuration of operating systems, applications, and users' settings
Vulnerability	Weakness of an asset or control that can be exploited by one or more threats.

15. Glossary

AES	Advanced Encryption Standard – defined in FIPS 197. Different modes of operation are covered in different documents.
CA	Certificate Authority
Authority	The Authority refers to the Department for Work and Pensions (DWP)
DA	Design Authority (DA)
DMA	Direct Memory Access
IPsec	Internet Protocol Security

ITHC	IT Health Check
LAN	Local Area Network
MDM	Mobile Device Management
NCSC	National Cyber Security Centre
NTP	Network Time Protocol
OS	Operating System
SUPPLIER	Is inclusive of Contractor, their employees or any sub-contractors used
TPM	Trusted Platform Module
USB	Universal Serial Bus
VPN	Virtual Private Network