Web Filtering Standard

Version No	1.3
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 and Governance
Document Owner Name	Ibrahim Gathungu
Document Owner Job Title	Director, ICS Standards
Document Contact Name	Anna Kowal-Hughes
Document Contact Job Title	Assoc Dir, ICS Standards
Business Scope	All Businesses
Function Role	All Functions
Geography Scope	Global
Effective Date	16-Dec-24
Approval Date	4-Dec-24
Next Review Date	30-Jun-27

Standard Chartered Bank
www.sc.com

Table of Contents

Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Anna Kowal-Hughes **[ICS Standards]**	Editorial changes: 1. Document template updated in line with Template for Group Standards, V 7.0 2. Document references updated 3. Roles references updated in line with the new org structure	Non-material	Jamie Cowan Head ICS Risk Framework & Governance	1.3	04-Dec-24	16-Dec-24

1 INTRODUCTION AND PURPOSE

When Staff are granted unrestricted access to online domains there is the potential for the Group's network to be opened up to several Information and Cyber security threats. Examples of these threats are:

- Malware infection;
- Explicit or illegal content (as stated in the next paragraph);
- Loss of data (when user is tricked to provide sensitive information on forged or malicious site);
- Data leakage – intentional, i.e. sites that can be used by Staff to transfer Group's data/information (such as web emails, chats).

In addition, allowing unfettered access to domains could also have legal connotations where there could be restrictions and legal formalities associated with restricted content access.

Web Filtering is important as it both increases the level of protection associated with the Group's network by ensuring that only sites, and therefore content identified as 'safe' can be accessed and can indirectly improve overall productivity by minimizing Internet abuse.

This Information Security Standard will define the minimum set of requirements for implementation and management of Web Filtering controls.

Note: The *Web Categories Status Full List* document defines categories that must be restricted / blocked or may be permitted. This category list document is classified as "Internal" to the Group. For the latest list, please contact Secure Web Browsing Services team.

1.1 Risks

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 ICS Standards.

The Standard is mandatory and applies to the Group businesses, functions, 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 Systems [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].

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 Standards.

2 ROLES & RESPONSIBILITIES

Technology Infrastructure Owner

A named individual accountable for the protection of owned Technology Infrastructure and for compliance with applicable Control Statements.

Information System Owner

A named individual accountable for the protection of the owned Information System and compliance with applicable Control Statements.

Information Asset Owner

A named individual with accountability for the protection and permissible use of owned information Assets in Information Systems and Technology Infrastructure.

Business Function Head

The Business Function Head is responsible for identifying their Critical Information Systems and ensuring that Ownership is assigned to Information Systems prior to the System being deployed to Production.

Process Owner (PO)

POs (as defined by Enterprise Risk Management Framework) are Business or Function managers responsible for the end-to-end business or function processes as identified within the Group's Process Universe. They are responsible for identification and management of the end-to-end process as defined in the Group's Process Universe and associated risks, including ICS related activities as mandated by the Standard. The PO is responsible for ensuring the provision of quality, timely, and adequate data, and management information to measure appropriate coverage and performance of control points (and subsequent measurement) against ICS Policy and Standards.

All Staff

All Staff are required to read and comply with the requirements of this Security Standard which are directly relevant to them.

People Leaders

People Leaders must comply with the requirements and ensure that their Staff are made aware of their responsibilities in complying to this standard.

Group Chief Information Security Office (Group CISO)

The Group CISO is responsible for compliance with the requirements of this Information Security Standard which are applicable to them and for ensuring the Business Function or Country or Region that they are aligned to are aware of the requirements of this Standard and their obligations to be compliant with the requirements of this Standard. As first line role holders they must also have in place a model for validation of control and its effectiveness.

CISO ICS Standards & Controls

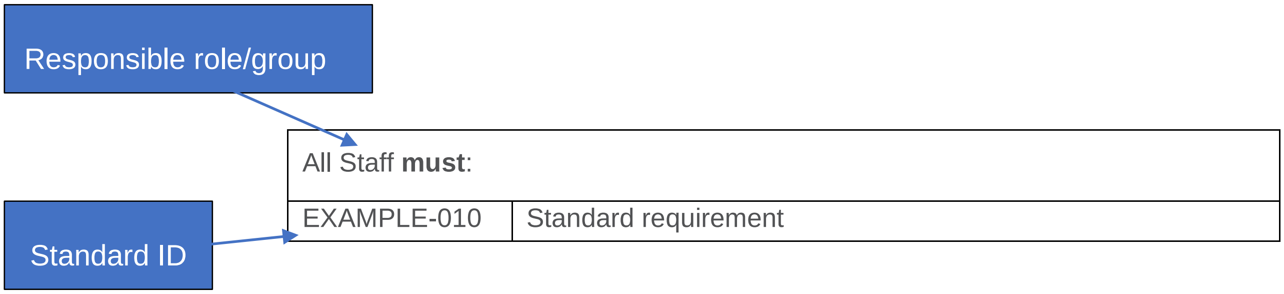
The CISO ICS Standards & Controls is the owner of this Information Security Standard and will ensure the document is updated to an agreed schedule.

***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:



All Staff **must**:	
EXAMPLE-010	Standard requirement

3.1 Control Area: Secure Web Filtering

Information System Owner **must**:	
WF-010	Ensure the Technology Infrastructure Owners and Process Owners implement Group approved web filtering solutions to protect Information Systems and Technology Infrastructure in.

Technology Infrastructure / Process Owner **must**:	
WF-020	Filter all web traffic traversing through the Group network to prevent exposure of Group Staff and Information Systems and Technology Infrastructure to inappropriate, offensive, illegal and dangerous web content.
WF-030	Ensure a dedicated web filtering solution must be used to control access to websites and file types based on categories and contents.
WF-040	Ensure Staff are prevented from accessing websites which are not yet categorised by the web-filtering solution.
WF-050	Ensure the solution can automatically identify new websites and add websites to categories. New websites must be assessed and added at least weekly but preferably daily.
WF-060	Ensure the web categories or websites and file types are reviewed, agreed and approved annually via the Group Non-Financial Risk Committee [GNFRC].
WF-070	Ensure access to web categories or websites, files types and content which pose a security risk to the Group must be restricted / blocked by default and exceptions must be formally agreed in line with the process rolled out by the GPO [Group Process Owner].
WF-080	Ensure the recertification of user's exception access to web categories or websites occurs once every 6 months. Note: The users must be notified a minimum of 4 weeks before expiry of exception access. Access must be revoked in case of no request from user on expiry date.
WF-090	Maintain an accurate and up to date catalogue of the allow-listed web categories or websites in the web filtering solution, including the justification and valid approval for allow-listing them.

Technology Infrastructure / Process Owner **must**:	
WF-100	Ensure the web filtering solution logs the websites accessed to allow Administrator(s) of the solution to produce audit reports on Staff internet access (including successful and unsuccessful access attempts). *Note: The logs must be implemented in line with Security Logging and Monitoring Standard.*

3.2 Control Area: Exception Access Management

3.2.1 Non-ICS Risk Categorised Requests (Individual)

Process Owner **must**:	
WF-130	Ensure a process is defined to handle requests received for restricted web categories or websites that fall under "Non-ICS Risk" type. *Note: The access will be provided for a period of 6 months requiring recertification before it can be extended*

3.2.2 ICS Risk Categorised requests (Individual)

Process Owner **must**:	
WF-140	Ensure a process is defined to handle requests received for restricted web categories or websites that fall under “ICS Risk” type.
WF-150	Ensure the process involves the relevant Business, Function or Regional CISO to review and approve these requests before access is granted. *Note: The access will be provided for the period of 6 months requiring recertification before it can be extended.*

Group CISO **must**:	
WF-160	Ensure the exception access requests to web categories or websites and file types are risk assessed and are approved or rejected based on the outcome of the assessment.

3.2.3 Request for Groups

Process Owner **must**:	
WF-170	Submit all requests for access by Groups to restricted categories to the GNFRC for review and approval via the Group CISO or delegate. The approved requests must be subsequently submitted to the STS Secure Web Browsing Service team for implementation. The requested access will be provided for a period of 6 months before requiring recertification. *Note: In case of urgent exception requests for Group Access, the request will be reviewed by Group CISO or delegate and process owner of STS Secure Web Browsing Service team. If the request seems valid, the access will be granted for a temporary period until the request is presented in the upcoming GNFRC for approval / rejection.*

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 Manager 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 A- Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISRO ICS Policy	Annual review includes: 1. Migrated existing standard to ERM standard template. 2. The existing Mobile Devices Standard document has been uplifted into this standard.		Liz Banbury [delegate of Group CISRO]	1.0	27-Mar-20	27 Mar-20

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	3. Consultation feedback, corrections incorporated					
CISRO ICS Policy	Annual Review – Alignment of Scope, Risks, Roles & Responsibilities with correct functions; Amended statements: **Administrative, Editorial**: WF-010-WF-040, WF-060, WF-090 **Administrative, Removal:** WF-110		Liz Banbury, Global Head, ICS Policy and Risk.	1.1	08-Jun 21	01-Jul 21
CISRO ICS Policy	WF-020 modification in line with ICSCR-21Jul2022-2 Document template uplift	Non-material	Paul Hoare Head, ICS Policy and Best Practice	1.2	08-Mar-23	22-Mar-23
Anna Kowal-Hughes **[ICs Standards]**	Editorial changes: 1. Document template updated in line with Template for Group Standards, V 7.0 2. Document references updated 3. Roles references updated in line with the new OTCR structure	Non-material	Jamie Cowan Head ICS Risk Framework & Governance	1.3	04-Dec-24	16-Dec-24