Anti-Malware Standard

Version No	**3.0**
Document Type	Standard
Parent Document	Group Information and Cyber Security Policy
Parent Framework	Information & Cyber Security RTF
Document Approver Name	Jamie Cowan
Document Approver Job Title	Head, ICS Risk Framework & Governance
Document Owner Name	Ibrahim Gathungu
Document Owner Job Title	Director, ICS Standards
Document Contact Name	Katarzyna Wencka
Document Contact Job Title	Director, ICS Standards
Business Scope	All Businesses
Function Role	All Functions
Geography Scope	Global
Effective Date	29 November 2024
Approval Date	15 November 2024
Next Review Date	12 November 2027

Table of Contents

Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Katarzyna Wencka **[ICS Standards]**	Administrative and editorial changes: 1. Document template updated 2. ICS risks in section 1.1 updated in line with definition from ERMF 3. References in section 4 updated 4. Scope section and roles names updated in line with organisational changes Changes to ICS controls and requirements: 1. ICSCR-28Jun24-3 & ICSCR-26Jun24-1 considered in applicable controls 2. Removed controls: AM-001, AM-005, AM-006, AM-007 (covered in General Group requirements); AM-008b (consolidated in AM-008a and in section 7.3); AM-210 (consolidated in AM-200); AM-230 (covered in other ICS Standards) 3. Sections “Schedule for Scanning” and “Review	Material	Jamie Cowan Head, ICS Risk Framework & Governance	3.0	15-Nov-24	29-Nov-24

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	Frequency" (removed due to approach uplift and consolidation in the general control requirements)					

1 INTRODUCTION AND PURPOSE

A malware is a software or program (covertly inserted into another software or program) intended to destroy data, run destructive or intrusive programs that will have adverse impact on the confidentiality, integrity, or availability of an Information System or Technology Infrastructure. Common types of malware threats include viruses, ransomware, worms, malicious mobile code, trojan horses, rootkits, and spyware.

There are many potential sources of malicious software or firmware, including websites, social media, USB memory sticks, unsolicited CDs, electronic mail, malicious insiders and software or documents copied over networks such as the internal network or the internet.

A malware infection can be extremely costly to remove often resulting in the extensive use of resource and time required to remediate. This may be through the loss of data or access to Information System or Technology Infrastructure, Staff time to recover a system, or the delay or loss of important work. Additionally, malicious software can spread from an infected system and can lead to severe disruption to services and possible reputational damage or even fines. Malicious software is a constantly evolving threat and therefore, to protect the Information Systems or Technology Infrastructure from all forms of malware adequate controls have to be implemented.

This Information Security Standard will define the minimum set of requirements for implementation and management of anti-malware controls.

1.1 Risks

The Anti-Malware Standard mandates that adequate anti-malware controls are implemented to protect all the Information Assets, Information Systems and Technology Infrastructure that comprise the Group's network.

Failure to adopt and implement this Information Security Standard may expose the Group to Risk which may result in:

- Financial Loss by External Attacker and/or Trusted Insider,
- Disclosure of Sensitive Information by External Attacker and/or Trusted Insider,
- Disruption of Business Operations by External Attacker and/or Trusted Insider.

1.2 Scope

This Standard must be read, and controls deployed in conjunction with all other applicable ICS Standards.

***Note**: In the context of the Anti-Malware approach, ICS Standards for Secure Configuration Management, Vulnerability and Security Patch Management as well as Secure Asset Management are of a key importance for ensuring robust and effective ICS posture.*

The Standard is mandatory and applies to the Group businesses, functions and countries and regions except where explicitly prohibited by local Law or Regulation [assessed as per section 4.2 Reporting Non-Compliance].

***Note:** In case of any Country specific LRM requirement, the approach defined in ERMF (Chapter Eleven, Part B, section 4.2 "Country-level Host Regulatory Obligations") must be followed.*

The Standard covers all Group Information Assets which are processed and or used by the Group's Information System [wherever the term 'Systems' or 'Information System' is used in a control statement it refers to both Information System and Technology Infrastructure].

Where the Control Statements include Information Asset [IA] or Security Business Impact Assessment [S-BIA] ratings, they are applicable only to those rated Systems. All other Control Statements apply to all Systems regardless of ratings and hosted environments [Production or Non-Production unless stated otherwise].

***Note**: Target and factual scope of anti-malware protection deployment is defined in line with the Anti-Malware Strategy and approach.*

The Systems owned and or managed by the Third Parties [including Cloud Systems, Vendor Systems, Regulatory Systems, Self Service Terminal [SST] and similar], must additionally refer to the ICS Standards for Security in Interactions with Third Parties and Secure Configuration Management.

Please note, any Systems which are deemed as 'Standalone Machines' must be assessed using the Security – Business Impact Assessment [S-BIA] and controls must be applied accordingly in line with applicable ICS controls defined in ICS Standards.

2 ROLES & RESPONSIBILITIES

Information System Owner
A named individual accountable for the protection of owned Information System and for compliance with applicable Control Statements defined in this Standard.

Application / Technology Infrastructure Owner
A named individual accountable for the protection of owned Application / Technology Infrastructure and for compliance with applicable Control Statements defined in this Standard.

Process Owner [Anti-Malware] ("AM PO")
The AM PO is a named individual accountable for the adoption of the applicable ICS controls (of this Standard) to ensure effective, compliant and consistent delivery of the Anti-malware services and solutions in the Group.
The PO is responsible ensuring quality, timeliness, and adequacy of provided data, and management information to measure appropriate coverage and performance of control points (and subsequent measurement) against ICS Policy and Standards.
In addition to that, the PO is accountable for providing operational capability to support Information Asset/System/Technology Infrastructure Owners to deliver required objectives of the Standard.

Group Chief Information Security Office (Group CISO)
Group CISO is responsible for:

- Complying with the control areas of this Information Security Standard which are applicable to them,
- Notifying 2nd LoD OTCR TTO as and when they become aware of any regulations relevant to ICS issued by non-financial services regulatory authorities,
- Identifying the relevant Process Owners responsible for implementing the regulation in their processes and informing 2nd LoD OTCR TTO,
- Implementing ICS Policy and Standards,
- Ensuring mechanisms are in place to demonstrate that necessary documentation and audit trail concerning implementation of ICS LRM requirements are maintained,
- Completing attestations to relevant regulatory authorities to confirm compliance to the relevant regulations, and
- Tracking remediation of gaps identified from LRM attestations in line with remediation programmes.

As first line role holders, the Group CISO will additionally perform effectiveness reviews to monitor first line compliance with this Information Security Standard.

CISO Awareness team are responsible for ensuring that the Group is provisioned with the appropriate awareness and training tools (messaging, content, strategy and governance and training support).

CISO ICS Standards & Controls

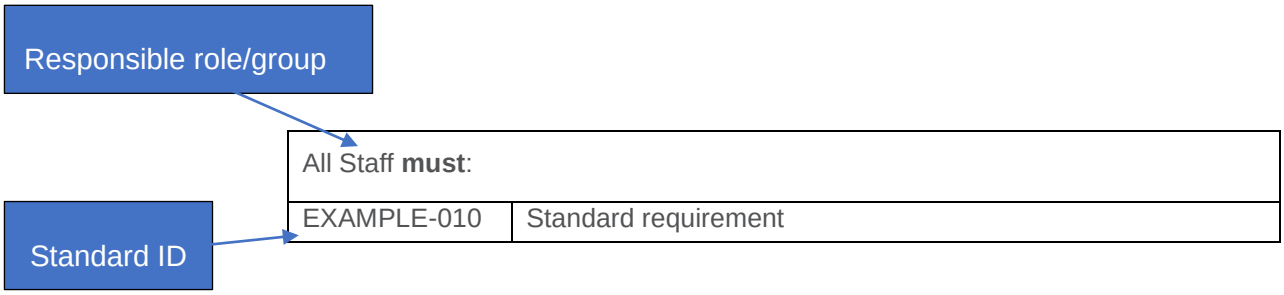
The CISO is the owner of this Information Security Standard and will ensure the document is updated to an agreed schedule.

***Note**: The Responsible role who **'must'** execute against this standard can do so either directly or by delegation. Where this is the case and a delegate exercises the control, the named role remains accountable.*

All roles & responsibilities including their corelations within ICS risk management activities are defined in Chapter Eleven, Part B, section 2 "Three LoD Responsibility and Governance Committee Oversight" of the Enterprise Risk Management Framework.

3 STANDARD REQUIREMENTS

This section outlines minimum mandatory requirements that apply to this Standard. The requirements are set out in the following format:



3.1 Control Area: Anti-Malware Operational Approach Definition and Maintenance

3.1.1 Process Definition and Governance

Process Owner [Anti-Malware] **must**:	
AM-002	Ensure that the operational approach to Anti-Malware [AM] includes: 1) documented definition of the Anti-Malware related activities, in line with: a) the applicable baseline requirements of the Standard; and b) identified (and prioritised) malware threat vectors. 2) defined and documented operational requirements and procedures for Information System/Technology Infrastructure/Application Owners (such as OS configuration guidelines, AM agent installation manual, etc.) essential to ensure predefined compliance level (with the Standard requirements). *[Note: The control statement requires the AM PO to document the operational approach, i.e., Process as well as to provide all supplementary documentation required for the Process to operate affectively. The final scope and approach to the AM activities is based on the applicable baseline requirements of the Standard and risk-based approach, i.e., may be changing as driven by threat landscape and profile of the Technology Assets in the Group.]* *[Reference: Secure Asset Management Standard]* *[Note: Process Owner [Anti-Malware] is the appointed CISO function.]* *[Objective:* *1) ICS Standards requirements are delivered and executed in a defined, consistent and effective manner to ensure that anticipated ICS risk is kept within the Group risk appetite.* *2) Approach, strategy and delivery of the Anti-Malware approach in the Group is formally defined and consistently deployed to ensure the potential ICS risk from malicious software is kept within the Group risk appetite.* *3) Scope of the Anti-Malware activities is defined based on the anticipated risk and malware threat landscape.]*

Process Owner [Anti-Malware] **must**:	
AM-003	Ensure that the operational approach covers essential AM components, such as: 1) AM awareness (see section 3.4 “Control Area: Awareness”), i.e. contribution (as demanded by respective Process Owner, to relevant ICS awareness and training programmes, in line with ICS Awareness and Training Standard, 2) AM vulnerability mitigation (see section 3.3 “Control Area: Vulnerability Mitigation”), 3) AM threat mitigation (see section 3.2 “Control Area: Anti-Malware Threat Mitigation”) and considers recommended AM baseline as outlined in the Standard. *[Reference: Section 7.1 “[AM-AP-010] Baseline AM recommendations for consideration in the AM Approach and Strategy”, ICS Awareness and Training Standard]]* *[Objective:* *1) The Group’s approach to AM protection considers comprehensive and complete mechanisms, including prevention, detection and correction.* *2) AM approach is tailored to the anticipated risk and technology present in the Group.]*
AM-004	Ensure that a threat-based approach to scoping and determining the AM strategy is applied based on: 1) identified and applicable malware risk/threat factors 2) monitored asset criticality (i.e., impact rating), 3) applicable baseline requirements of the Standard, AND define the relevant AM operational controls for respective Technology Asset categories/groups. *[Note: All Technology Assets are in scope of the AM Standard, however how the AM controls are deployed and what solutions are used (i.e., AM agent, hardening, etc.) it is a matter of the AM strategy as defined by AM PO.]* *[Objective:* *1) ICS Standards requirements are delivered and executed in a defined, consistent and effective manner to ensure that anticipated ICS risk is kept within the Group risk appetite.* *2) Approach, strategy and delivery of the Anti-Malware approach in the Group is formally defined and consistently deployed to ensure the potential ICS risk from malicious software is kept within the Group risk appetite.* *3) Scope of the Anti-Malware activities is defined based on the anticipated risk and malware threat landscape.]*

3.2 Control Area: Anti-Malware Threat Mitigation

3.2.1 Anti-Malware Solutions

Process Owner [Anti-Malware] **must**:	
AM-008a	Ensure that the AM approach is supported with relevant tools or software considering applicable requirements referenced in this standard. *[Reference: Security Logging and Monitoring Standard, Identity and Access Management Standard]* *[Reference: Section 7.1 "[AM-AP-010] Baseline AM recommendations for consideration in the AM Approach and Strategy"]* *[Note: the AM tooling coverage is technical compatibility with Group approved product and platforms.]* *[Objective:* *1) The AM Process and approach is, where required' supported with specialised software and solutions to mitigate the risk anticipated from malware infection to levels defined within the Group risk appetite.* *2) Resources critical for effective AM Process delivery: (1) are managed centrally to ensure consistency of the AM approach across the Group AND (2) where technically feasible and effective, are integrated with other Group solutions to improve the AM risk posture and increase effectiveness of the AM Process delivery.]*
AM-008c	Ensure the scope and configuration of AM solutions is predefined based on the identified malware threat profile for specific Asset categories and considers applicable baseline in referenced in this Standard. *[Reference: Section 7.1 "[AM-AP-010] Baseline AM recommendations for consideration in the AM Approach and Strategy"]* *[Objective:* *1) The AM Process and approach is, where required' supported with specialised software and solutions to mitigate the risk anticipated from malware infection to levels defined within the Group risk appetite.* *2) The scope, extent and type of AM protection is tailored to the Asset category, technology used and risk anticipated from malware infection].*

Information System Owner and/or Technology Infrastructure Owner **must**:	
AM-040	Ensure a Group approved anti-malware solution is implemented and run-on Information Systems and Technology Infrastructure as per scope, instructions and configuration guidelines defined by the AM Process Owner. *[Note: This includes Appliances and Group Services hosted in Cloud.* *Note: For Group approved (Employee Owned) mobile devices, the Staff must ensure relevant protection of the device, in line with applicable requirement of the Acceptable Use Standard.]* *[Reference: Acceptable Use Standard]* *[Objective:* *1) The AM Process and approach is, where required' supported with specialised software and solutions to mitigate the risk anticipated from malware infection to levels defined within the Group risk appetite.* *2) The scope, extent and type of AM protection is tailored to the Asset category, technology used and risk anticipated from malware infection].*

Information System Owner and/or Technology Infrastructure Owner **must**:	
AM-060	Report any issues with installed AM solution or its integrity in line with the AM PO requirements and guidelines. *[Objective:* *1) The AM Process and approach is, where required' supported with specialised software and solutions to mitigate the risk anticipated from malware infection to levels defined within the Group risk appetite.* *2) The scope, extent and type of AM protection is tailored to the Asset category, technology used and risk anticipated from malware infection].* *3) Any issue or exception with coverage and roll-out of applicable AM solutions must be promptly reported to ensure required mitigation or resolution is in place.*

3.2.2 Anti-Malware Response Capability

Process Owner [Anti-Malware] **must**:	
AM-135	When requested, contribute to relevant Group ICS incident management and response processes to ensure: 1) well documented and tested emergency process is in place to deal with a malware related Information security incident. 2) any acknowledged malware incident or suspicion of malware incident is reported and handled in line with applicable Group's Process(es) for ICS incident response and management (or relevant AM response capability). *[Note: The process can be defined/embedded within AM Process or existing Group's Process(es) for ICS incidents response and management.* *[Reference: ICS Security Incident Response and Management Standard]* *[Objective: Malware related events or incidents must be promptly and effectively handled to limit the impact of malware infections.]*
AM-150	Ensure that available AM related events and logs delivered to applicable Group Process for Security Logging and Monitoring. *[Note: the correlation, monitoring and analysis of the event can be either embedded within AM Process capabilities or existing Secure Logging and Monitoring Process(es).]* *[Reference: Section 7.1 "[AM-AP-010] Baseline AM recommendations for consideration in the AM Approach and Strategy"]* *[Reference: Secure Logging and Monitoring Standard]* *[Objective: Malware related events or incidents must be promptly and effectively handled to limit the impact of malware infections.]*

3.2.3 Anti-Malware & Defensive Architecture

Process Owner [Anti-Malware] **must**:	
AM-160	Ensure that applicable AM protection is defined and deployed (in line with the predefined AM Strategy) on Technology Assets to ensure effective malware threat prevention through IT architecture. *[Note: Applicable baseline requirements, as defined in section 7.1 "[AM-AP-010] Baseline AM recommendations for consideration in the AM Approach and Strategy" should be considered for AM countermeasures selection.]* *[Objective:* *1) The scope, extent and type of AM protection is tailored to the Asset category, technology used and risk anticipated from malware infection].* *2) Targeted AM solutions (such as dedicated tooling, architecture, or activities) are implemented and maintained to constitute a defensive architecture against most common malware infection or propagation vectors.]*

3.2.4 Malware Threat Prevention & Intelligence

Process Owner [Anti-Malware] **must**:	
AM-170	Use relevant and available Group Cyber Threat Intelligence (as defined by the Security Logging and Monitoring Standard) for scoping, selecting and deploying AM controls. *[Objective: The AM approach and strategy is continuously uplifted and enhanced in correspondence to applicable threats and ICS risk landscape.]* *[Reference: Security Logging and Monitoring Standard]*
AM-180	Define and communicate (to the Group appointed Security Architecture function) configuration or architecture guidelines, for technologies and products during onboarding, supporting effective malware threat prevention, in line with applicable baselines of the Standard. *[Reference: Section 7.1 "[AM-AP-010] Baseline AM recommendations for consideration in the AM Approach and Strategy"]* *[Reference: ICS Secure Configuration Management Standard – SCM-030]* *[Objective:* *1) Technology Products used by the Group support effective delivery of the AM strategy and via relevant configuration and architecture.* *2) The scope, extent and type of AM protection is tailored to the Asset category, technology used and risk anticipated from malware infection.]*
AM-190	Define and recommend additional malware threat prevention measures: 1) considering applicable factors of the AM baseline in this standard. 2) in line with malware threat profile identified for specific Asset categories. *[Reference: Section 7.1 "[AM-AP-010] Baseline AM recommendations for consideration in the AM Approach and Strategy"]* *[Objective: The scope, extent and type of AM protection is tailored to the Asset category, technology used and risk anticipated from malware infection].*

3.3 Control Area: Vulnerability Mitigation

Process Owner [Anti-Malware] **must**:	
AM-200	Deliver and maintain operational and configuration guidelines for AM technology and products used in the Bank (in scope of the AM approach and strategy) that: 1) consider baseline requirements of the Standard, 2) include (optional) enhanced controls (together with the guideline for their applicability), 3) are aligned with vendor specification and recommendations (where technically feasible), 4) are embedded in the standard technology build (if feasible), 5) include required configuration and compatibility list/issues, 6) are tested before communicated for deployment. *[Reference: Section 7.1 "[AM-AP-010] Baseline AM recommendations for consideration in the AM Approach and Strategy"]* *[Objective:* *1) Technology Products used by the Group support effective delivery of the AM strategy and via relevant configuration and architecture.* *2) The scope, extent and type of AM protection is tailored to the Asset category, technology used and risk anticipated from malware infection.]*

Information System Owner and/or Technology Infrastructure Owner and/or Application/Technology Product Owner **must**:	
AM-220	Ensure the required architecture, configuration, and operations (as shared by the AM Process Owner) are deployed and maintained effectively for owned Information System/ Technology Infrastructure/Application. *[Objective:* *1) Technology Products used by the Group support effective delivery of the AM strategy and via relevant configuration and architecture.* *2) The scope, extent and type of AM protection is tailored to the Asset category, technology used and risk anticipated from malware infection.]*

3.4 Control Area: Awareness

Process Owner [Anti-Malware] **must**:	
AM-240	Ensure that AM related content and guidelines for All Staff is available and fed into the Group Awareness & Training Process, as requested by respective Process Owner, in line with applicable requirements of the ICS Training and Awareness Standard. *[Note: The guidelines should be defined considering the baseline recommendations of the section 7.1 "[AM-AP-010] Baseline AM recommendations for consideration in the AM Approach and Strategy" and may be customized for specific operations or duties]* *[Objective: Effective AM protection must be supported by increasing and maintaining Staff awareness of malware related threats and infection vectors to mitigate the likelihood of malware incidents due to lack of Staff cyber hygiene.]* *[Reference: ICS Training and Awareness Standard]*

Process Owner [Anti-Malware] **must**:	
AM-250	Report, where required, identified training and awareness needs (in AM area) to respective Process Owner(s). *[Reference: Section 7.1 "[AM-AP-010] Baseline AM recommendations for consideration in the AM Approach and Strategy"]* *[Objective: Effective AM protection must be supported by increasing and maintaining Staff awareness of malware related threats and infection vectors to mitigate the likelihood of malware incidents due to lack of Staff cyber hygiene.]*

4 INFORMATION & SUPPORT

4.1 General Information and Support

For queries relating to this Security Standard please contact the ICS Standards team via: *ICSStandards*.

4.2 Reporting Non-Compliance

As a general guideline, any non-compliance against the Applications and underlying Technology Infrastructure in CMDB should follow the ICS Non-Compliance Register (ICS NCR) process. Further assessment of these non-compliance should follow the issue management process, i.e. iTrack for issues with remediation plan or ICS Dispensation when there is an explicit decision not to remediate the issue.

4.3 Breach of this Standard

- Failure to comply with this Standard may result in formal action under the Group Disciplinary Standard, that for serious breaches could include termination of employment.
- Any actual or suspected breaches must be reported immediately to your People Leader or to your Compliance representative from the Group.
- All breaches of this Standard must be reported to the Document Owner of the Standard.

5 GLOSSARY

The ICS Standards Glossary has been defined and is available via the *GovPoint* – see the *Technology Glossary* via the *GovPoint Glossary* reference.

6 REGULATORY / INDUSTRY REFERENCES

All Regulatory/Industry References are available via the *ICS Master Control List* document published on: *Control Framework Library*

7 APPENDIX

7.1 [AM-AP-010] Baseline AM recommendations for consideration in the AM Approach and Strategy[1]

Area	Recommended baseline
Threat Mitigation: ***Anti-Malware Software***	1) Installation & maintenance of AM software on pre-defined (as per AM Strategy) Technology Asset categories. 2) Enabling anti-malware and host-based IPS functionalities on applicable hosts. 3) Ensure that AM solution: a. is managed centrally so that policy enforcement and configuration is carried out centrally, including an automated malware definition refresh, b. enforces and actively monitors host compliance (for example: applies relevant schedule/frequency/approach for updates, scanning or verification; alerts if host-agent features or agent integrity is corrupted, c. enables remediation of issues identified by the AM tool (such as AM agent failures, signature accuracy, etc.), d. Provides relevant logging to support malware identification capabilities and where feasible and effective, is integrated with applicable Group solutions (such as SIEM, security monitoring tools, SCCM, e. Alerts if a malware is detected and sends all malware detection logs to a central console or to SIEM solution, f. Provides real-time monitoring of host activities to detect and contain malware events, g. Examines files before execution, h. Cures/block/deletes/disinfects/quarantines files or content to mitigate the likelihood of malware spreading (for both file and fileless malware), i. Is kept up to date (including newest malware and Indicator of Compromise definitions and provides relevant functionalities and updates to agents, j. Supports various methods of malware activity identification, such as heuristic scans and signature-based verification, detection of potentially malicious behaviour (such as registry change, logon credential dumps, lateral movement). 4) Diverse, if required, the AM solutions and tooling to ensure layered AM protection to decrease the risk of malware infection (for example – using different vendors or solutions to protect different Technology Asset categories).
Threat Mitigation: ***Malware Threat Prevention***	1) Implementation of IPS/IDS for hosts based on identified malware threat profile. 2) Implementation of firewalls solutions to support identification and blocking of malware related threat and infection vectors. 3) Use of approved applications list to limit the likelihood of malware infection and outspread as per applicable controls of Secure Asset Management and Secure Configuration Management Standards. 4) Enhanced email protection, such as: prohibiting or blocking sending or receiving specific types of files or content (such as executables, binaries, shared libraries, URLs or scripts) to limit the likelihood of malware infection; analysing email messages for the known/potential malware infection vectors/patterns, etc. 5) Recommending required approach and scope for scanning and filtering files entering Group network.

[1] The table presents the industry best practises used to prevent or mitigate malware threats. The recommended baseline outlines the key factors that the AM Strategy and approach must consider and embed where/when relevant. It is acceptable that specific factors or recommendations are not implemented (or implemented on specific assets or partially implemented) if recognised as not relevant to the current IT environment or malware threat exposure.

Area	Recommended baseline
Threat Mitigation: ***Defensive Architecture:***	1) BIOS/UEFI protection: define the controls for ensuring configuration integrity to countermeasure malware threats using BIOS/UEFI as infection vector. 2) Browser isolation: can be used to ensure the malware infection likelihood or impact is limited with separated web browsers for corporate and non-corporate content browsing. 3) Sandboxing: for suspicious files and programs inspection in control environment to contain the malware infection and outbreak. 4) Virtualization: deployed to segregate applications or other software component on host with elevated malware risk profile.
Threat Mitigation: ***AM Architecture:***	1) Ensure that AM solution or protection (for example through dedicated hardening, content blocking or network configuration) is deployed on Technology Assets with elevated malware risk profile (based on risk assessment), such as: a. Network perimeter, b. Email exchange servers, c. End-user infrastructure, d. File shares and file sharing solutions.
Threat Mitigation: **AM Response Capability**	1) Malware related events should be captured and analysed to: a. Support the malware identification and containment capabilities, b. Proactively monitory and identify malware related threats, c. Accelerate response to malware incidents and improve response capabilities. 2) A dedicated team or staff members should be prepared to support management and response of malware related incidents. 3) Data backup and restoration strategies should consider the restoration needs as a result of malware infection or outbreak.
Threat Mitigation: ***Threat Intelligence***	1) Relevant threat intelligence should be identified and analysed as a key input factor to be considered in the AM strategy and approach. 2) Threat intelligence to be used as a modelling factor for appropriate controls selection and application.
Vulnerability Mitigation: ***Host hardening***	1) Disabling automated execution of files with elevated malware threat profile. 2) Disabling unnecessary services or accounts. 3) Hardening of application components with elevated malware threat profile (such as web-browsers, email clients, word processors). 4) Disabling external media AutoRun and AutoPlay features. 5) Disabling the use of external disk drives on high-risk Assets. 6) Deployment of network access tool preventing unauthorised or non-compliant Technology Assets from granting access. 7) Removing or changing default/build in accounts and logon credentials.
Vulnerability Mitigation: ***Standard builds and baselines***	1) Required AM configuration should be, where required, embedded in the standard builds and configuration baselines for technology product, platforms, and Applications.

Area	Recommended baseline
Awareness	1) Define AM specific Staff guidelines for secure behaviour to outline AM best-practise and behaviour, such as: a. Using caution with links and email attachments, b. Avoiding downloading and installing unapproved software or programs, c. Handling corporate mobile devices in line with the Group procedures, d. Ensuring that owned corporate devices are up-to-date with relevant patches applies but following schedules updates and restarts, e. Limit the user or power or administrative accounts and do not use them when contacting regular host operations. 2) Define procedures for All Staff, IT Administrators or Information System/Technology Infrastructure Owners on how to respond to a malware event or incident. 3) Feed the AM related content into Group Awareness & Training Process.

Appendix A – Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISO Policy	Annual review includes: 1. Migrated existing standard to ERM standard template. 2. The existing Malware Standard document has been uplifted into this standard. 3. Consultation feedback, corrections incorporated	Material	Liz Banbury	1.0	23-Nov-19	23-Nov-19
CISO Policy	Annual Review – Alignment of Scope, Risks, Roles & Responsibilities with correct functions; Amended statements: Administrative, Editorial: AM-010-040, AM-060-080	Non-material	Liz Banbury, Global Head, ICS Policy and Risk.	1.1	08-Jun-21	01-Jul-21
CISRO ICS Policy	1. Document template updated (in line with the ERM template) 2. Risks section realigned with new ICS RTF 3. ICSCR-18Aug2021-1 – update of scanning schedule and approach 4. Standard approach uplifted to support more flexibility in adoption and	Material	Samantha Finan, Global Head, ICS Policy, Standards and Reporting	2.0	22-Jun-22	01-Jul-22

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	drive process-oriented delivery 5. Additional AM aspects included, such as response capability, awareness, secure configuration aspects, recommended AM baseline 6. New controls: AM-001 to 008, AM-135 to AM-260 7. Amended controls: AM-040, AM-060 8. Removed controls: AM-020, AM030, AM-050, AM-070 to 130 9. Non-inclusive terminology replacement (ICSCR-3Mar2022-1)					
CISRO ICS Policy	Administrative and editorial changes: 1. Document template updated in line with the Template for Group Standards, v5.6 2. The Standard name updated from 'Group Information and Cyber Security Standard: Anti-Malware' to 'ICS Anti Malware Standard' 3. AM-260 (All Staff relevant) removed in line with the ICSCR-	Non-material	Paul Hoare Head, ICS Policy and Best Practice	2.1	28-Sep-23	10-Oct-23

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	18Feb2022-1 (introduction of the AUS)					
Katarzyna Wencka **[ICS Standards]**	Administrative and editorial changes: 1. Document template updated 2. ICS risks in section 1.1 updated in line with definition from ERMF 3. References in section 4 updated 4. Scope section and roles names updated in line with organisational changes Changes to ICS controls and requirements: 1. ICSCR-28Jun24-3 & ICSCR-26Jun24-1 considered in applicable controls 2. Removed controls: AM-001, AM-005, AM-006, AM-007 (covered in General Group requirements); AM-008b (consolidated in AM-008a and in section 7.3); AM-210 (consolidated in AM-200); AM-230 (covered in other ICS Standards) 3. Sections "Schedule for Scanning" and	Material	Jamie Cowan Head, ICS Risk Framework & Governance	3.0	15-Nov-24	29-Nov-24

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	"Review Frequency" (removed due to approach uplift and consolidation in the general control requirements)					