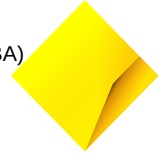
Group Information Security (IS) Protection from Malware Standard

Table of Contents



Purpose and scope

Purpose

The Group Information Security (IS) Protection from Malware Standard (Standard) supports the Group Information Security Policy.

The Group has an obligation to keep information secure. Software and information processing facilities are vulnerable to the introduction of malware, such as computer viruses, network worms, Trojan horses, malware developed by Advanced Persistent Threats, ransomware, man-in-the-browser and logic bombs. The Standard is intended to minimise the risk of the Group's Systems and data being compromised by computer viruses, worms, and other malicious code.

Scope

This Standard applies to:

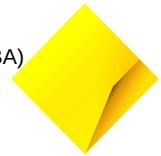
- The Group, its Directors, Employees, Contractors and Secondees;
- End-user laptops, workstations and Virtual Desktop Infrastructure (VDI);
- Servers;
- Cloud Workloads; and
- Internal and external parties providing services to the Group to the extent permissible within their legal and contractual obligations.

In instances where a Group entity is governed by a more stringent regulation or requirement, the more stringent requirement will apply.

Group Information Security Statements

This Standard builds upon requirements in external standards and regulatory frameworks listed under the External sources of obligations section, and statements in the Group Information Security Policy, specifically:

SEC-03	Service Providers must demonstrate an equivalent level of control to the Group Information Security Policy relevant to the Service they provide.
ORG-01	BUs, SUs, and Subsidiaries are accountable for information security within their Systems and Services.
ORG-03	Security roles and responsibilities must be clearly defined for each System or Service including Third Party stakeholders such as Suppliers and partners.
ORG-04	Processes for the On-boarding of external parties and Service Providers must ensure security requirements are met and understood.
ACC-11	Authentication processes must be resilient against foreseeable attacks.



OPS-01	Systems and Services must be built and maintained to a defined Secure State.
OPS-03	Systems and Services must be periodically assessed for vulnerabilities, secure configuration, and unauthorised changes.
OPS-09	Systems and Services must be protected from malicious code and software.
OPS-13	Security logs must be monitored to detect malicious or unauthorised activity.
DEV-01	Security requirements must be included in the development of new information Systems or enhancements to existing Systems.
DEV-02	Applications must prevent the abuse, manipulation, or unauthorised disclosure of information.
ISIM-03	Information Security Incidents must be managed through established processes with defined responsibilities.

Controls against malware

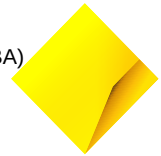
General

1. Malware detection and removal is supported by anti-malware controls. Malware protections must include where possible multiple security capabilities to create an effective defence in depth strategy.
2. Malware protection activities must include:
    - Monitoring external threat intelligence sources (e.g. government agencies, security Third Parties and specialist threat intelligence organisations) to identify new malware threats;
    - Informing external parties of the organisation's malware protection requirements; and
    - Implementing emergency procedures for dealing with malware-related incidents (e.g. sharing detected malware with malware protection software Service Provider to create a signature that can be widely distributed).
3. Endpoint protection, detection and response software with signature and non-signature based detection and protection mechanisms must be deployed and kept current on compatible Systems.
4. Where Endpoint protection, detection and response capabilities cannot be deployed, compensating controls and safeguards must be used to limit the risk of potential infection and spread of malware within the environment.
5. Network Policy Enforcement Points (PEP) must be managed in line with the Group IS Network Security Standard. More details can also be found in a relevant Protection from Malware Requirements and Guidelines.

6. Application Control must be implemented to ensure that only authorised software can be executed.
7. Use of macros must be controlled (e.g. in Microsoft Office).
8. Operating Systems (OS) and applications (web browsers, Microsoft Office, PDF) must be configured to the Group IS Vulnerability and Secure Configuration Management Standard. Other applications (e.g. PowerShell scripts) must be configured to a relevant Protection from Malware Requirements and Guidelines.
9. Application features that are not essential must be removed or disabled.
10. Controls to prevent the execution of malicious code must consider content and applications running within containers.
11. Patches, updates or software vendor mitigations for security vulnerabilities must be kept up to date in line with the Group IS Vulnerability and Secure Configuration Standard.
12. Data originating from outside the Group must be scanned for malicious code by a Group approved malware detection/protection tool as per a relevant Protection from Malware Requirements and Guidelines.
13. The risk of downloading malware must be reduced by implementing appropriate controls, including but not limited to:
    - Restricting the sources from which code can be downloaded (e.g. block-listing forbidden sites, USB);
    - Limiting the downloading of specific types of code and file types e.g. sourced from the internet or email;
    - Allowing only trusted code or file types from a known source to be downloaded; and
    - Running code in a protected environment e.g. sandbox, approved Standard Operating Environments (SOEs) with security tools.
14. Users of Group Systems must complete mandatory information security awareness training.

Logging requirements

15. The security logging capability of anti-malware detection tools deployed must be configured to log relevant security related events. Security logs must be sufficient to:
    - Detect changes to the configuration of Anti-malware Software or supporting controls;
    - Track the activity of the malware detected;
    - Identify events of interest that describe the malicious activity; and
    - Provide a chronology of the events that took place.
16. Security logs of anti-malware detection tools must be captured and reviewed on a regular basis or on-boarded to a real-time monitoring Service with access controls as per the Group IS Identity and Access Management Standard.



17. Malware related events must be centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned by an appropriate cyber security response team when cyber security events are detected.

18. Unauthorised modification of malware protection capabilities must be logged, and a security incident must be generated if required.

Reviewing Anti-malware Software

19. Systems with Anti-malware Software installed must be regularly reviewed to ensure that:
    - Malware Protection Software has not been disabled;
    - The configuration of Malware Protection Software is correct; and
    - Updates are applied correctly within defined timescales.

Endpoint protection, detection and response software

20. Group Systems managed by Third Party Service Providers (cloud Service Providers, managed Service Providers, etc.) must use Anti-malware Software, or compensating controls.

21. Endpoint protection software must be configured to comply with Group minimum requirements, as outlined in a relevant Protection from Malware Requirements and Guidelines. Group Systems and End User Devices must be scheduled for scanning, using up to date versions and configurations, which can be found in a relevant Group guideline.

22. Real time scanning must be enabled to scan all files prior to permitting access to network traffic entering the corporate network (including email, files entering the network via file transfer, or files downloaded from public internet websites).

23. Host Based Firewall must be enabled and configured for inbound and outbound connections. Only approved and documented flows based on business requirements are permitted.

24. Endpoint Detection and Response (EDR) capability must be deployed and enabled to in-scope managed Systems.

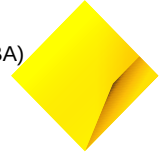
Identification and reporting a malware incident

General

25. Detection of malware incidents must be reported and managed (both manually and through automated tools).

26. Upon detection of suspicious activity, users must immediately report suspected cyber incidents by emailing iRespond@cba.com.au with the details of the suspicious activity. Service Providers must report suspicious activity as per requirements in their contract. If the contract contains no details on reporting suspicious activity, the Service Provider must immediately report suspected cyber incidents by emailing iRespond@cba.com.au with the details of the suspicious activity.

27. A relevant cyber security team with the assistance of relevant stakeholders is responsible for the detection, analysis, containment, eradication and recovery of malicious code present on the Group's



Systems (e.g. for CBA and Bankwest this is the Cyber Defence Operations (CDO) Cyber Attack Response Team (CART)).

28. Malware incidents must be managed in line with the Group IS Detection, Analysis, Response and Forensic Evidence Standard.
29. Incident closure must be managed in line with the Group IS Detection, Analysis, Response and Forensic Evidence Standard.

Risk management requirements

L1 Risk Type: Cyber Security

L2 Risk Type: "External Attack" or "Internal Attack or Action"

Risk definition: Disruption to Group systems, services or a compromise or loss of the data as a result of an external cyber-attack. Disruption to Group systems, services or a compromise or loss of the data as a result of internal attack or action by employee, ex-employee, contractor, subcontractor.

Key impacts associated with protection from malware include:

- Loss of data confidentiality;
- Loss of data integrity;
- Loss of System and data availability;
- Damage to the Group's reputation; and
- Financial loss.

Please refer to the Operational Risk and Compliance Risk Taxonomy on Policy.CBA for more information.

Risk appetite and monitoring

The Cybersecurity risk appetite indicators can be found in the Board approved Group Risk Appetite Statements and the Technology Risk Appetite Statement.

Mitigation and escalation

Issues and incidents related to cyber security risks must be escalated and managed in line with the requirements set out in the Group Issue Management Standard and the Group Incident Management Standard.

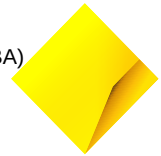
Key control objectives

Key control type

Protection from Malware execution

To ensure that Group information and endpoints are protected against malware by restricting the delivery and execution of malware and untrusted applications which would cause damage or access sensitive data.

Please refer to the Technology Controls Library for more information.



Accountabilities

Line 1 Risk (Line 1)

Line 1 Risk is responsible for:

- Performing periodic control assurance of in-scope controls, as per the Group Operational Risk Management Framework; and
- Recording and tracking of identified issues and actioning progress to the point of resolution.

Line 1 Risk needs to be consulted on:

- Appropriateness of control objectives to mitigate the risks ensuring alignment with the controls framework;
- Appropriateness of the control design to mitigate identified risks; and
- Guidance as to the implementation and maintenance of the control.

Line 2 Risk (Line 2)

Line 2 Risk is responsible for:

- Providing independent advice and assurance over alignment of the Standard with industry standards, compliance obligations and the Group Risk Management Approach (RMA); and
- Providing independent advice and assurance over the on-going governance and enforcement of the Standard.

Group Audit & Assurance (Line 3)

Providing independent assurance that the Group's risk management, governance and internal control processes are operating effectively, as per the approved audit plan.

Cyber Defence Operations (CDO)

Cyber Defence Operations is responsible for:

- Implementing procedures for dealing with malware-related incidents; and
- The detection, analysis, containment, eradication and recovery of malicious code present on the Group's Systems.

Breach of Standard

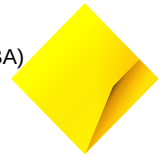
Consequences

Failure to follow this Standard may amount to a breach of the Group Information Security Policy.

A request for an Exception to the requirements of this Standard must be reported and recorded via a Group approved compliance management process (e.g. the Policy and Compliance Tool (PACT)).

Escalation

Potential or realised breaches of obligations outlined in this Standard must be escalated according to the Group Incident Management Standard.



Definitions

	In this Standard, defined terms are capitalised. Those terms have the meaning given to them below or, if not defined below, in the Group Glossary or the Group Information Security Policy.
Advanced Persistent Threat	An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organisations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organisation; or positioning itself to carry out these objectives in the future.
Anti-malware Software	Software that provides a defence mechanism to mitigate the risk of a computing device being infected with or affected by malware.
Application Control	A control designed to protect against unapproved and malicious programs executing on a computer. It warrants that only specifically authorised programs, software libraries (Dynamic Link Libraries (DLLs)), scripts, installers, and device drivers can be executed, while all others are prevented from executing. Restricting the running of applications on a System to only those that are specifically authorised is intended to increase protection against the execution and spread of malware.
Cloud Workloads	An application, Service, capability, or a specified amount of work that consumes cloud-based resources.
Endpoint	End-user devices, such as laptops, and workstations and Virtual Desktop Infrastructure (VDI), and servers.
Endpoint Detection and Response (EDR)	A proactive approach to threat and is effective to detect and prevent threats from further propagation.
End User Device	Laptops, desktops and VDI.
Host Based Firewall	Software used to secure the endpoint by enforcing rules on ingress and egress network traffic**.**
Malware Protection Software	Software that is used to prevent, detect and remove malware.
Service	A set of technology infrastructure shared by Systems and applications, such as a network, enterprise database or management infrastructure.
Service Provider	An organisation contracted by the Group to provide support, facilities or technical input to information processing.
System	A computer, or collection of computers and processing devices, that support a business process. An application would typically run on a System.
Trojan	Programs that appear to be benign but actually have hidden malicious purpose.

Standard governance

Approver	Group Security Lead Cyber
Exemption Authority	Chief Security Officer (via the PACT process)
Owner	Executive Manager Group Cyber Governance and Compliance
Support	InfoSecPolicy@cba.com.au
Review Cycle	24 months
Next Review Date	15 February 2027

Relevant documents

Related internal documents	Group Glossary Group Issue Management Procedure Group Incident Management Procedure Group Information Security Policy Group Operational Risk Management Framework Operational Risk & Compliance Risk Taxonomy Technology Controls Library Risk Management Approach (RMA) Group IS Vulnerability and Secure Configuration Management Standard Group Risk Appetite Statements Group IS Detection, Analysis, Response and Forensic Evidence Standard Group IS Network Security Standard Group IS Identity and Access Management Standard IS Protection from Malware Requirements and Guidelines
External sources of obligations	Australian Prudential Regulation Authority (APRA) Prudential Standard CPS234 – Information Security (Australia) International Organization for Standardization (ISO) 27001/27002 Information Security Management National Institute of Standards and Technology (NIST) Cybersecurity Framework Society for Worldwide Interbank Financial Telecommunication (SWIFT) Monetary Authority of Singapore (MAS)
Leveraged external documents	Australian Signals Directorate (Australian Cyber Security Centre) - Essential Eight Maturity Model (July 2021 Update)

Material revisions

Version	Approval Date	Effective Date	Details
1.0	16 July 2018	16 July 2018	Endorsed by ES RCC 2 May 2018. The Malicious Code Management Standard has been rewritten and renamed to Protection from Malware Standard. Other Malware Protection Techniques explained.

2.0	15 April 2020	15 October 2020	Noted/Approved at ES NFRC on 15 April 2020. Key changes include:
			New requirements:
			• Malware protection activities to include monitoring of threat intelligence, informing external parties of malware protection requirements of the Group, and implementation of emergency procedures for responding to malware-related incidents;
			• Controls must be implemented to reduce the risk of malware infection, such as:
			  ○ Ensuring only authorised applications can be executed;
			  ○ Restricting sources from which code can be downloaded;
			  ○ Running code in a protected environment;
			• Users of Group systems must complete training on basic malware infection techniques, receive current information on malware threats as appropriate for their role, and report suspected or actual malware where identified;
			• Regular reviews of servers, workstations and mobile devices to be performed.
			Amendment of existing requirements:
			• Where valid business or technical reasons result in non-compliance with the obligation to implement Anti-malware Software, such non-compliance must be formally documented and approved;
			• Detail on the configuration of Anti-malware Software expanded;
			• Detail on the components of Group systems and user devices that Anti-malware Software must be configured to scan expanded.

3.0	13 February 2023	15 February 2023	Endorsed by the Technology Policy Governance Committee on 2 February 2023. New requirements: • Inclusion of requirements set out in the Australian Cyber Security Centre Essential Eight Strategies, including blocking of macros, implementation of Application Control, application hardening, and Endpoint Detection and Response; • Clarification of the scope of the Standard; • Guidance added as to when Group security hardening guidelines should be consulted; • Patches must be kept current; and • Malware related events must be centrally logged. Amendment of existing requirements: • Change of CSC to the CDO; • Amendment and addition of several definitions for clarity; • Updated to the new Standard template as required by the GPF.
4.0	24 January 2025	31 January 2025	Endorsed by Group Security Lead Cyber on 24 January 2025. New requirements: • Unauthorised modification of malware protection capabilities must be logged, and a security incident must be generated if required. Amending of existing requirements: • Clarification of OS and application configuration requirements; • Examples added to clarify appropriate controls to reduce the risk of downloading malware; • Identification and reporting a malware incident section brought up to date with current processes and now points to requirements in the IS Detection, Analysis, Response and Forensic Evidence Standard instead of duplicating requirements from that Standard.