Security Standard – Malware Protection (SS-015)

Chief Security Office

Date: March 2020

Department for Work & Pensions

1. Revision History

Version	Author	Description	Date
0.1		First Draft	09/11/16
0.2		Adoption of Table Format	22/11/16
0.3		Merging of Comments and Peer Review. Applied to Standard Template.	12/12/16
0.4-0.5		Moved to new template and minor updates to content	22/02/17
1.0		1st published version	20/03/2017
1.1		Version for external publication	30/03/2020

2. Distribution

Version	Role/Area	Role	Date

3. Approval History

Version	Approver Title	Role	Date
1.0		DWP Chief Security Officer	20/03/2017
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

1. Revision History 2
2. Distribution 2
3. Approval History 2
4. Introduction 4
5. Purpose 4
6. Exceptions 5
7. Audience 5
8. Scope 5
9. Security Controls Assurance 5
10. Malware Protection Security Requirements 6
    - 10.1. Product Selection and Installation 6
    - 10.2. User Awareness Training 6
    - 10.3. Operating System 7
    - 10.4. Anti-malware software 7
    - 10.5. Browser 8
    - 10.6. Removable Storage 8
    - 10.7. VPN 8
    - 10.8. Instant Messaging 9
    - 10.9. General Software Controls 9
    - 10.10. File Transfer Controls 9
    - 10.11. Threat Intelligence 10
    - 10.12. Anti-Malware Software 10
    - 10.13. Content Inspection and defence in depth 11
    - 10.14. Log Configuration and Collection 12
    - 10.15. Log Review and analysis 12
    - 10.16. Malware Incidents Preparation and Real Time Controls 13
    - 10.17. Malware Incidents Post Mortem 14
11. Introduction 14
12. Accessibility 14
13. Definition of Terms 14
14. Glossary 15

4. Introduction

4.1. This Malware Protection Security Standard provides the list of controls that are required to secure User Access Devices, Servers and infrastructure components to an Authority approved level of security. This standard provides a list of security controls to protect citizen and operational data to be stored or processed in order to minimise the risk from known threats both physical and logical to an acceptable level for operations.

Quoting NIST (National Institute of Standards and Technology) the definition of malware is:

"*Malware, also known as malicious code, refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system.*

Malware is the most common external threat to most hosts, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations."

Statement of Applicability of this standard:

Traditionally malware protection and mitigation has been associated with desktop endpoints exclusively. However, there are a number of usage cases for malware based controls. Agent based malware mitigation software MUST be considered on desktop endpoints, mobile end points, indeed all End User Devices along with all server end points (physical and virtual including Hypervisor) and at the content inspection and inline infrastructure layers.

Malware detection capability MUST be considered on webserver end points, mail server endpoints, remote access server's/ VPN concentrators, firewalls, proxy and reverse proxy servers and intrusion prevention systems

4.2. Furthermore, the security controls presented in this standard are taken from the international best practice for Malware Protection and have been tailored for Authority suitability.

5. Purpose

5.1. The purpose of this document is to enable Suppliers 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 Malware Protection 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

This standard is intended for Suppliers, system administrators, security groups, and IT staff involved in securing environments for Authority systems and applications and provides requirements on how to manage malware mitigation, logging and incident handling

8. Scope

8.1. This standard is to cover systems handling data within the OFFICIAL tier of the Government Security Classification Policy (GSCP). All endpoints that are capable of having Anti-Malware software based agents installed to help protect against and remediate infection, MUST meet all the requirements in this standard to attest to meet the Authority standard. All endpoints that are also receiving auxiliary agentless anti-malware mitigation via IDS/ IPS, Next Generation Sandboxing devices, and other Content Inspection devices MUST meet all of the logging and incident handling requirements.

8.2. The security control requirements laid out in this standard are product agnostic and applicable for all Information systems that provide services to the Authority.

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 may be subjected to a formalised IT Health Check penetration test to provide evidence of adequacy and effectiveness.

10. Malware Protection Security 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. Product Selection and Installation

Reference	Security Control Requirement
10.1.1.	When reviewing Anti-Malware software and Anti-Malware Content Inspection devices / services for procurement and deployment, Suppliers MUST demonstrate a clear awareness of the other Anti-Malware technologies that provide similar functionality throughout the systems architecture. The purpose of this awareness is to avoid the duplication of identical scanning engines throughout the security control points in the infrastructure and therefore decrease any unnecessary performance penalties.*
10.1.2.	If open source Anti-Malware software is chosen, clear SLA's and escalation processes MUST be defined in the case of software failure IE) signature updates that may cause large scale false positives that may adversely affect legitimate business software. (Note: Commercially based Anti-Malware will have well-defined SLA's as part of the procurement and commercial contract. Open source Anti-Malware software will not necessarily have these in place by default).

10.2. User Awareness Training

Reference	Security Control Requirement
10.2.1.	All Supplier staff, including contractors MUST complete Security Awareness training as part of their induction training. This should be completed as early as possible to the start date of their employment or contract. The ideal timeline would be within the first week of employment or contract commencement.
10.2.2.	Long term staff MUST be appropriately informed of, and complete any new modules of Security Awareness training within one month of release.
10.2.3.	Long term staff MUST also complete Security Awareness training at least annually.
10.2.4.	Historical records of training engagement and successful completion MUST be recorded and auditable for each individual member of staff, including contractors.
10.2.5.	Privileged Users who manage the Anti-Malware software, hardware, processes and services MUST be able to demonstrate the appropriate level of training for the products, processes and services that they manage.

10.3. Operating System

Reference	Security Control Requirement
10.3.1.	The principle of least privilege MUST be applied to ensure that end users have only the required access to perform their business tasks, and have no access to modify any system parameters on the Operating System other than for HID (Human Interface Devices) for their personal ergonomic requirements. This includes, but is not limited to restricting access to system logs, driver settings, time settings, host based firewalls, process browsers, and service management settings.
10.3.2.	Operating Systems MUST be running versions that are still under active vendor support and must be patched under time sensitive operating procedures according to SS-033 Patching Security Standard
10.3.3.	If an Operating System is in use that is no longer under vendor support, a clear migration plan MUST exist and be well-defined and monitored. Furthermore, other mitigations to ensure clear restrictions to Internet based traffic and an adequate level of inline Content Inspection MUST be in effect. (This is because end point Anti-Malware software on these systems will not provide the required level of protection).

10.4. Anti-malware software

Reference	Security Control Requirement
10.4.1.	Standard business users MUST not have any access to modify or disable the scanning parameters of the Anti-Malware software. This includes preventing user access to disable Anti-Malware capabilities in the BIOS.
10.4.2.	Access to the Anti-Malware software console MUST be protected to avoid any tampering by non-privileged users.
10.4.3.	Any privileged access exercised to modify Anti-Malware software scanning parameters MUST be fully logged and auditable.

10.5. Browser

Reference	Security Control Requirement
10.5.1.	Standard business users MUST NOT have any access to modify any of the browser based settings such as, but not limited to, privacy settings, proxy settings, Active X, and Java based settings.
10.5.2.	Users MUST NOT have the ability to install or modify any browser based plugins.
10.5.3.	The only browser based parameters that a standard business user MUST have access to, is for the accommodation of ergonomic requirements such as modifying the zoom feature for vision assistance.
10.5.4.	Configuration on the browser MUST severely limit non-essential browsing features such as web based popups and iFrames that do not meet standard size requirements.
10.5.5.	Users MUST: i) only use corporately approved browsers, ii) NOT have the ability to install any non-approved browsers This is a specific clause to item 10.9.1.

10.6. Removable Storage

Reference	Security Control Requirement
10.6.1.	Access to USB interfaces for standard business users on end user devices such as, but not limited to Thin Clients, and Laptops MUST be restricted to HID's and authentication tokens only.
10.6.2.	If an exception is granted for the business use of removable media the auto-run feature MUST be disabled and an on demand Anti-Malware software scan MUST be completed and successfully passed prior to the data being persisted on department systems
10.6.3.	If removable media is to be introduced by exception, the device SHOULD be first introduced to an air gapped machine and the Anti-Malware software scan successfully completed prior to the introduction to the main department corporate network.

10.7. VPN

Reference	Security Control Requirement
10.7.1.	Any VPN Concentrators aggregating remote workers access to Authority systems MUST perform a posture check of the devices attempting remote connectivity. This MUST include checks on patching levels, Anti-Malware software signature levels Anti-Malware software service status and confirmation that the device is appropriately authorised to access the network
10.7.2.	If remote workers end point devices do not meet posture check requirements of the VPN concentrator, they MUST have a clear facility in a quarantine/ staging area to rectify patching levels, Anti-Malware software signature levels and service status in order to reattempt successful connection.

Reference	Security Control Requirement
10.7.3.	Remote workers end point devices MUST NOT have the ability to split tunnel during VPN connectivity and MUST NOT be able to browse the Internet except exclusively via the VPN subject to all Authority outbound Internet browsing security controls.

10.8. Instant Messaging

Reference	Security Control Requirement
10.8.1.	If communicating with approved federated third parties (including Suppliers) via an Instant Messaging channel, file transfer MUST have an on demand scan Anti-Malware software scan enabled.

10.9. General Software Controls

Reference	Security Control Requirement
10.9.1.	Standard business users MUST NOT have the ability to install unauthorised software on any Authority end points
10.9.2.	End point controls MUST consider the use of application whitelisting technologies to help mitigate the deployment of unauthorised software and malware execution.
10.9.3.	All approved software MUST be subject to the same patching standards as the underlying Operating System patching standards.
10.9.4.	Any software found to have bypassed any control mechanisms for installation MUST be subject to a formal review and uninstallation if deemed necessary.

10.10. File Transfer Controls

Reference	Security Control Requirement
10.10.1.	File Transfers MUST be subject to at least one layer of content inspection by Anti-Malware software prior to the data being resident/ persistent on department systems
10.10.2.	File Transfers with approved third parties (including suppliers) MUST be subject to at least two layers of content inspection. Where decryption is possible, this MUST be done firstly by a Security Boundary service, such as a Next Generation Firewall, Web Application Firewall, or Proxy Server, and secondly by a real time scan using the Anti-Malware software on the target end point.
10.10.3.	File Transfers MUST only be executed with approved third parties (including suppliers) with active contracts/ commercial and inter-departmental agreements.

10.11. Threat Intelligence

Reference	Security Control Requirement
10.11.1.	Anti-Malware threat intelligence feeds MUST be regularly collected and reviewed from known, trusted third parties (including Suppliers). These MUST be digested by a dedicated team and distributed to relevant stakeholders for consumption.

10.12. Anti-Malware Software

Reference	Security Control Requirement
10.12.1.	Anti-Malware software MUST be installed, verified and actively running on the end points indicated on the Statement of Applicability.
10.12.2.	Anti-Malware software MUST have on-access (real-time) scanning enabled by default for general web browsing, file and folder download and upload via email attachments.
10.12.3.	Anti-Malware software MUST have as a minimum frequency interval a weekly on-demand scan completed of the entire file and folder structure. This MUST include a scan of the start-up files, boot records and memory.
10.12.4.	If Anti-Malware software has any on-access (real-time) and/or on-demand scan exceptions required, then these MUST be auditable, well-defined and justified with a clear operational requirement. Vendor documentation outlining requirements for Anti-Malware software scan exceptions MUST be indexed and archived for easy reference for operational and auditing contexts.
10.12.5.	Anti-Malware software MUST be configured to log any malware detection to a centralised repository that is actively reviewed.
10.12.6.	Anti-Malware software MUST be configured to disinfect, delete, quarantine or encrypt malware upon detection. Encryption of the malware MUST be reversible in the case of false positive detection (IE: an XOR of the file is generally sufficient).
10.12.7.	Anti-Malware software MUST be configured to automatically update signature or definition files in near real-time from a centralised internal source and from the Internet directly as a fall-back mechanism.
10.12.8.	Anti-Malware software MUST endeavour to be running the latest version of the underlying detection engine as well as the signature or definition files.
10.12.9.	Anti-Malware software procurement and deployment processes MUST consider the use of heuristic scanning methods as well as traditional signature or definition based scanning.
10.12.10.	Anti-Malware software MUST be periodically verified for integrity. This verification check MUST be managed via a centralised console and adequately monitored. The meaning of integrity is that the service/ process associated with the software is running, the software remains tamper proof, the file and folder scanning exceptions are as expected, the efficacy of the detection engine is reviewed and the signature or definition files are being updated as expected.

Reference	Security Control Requirement
10.12.11.	Anti-Malware Software MUST have its resource management options appropriately configured to ensure that CPU, memory and hard disk usage are never exhausted during operation

10.13. Content Inspection and defence in depth

Reference	Security Control Requirement
10.13.1.	Any standard users MUST be subject to a whitelisting and blacklisting URL reputation service for inspection for outbound Internet Browsing.
10.13.2.	URL blacklisting reputational feeds for Internet Browsing MUST be updated in as near to real-time as operationally feasible on the Content Inspection boundary devices such as Next Generation Firewalls, Proxy Servers, or Web Content Filtering gateways referenced by the Internet Browsing boundary routers.
10.13.3.	URL blacklisting and Content Inspection for Internet Browsing MUST work in a blocking state for known malicious sites. In other words, URL blacklisting Content Inspection MUST NOT work in an “Inspect only” state for known malicious sites.
10.13.4.	Email Content Inspection MUST have at minimum two layers of Anti-Malware scan performed prior to persisting attachments. This will take the form of Email Content Inspection on the relevant Mail Gateway and also on the desktop, server or mobile endpoints Anti-Malware software inspection engine.
10.13.5.	Intrusion Detection systems MUST be configured and maintained with the latest signatures and rule sets to help detect malware intrusion attempts and also Indicators of Compromise.
10.13.6.	Intrusion Prevention systems MUST be configured and maintained with the latest signatures and rule sets to help mitigate malware intrusion attempts and also block outbound command-and-control traffic noted also as Indicators of Compromise. If configured they MUST be in a block rather than inspect only mode after the initial installation and learning phases are completed.
10.13.7.	Any Content Inspection technology capable of operating in an active blocking mode, (as opposed to only inspecting content), MUST have a clear and tested set of procedures to overcome any false positives that may affect legitimate business process as part of an update that may inadvertently affect the Content Inspection engines, signatures, rules, blacklisting, reputational services or definition updates.
10.13.8.	Consideration MUST be given to complementary end point agent based Defence in Depth technologies, such as Next Generation Anti-Malware Software (in addition to traditional Anti-Malware Software), host-based firewalls/ intrusion prevention software and micro-virtualisation technologies.
10.13.9.	Consideration MUST be given to complementary agentless Defence in Depth technologies such as Isolation and Rendering technologies, Sandboxing technologies and Data Science based solutions to help identify Indicators of Compromise.

10.14. Log Configuration and Collection

Reference	Security Control Requirement
10.14.1.	Anti-Malware Software on every operational endpoint noted in the Statement of Applicability MUST be configured to log any disinfection, deletion, quarantine or encryption actions in near real-time to a native centrally managed console for the Anti-Malware Software in use. Where near real-time logging is not possible, digest logging MUST be configured.
10.14.2.	The Anti-Malware Centralised Console MUST be configured to forward in near real-time or in a digested format logs aggregated from the clients it manages to a centralised SIEM system.
10.14.3.	Any of the technologies in use in the “Content Inspection and Defence in Depth” subsection MUST have its detection, inspection, blocking, quarantine, deletion, disinfection, traffic, and encryption logs (where applicable) configured to forward in near real-time or in a digested format to a centralised SIEM.
10.14.4.	Modifications to any element that affects the general operating parameters of any Anti-Malware technology noted in the “Detection Mechanisms” section including changes to logging facilities, administrative access, rule creation, and any content inspection updates MUST be tamper proof and logged either in near real-time or digested format to a centralised SIEM. This statement applies equally to system initiated changes to the general operating parameters such as signature or definition file updates and system administrator changes to general operating parameters such as file and folder exception modification, privilege access modifications and rule creation.
10.14.5.	Management of the centralised SIEM MUST NOT have any overlap for individual system administrators that manage ANY of the systems noted in the Detection Mechanisms section.

10.15. Log Review and analysis

Reference	Security Control Requirement
10.15.1.	Baseline Management Information of the Anti-Malware Software logs and the Defence in Depth system logs MUST be validated, reconciled and processed for monthly reporting. (This process MUST include the removal of any false positives that may have occurred during the reporting period so as not to overstate the incidence of malware detection, infection and action).

10.16. Malware Incidents Preparation and Real Time Controls

Reference	Security Control Requirement
10.16.1.	The incident response MUST contain well-defined procedures including escalation processes to adequately deal with a Malware risk event precipitation.
10.16.2.	The escalation process MUST contain a RACI matrix that is explicitly tied to individuals, their titles and respective well-defined action points during a Malware risk event precipitation.
10.16.3.	The escalation process MUST have qualitative and quantitative upper bounds defined to trigger the actual escalation process to the relevant parties indicated in the RACI matrix in point 10.16.2. Upper bounds can be defined to metrics such as, but not limited to: number of hosts affected, number of users affected, internal or external service interruption statistics, and the particular environment compromised
10.16.4.	Malware Incident Response MUST take into consideration accidental tip-off to malicious insiders as part of the well-defined procedures outlined in point 10.16.1 In other words, escalation MUST operate on a need-to-know basis, rather than be broadcast based.
10.16.5.	The Incident Response MUST have well-defined upper bounds to trigger the isolation and intentional service disruption in order to effectively contain, disinfect and remediate the Malware related incident. Point 10.16.2 implies that the decision to take this action MUST be tied to an individual/ individuals as indicated by the RACI.
10.16.6.	The Incident Response MUST record all actions taken as part of the specific incident response handling timeline. This is in accordance with the ACPO Good Practice Guide for Digital Evidence Principle 3. This will be crucial for any forensic, post mortem and lessons learnt work to be completed subsequently.
10.16.7.	For data and services provided in offshore locations, the Incident Response MUST have clear guidance to the laws, processes and procedures relating to Malware Incidents that may precipitate in these locations.

10.17. Malware Incidents Post Mortem

Reference	Security Control Requirement
10.17.1.	Subsequent to the containment of a Malware related incident and return to BAU the Incident Response MUST ensure that adequate forensic work is completed on a need-to-know basis to quantify the actual impact of the Malware infection. (Impact can be defined as the degradation of the Authority's Confidentiality, Integrity, Availability and Non-Repudiation relating to its data, systems and reputation).
10.17.2.	Subsequently following the containment of a Malware related incident and return to BAU, the Incident Response MUST ensure that an adequate post mortem is completed by those individuals implicitly noted in Point 10.16.2 and that a Lessons Learnt log be recorded and archived for future review and audit.
10.17.3.	The Incident Response, particularly relating to recovery from Malware risk event precipitation, MUST include well-defined procedures to restore data from secure backups.

11. Introduction

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. Definition of Terms

Term	Definition
MUST	Within this document the term MUST means mandatory; it is an absolute requirement and where cannot be met an exemption needs to be in place.

14. Glossary

ACPO	Association of Chief Police Officers
BAU	Business As Usual
Authority	The Authority refers to the Department for Work and Pensions
HID	Human Interface Devices
IoC	Indicators of Compromise
IDS	Intrusion Detection System
iFrames	Inline Frames
IPS	Intrusion Prevention System
RACI	Responsible, Accountable, Consulted and Informed
SAM GB	Software and Asset Management Governance Board
SIEM	Security Information Event Management
SLA	Service Level Agreement
SUPPLIER	Is inclusive of Contractor, their employees or any sub-contractors used
USB	Universal Serial Bus
VPN	Virtual Private Network