Network Security Management Standard

Version No	4.1
Document Type	Standard
Parent Document	Group Information and Cyber Security Policy
Parent Framework	Information and Cyber Security
Document Approver Name	Jamie Michael Cowan
Document Approver Job Title	Head, Frameworks, Reporting & Governance, T&O Risk & Control
Document Owner Name	Ibrahim Gathungu Munyori
Document Owner Job Title	Director, ICS Standards Formulation
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
Approval Date	15/11/2024
Effective Date	15/02/2025
Next Review Date	15/11/2027

Table of Contents

Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Anna Kowal-Hughes	Network Security Management Standard	Non-Material	Jamie Michael Cowan	4.1	15/11/2024	15/02/2025

The full version history is included at the end of the document.

1. INTRODUCTION AND PURPOSE

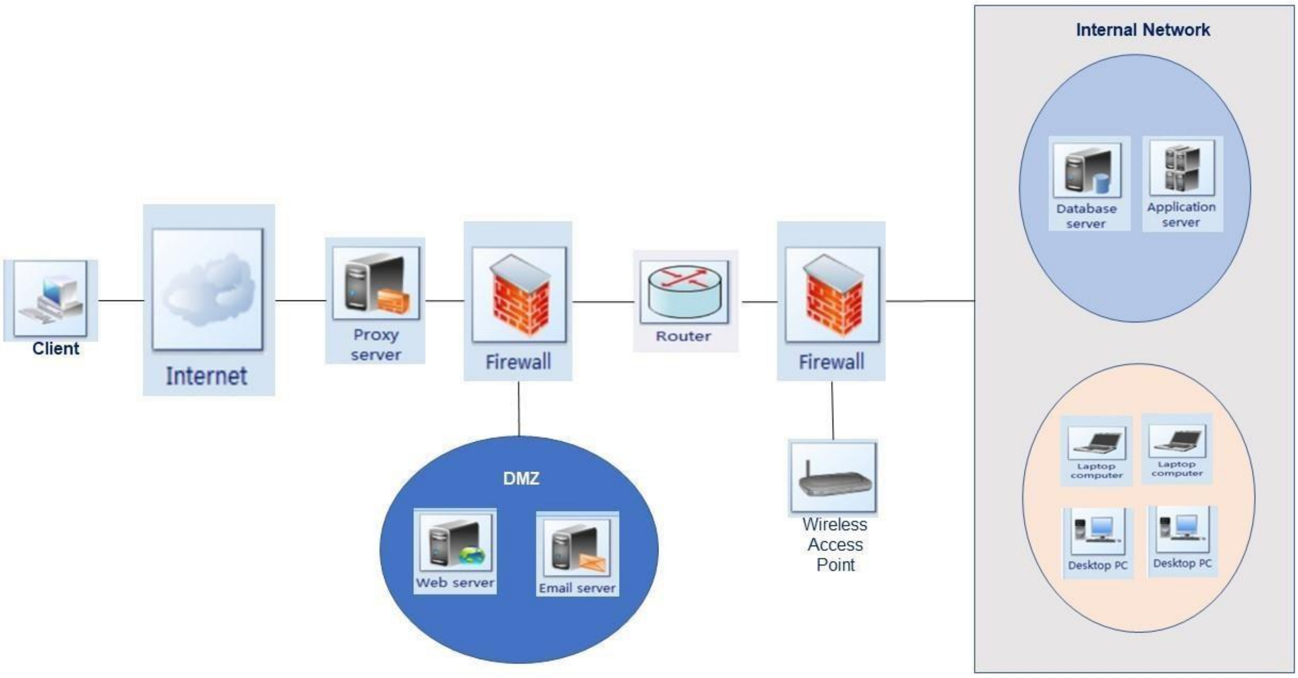
This Information and Cyber Security Standard defines the minimum set of requirements for establishing and maintaining secure network infrastructure.

The "Network" is formed by a collection of devices (for example: switches, routers, wireless access points, computers, servers, virtual machines) that are connected to each other physically or logically [For example: Wired Local Area Network [LAN], Wireless Local Area Network [WLAN], Wide Area Network [WAN], Leased Line, Internet] for sharing data or resources [For example: software, multi-function devices [MFD], data storage].

The Internal Network is a trusted domain of a single organization. It is a private network secured from external sources wherein connected devices to it are wholly managed and controlled by a single group or administrative domain.

The Perimeter Network is a secured network segment that acts as a boundary between a trusted internal and untrusted external network.

The types of networks are LAN, WLAN, Metropolitan Area Network [MAN], WAN, Virtual Private Network [VPN], Internet.



Note: The above diagram is an example illustration of perimeter network and not the actual representation of Group's network.

One of the key components of Network security is Network Segmentation. Network Segmentation is the isolation of traffic into distinct manageable pockets which reduces the amount of exposure should an attack be successful, and assets are compromised. Segmentation also allows for improved access management to the network.

The Group has a global footprint catering to the needs of our staff and customers. Therefore, it is important for the Group's business and functions to be interconnected and provide support to our customers in a seamless manner. This requires efficient management of the network to ensure that the confidentiality and integrity of the data transmitted is secured and that availability is not disrupted.

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 as per the applicable ICS Standards.

2. ROLES AND 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.

They are also responsible for ensuring that the Technology Infrastructure Owners, Process Owners correctly apply the controls as set out in this standard.

As first line role holders they must have in place a model for validation of control existence and effectiveness.

- Network Engineering team is responsible for a secure network design and architecture.
- Network Delivery team is responsible for implementation and maintenance of Information Security controls as part of their operational processes to ensure the Network operations are carried out in a secure manner.
- Voice and Video Engineering team is responsible for secure Voice and Video infrastructure design and architecture.
- Voice and Video Delivery team is responsible for implementation and maintenance of Information Security controls as part of their operational processes to ensure the operations are carried out in a secure manner. Network Security team is responsible for engaging with the Network Delivery teams to ensure the implementation and maintenance of network security controls as defined in this Information Security Standard.
- Cyber Defence Centre [CDC] is responsible for monitoring of alerts and anomalies generated by the Network Devices and applications and take the relevant course of action as per the define process to address them.
- ICS Application and Infrastructure Vulnerability Management [AIVM] team is responsible for checking the technical implementation of controls via periodic scans of the Network Devices and applications.

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

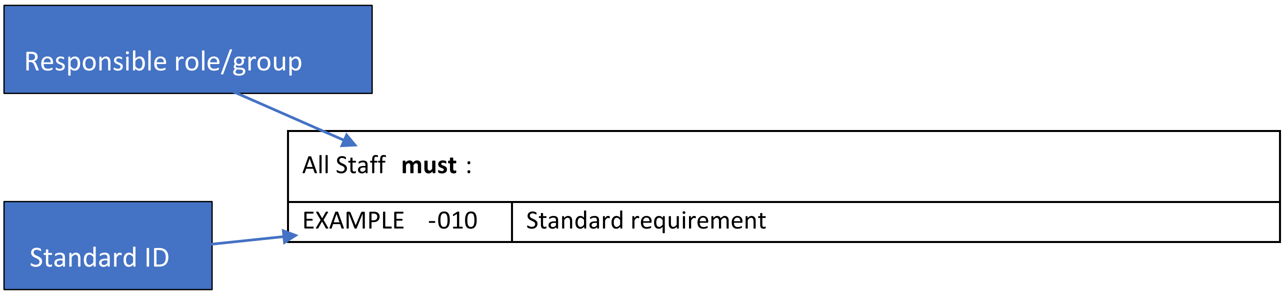
CISO ICS Standards & Controls

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 Security by Design

***Objective**: To ensure that the Group's networks are designed securely to protect the organization's Information Assets and Information processing facilities from internal and external threats.*

Information System Owner and/or Technology Infrastructure Owner **must**:	
NSM-010	Ensure the Group's Network Devices, Network Channels, Network Links and Network Segments are designed, and controls are applied: a) in accordance with the Enterprise Security Architecture; b) to incorporate Security Architecture Principles. (e.g. 'secure by design', 'defence in depth', 'secure by default', 'default deny', 'fail secure', 'secure in deployment' and 'usability and manageability').
NSM-020	Ensure up to date information about all Network Devices, Network Channels, Network Links and Network Segments (including assigned IP ranges) is maintained and recorded in the Group owned IT Asset Register. All assigned IP addresses of the IT Asset including management, data, and public IP addresses of the IT Asset, if any, must be documented in IT Asset Register including information: a) about which of them are active; b) in which Network Segment they exist. *[Reference: Information Classification Standard - INC-090, INC-100, INC-110, INC-130]*
NSM-030	Design and maintain Network Configuration Documentation that must include: a) Network Architecture Diagram, which shows of what components Network consist of; b) Network Channels and their configuration; c) Network Links and their configuration; d) Network Segments and their configuration; e) Services and their configuration; f) Protocols and their configuration; g) Ports and their configuration; h) Implemented Security Features and their configuration; i) Wireless Networks and their configuration;

Information System Owner and/or Technology Infrastructure Owner **must**:	
	j) Firewalls and their configuration; k) Routers and their configuration; l) Switches and their configuration; m) Proxies and Reverse Proxies and their configuration; n) Intrusion Detection Systems [IDS] / Intrusion Prevention Systems [IPS] and their configuration; o) rulesets for all types of Network Devices; p) Network Management Interfaces and their configuration; q) Load Balancers and their configuration.
NSM-035	Design and maintain Network Configuration Documentation that must include Network Architecture Diagram, which shows Payment Card Data flows and Payment Card Data Connections.

Process Owner **must**:	
NSM-060	Ensure that a network refresh strategy, for all Network IT Assets, is documented and reviewed annually to enable identification and remediation of obsolete or unsupported software and hardware (including firmware). *[Reference: NSM-020]*
NSM-061	Ensure domain name/address resolution is offered securely by: a) Defining a process for implementing protection mechanisms and methods of validating the integrity of DNS records, to prevent DNS attacks such as DNS hijack, spoofing, cache poisoning and tunnelling. b) Architecture and provisioning for name/address resolution service to ensure the systems that collectively provide name/address resolution service are fault-tolerant and define internal and external domain separation. c) Establishing centralised name record lifecycle management for both internal and external DNS records. *Reference: Secure Asset Management standard sets the governance and validation requirements for process effectiveness and compliance to all ICS Standards.*

3.2. Control Area Network Administration and Configuration

Objective*: To ensure that the Group's Network Devices and applications are configured to function as required, and to prevent unauthorized or incorrect updates.*

Information System Owner and/or Technology Infrastructure Owner **must**:	
NSM-090	Ensure that all Network Devices, Network Channels, Network Links and Network Segments are following unique/consistent naming convention that should indicate at least: Type and Location.
NSM-100	Ensure Network Channels, that is, Product Services and Acquisition Channel [PSAC], Business Partner Extranet Connectivity [BPEC] and Product Services Delivery Channel [PSDC] are implemented as per the intended purpose.
NSM-120	Identify types of network security incidents (including but not limited to: DoS, DDoS, APT, botnet attack, unauthorised device, unauthorised Wireless Access Point, unauthorised access, unauthorised security configuration change, anomaly in outbound or inbound network traffic, port scanning, unauthorised privilege escalation, endpoint attack, code and SQL injection, Cross-Site Scripting, man-in-the-middle attack (including but not limited to: network traffic eavesdropping, session hijacking, replay attack, IP spoofing) then document, test and maintain an Incident Response Plan for all of them.
NSM-130	Review annually all Network Devices, Network Channels, Network Links and Network Segments. For Network Devices/Channels/Links/Segments under PCI DSS requirement, perform the review every 6 months. The review includes: a) Rulesets - to remove redundant or unused rules (a hit counter may be used in order to identify those rules which are not utilised); b) Temporary Rulesets - to check if they are removed in line with set expiry dates; c) Identification if they are still required to ensure that redundant or unused ones are removed; d) Retaining evidence that the review is completed on time.
NSM-141	Ensure that firewall is be configured to: a) protect communication protocols that are prone to abuse (e.g. IPsec, HTTPS, SFTP, SSH, TLS, SIP, SMTP, MFT, DNS and UUCP); b) block network packets typically used to execute denial of service attacks (e.g. ICMP Echo, UDP and TCP Echo, Charge and Discard) *Exception: Use of ICMP Echo and Eco reply within internal network limited for troubleshooting purpose*; c) deny incoming traffic where the source address is known to have been spoofed (e.g. where the source address claims to be from the destination network); d) deny outgoing traffic where the source address is known to have been spoofed (e.g. where the source address does not reflect the network from which it originates); e) limit the disclosure of information about networks at the network level by using IP masquerading (i.e. Network Address Translation [NAT] or Port Address Translation [PAT] or zone file transfer restriction on Domain Name System [DNS]. *Exception: SNMP internal ping (echo)*
NSM-142	Ensure that any change to the Network Devices, Network Channels, Network Links and Network Segments configuration will generate an alert that will be monitored and validated to ensure that all changes are approved and follow Group's Change Management Process.

Information System Owner and/or Technology Infrastructure Owner **must**:	
NSM-150	Review weekly all IDS/IPS devices and IDS/IPS software to check if signatures have been updated timely and successfully.
NSM-170	Ensure secure communication protocols are enabled to secure end-to-end connectivity (For example: VPN) and transmission of Information classified as Confidential or Restricted or Information Asset rated 5 or 4 for Confidentiality. *Note: This is applicable to both Internal and External communication.* *[Reference: APPENDIX: Secure Communication Protocols and Cryptography Standard]*
NSM-180	Ensure a Group documented, and approved solution (employing jump host or broker type solution) is provided and used to perform administration and maintenance activities. *[Reference: Identity and Access Management Standard]*
NSM-200	Ensure access to the Internal Network via the Internet is restricted by routing network traffic through perimeter traffic inspection, filtering and authentication systems so that access to specific Information Systems (including network components) is only granted where there is a business need.
NSM-210	Ensure a Group documented, approved, and dedicated secure remote access solution is provided and used for all external access to the Internal Network. *[Reference: Identity and Access Management Standard]*
NSM-220	Identify unauthorized device connections and ensure these are assessed and managed accordingly.
NSM-230	Remove access to the Internal Network when it is no longer required
NSM-240	Manage IDs used by vendors to access, support, or maintain network components via remote access and ensure that access is only enabled for the time period required. All activities must be monitored.
NSM-241	Inform DNS Process Owner about: a) Specific name/address resolution requirements for the owned system (if any). b) Additional (business or regulatory context) which may require enhanced secure name/address resolution to adhere to PO guidance.

3.3. Control Area Network Segmentation

Objective*: The Group's business resources must be partitioned to protect the organization's Information Assets and Information Systems from internal and external threats. Essentially all Group Information Asset classes must be segmented into distinct enclaves and separated from the general computing environment.*

Information System Owner and/or Technology Infrastructure Owner **must**:	
NSM-300	Implement controls to segregate and restrict connectivity between networks containing Information Systems that are supporting defined business processes up to and including Line of Business and Sub Line of Business. *Note: A segment may contain multiple Information Systems of different S-BIA rating to minimise the need for cross segment traffic flows.* *Note: Production and Non-Production Environments should also be in separate segments.* *Note: By minimum all Information Systems impact rated as 5 need to be put in a network segment.*
NSM-320	Use a Reverse Proxy Firewall, placed in the perimeter network for all connections to the Internal Network via the Internet. The proxy firewall must be configured to forward the communication by establishing a new onward Transmission Control Protocol/Internet Protocol [TCP/IP] connection.
NSM-330	Implement a perimeter network between all Internal and External Networks to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. This must include that direct public access between the Internet and any Payment Card Data is prohibited.
NSM-340	Implement Firewalls in the following places: a) at each Internet Gateway; b) between each perimeter network and any Internal Network; c) between each perimeter network and the Internet; d) between each Network Segment; e) between WLAN networks and cardholder data environment. *Note: Exception for CorpNet and MCorpNet within point e), which is considered necessary for business purpose*

3.4. Control Area Telephony Conferencing and VoIP Management

Objective*: To ensure that the network communication devices are securely configured to prevent exploit by both external and internal threats.*

Information System Owner and/or Technology Infrastructure Owner **must**:	
NSM-371	For Voice, Video and Messaging communication implement firewalls where SIP link is terminated and implement perimeter network setup for deploying the session border controller to ensure no direct connection from External Network to Internal Network and Internal Network to External Network is established. *Note: This requirement does not apply to unified communications, softphone, or similar solutions where this is not possible.*

3.5. Control Area Network Traffic Protection

Objective*: To ensure the Group’s data in transit stay protected when transmitted internal and external to the network.*

Information System Owner and/or Technology Infrastructure Owner **must**:	
NSM-450	Use only Group authorized Network Management Interfaces to manage Technology Infrastructure. Such Management Interfaces must accept connection requests only from approved authorised sources.

3.5.1 Wireless access point

Information System Owner and/or Technology Infrastructure Owner **must**:	
NSM-470	Ensure that all WAPs (and identification of used devices) connected to the Group's Network (e.g. using Wi-Fi, satellite, microwave links, Bluetooth, infrared or ZigBee) are subject to an information risk assessment, approved and authorised with business justification.
NSM-471	Design and maintain Wireless Network Configuration Documentation that must include: a) placement and configuration of Wireless Access Points (hardware devices that provide interfaces between the wireless network and a wired network); b) methods of limiting access to authorised users (including section for guests or non-employees); c) use of encryption for protecting information in transit; d) maintaining an inventory of authorised Wireless Access Points, which includes a documented business justification for each access point; e) detection of rogue Wireless Access Points and unauthorised wireless devices (e.g. using automated discovery/mapping tools).
NSM-472	Ensure that Wireless Access Points are configured to: a) use the minimum power setting that delivers the range required; b) change default Service Set Identifier [SSID] in a way that does not reveal important information about the network; . c) enforce encryption of all communication; d) terminate associations after a configurable time period (as assessed suitable by risk assessment); e) not sharing WPA2-PSK keys across multiple endpoint devices [if WPA2 is used with pre-shared keys (WPA2-PSK)]; f) ensure that access to the Internal Network using WAP is limited to authorized users.

Information System Owner and/or Technology Infrastructure Owner **must**:	
NSM-473	Ensure that Guest Wireless Access Points are in addition configured to: a) prevent connectivity to Group's network (exclusion security gateway); b) prevent inter-client communication; c) permitting usage of VPN; d) forcing accepting Term of Use before allowing network connectivity; e) enforce Group web browsing policy. Exclusion: Encryption is not required for Guest Wireless Access Points.
NSM-500	Review all requests for new wireless networks and WAPs. *Note: Guest Wireless network or WAP must not connect to Group's internal network.*
NSM-501	Ensure that Wireless Intrusion Detection Systems [WIDS] or Wireless Intrusion Prevention Systems [WIPS] are used. *Note: Where technically feasible they should be used both at the same time.* *[Reference: NSM-515]*

3.5.2 Network Boundary Protection

Information System Owner and/or Technology Infrastructure Owner **must**:	
NSM-490	Perform weekly Information Systems and Technology Infrastructure discovery scans on Group internal network (including perimeter network) to identify unauthorised network devices (including Wireless Access Points and wireless devices) and active IPs.
NSM-510	Deploy Network Intrusion Detection Systems [NIDS] / Network Intrusion Prevention Systems [NIPS] tools on Information Systems and Technology Infrastructure: a) at each Internet Gateway; b) at each perimeter network boundary. Exception: If SDWAN is deployed on Internet Gateway then this control is not applicable. *[Reference: NSM-515]*
NSM-515	Ensure encrypted traffic has the visibility required for network traffic inspection for ICS monitoring, DLP and other ICS threat prevention & detection purposes. *Note: The visibility of the network traffic should be:* *a) decrypting the traffic;* *b) terminating encrypted connections/tunnels by the monitoring solution;* *c) on-host (local) TCP/IP stack monitoring;* *d) network traffic copy & decryption on dedicated monitoring device;* *e) other method ensuring required level of the traffic inspection.* *The method deployed must allow effective network monitoring as defined by requesting party.* *[Reference: NSM-501, NSM-510, NSM-520, NSM-540, DLP-140, DLP-150, AM-020, AM-110]*

3.5.3 Filtering and Routing Traffic

Information System Owner and/or Technology Infrastructure Owner **must**:	
NSM-520	Use Web Application Firewalls [WAF] to protect HTTP and HTTPS conversation during web access to Internet-facing Information Systems. *[Reference: NSM-515]*
NSM-540	Configure firewall rules to inspect and filter traffic by checking the following within packets with least access principles: a) Source and Destination Address b) Port Number. *[Reference: NSM-515]*
NSM-550	Configure external routers to: a) filter traffic through ACL's; b) deny all traffic unless explicitly permitted; c) use anti-spoofing filter; d) use stealth mode.
NSM-560	Configure and maintain all devices to block malicious traffic on entry and exit from the Group boundary by scanning for malicious code.

3.5.4 Preventing direct connections

Information System Owner and/or Technology Infrastructure Owner **must**:	
NSM-570	Configure all externally initiated VPN connections that cross the Internet Gateway to terminate at the perimeter network.

NSM-580	Protect all web connectivity between Group owned and managed Systems and the external network by enforcing the following:
	a) usage of Secure Protocols (including but not limited to: HTTPS, SFTP, SSH, TLS,
	SIP, SMTP, MFT);
	b) Uniform Resource Locator [URL] Filtering;
	c) authorization;
	d) Application Programming Interface [API] connectivity rules.

NSM-600	Review connections to the perimeter network every three months to check for any unauthorized access.

3.6. Control Area Network Segment Protection

***Objective**: To ensure that the network segments are protected to prevent exploitation from both external and internal threats.*

Information System Owner and/or Technology Infrastructure Owner **must**:	
NSM-620	Deploy Host-based Intrusion Detection Systems [HIDS] tools on Information Systems and Technology Infrastructure which store or process: a) Information classified as Confidential or Restricted; b) Information Asset rated 5 or 4 for Confidentiality.
NSM-630	Ensure that only uniquely identified and authorized devices can access Group's network. *Note: this is to prevent for example connections to Group's network through rogue access points, both wire and wireless.*

3.7. Control Area Network Device Protection

***Objective**: To prevent unauthorised configurations being carried out on Network Devices.*

Information System Owner and/or Technology Infrastructure Owner **must**:	
NSM-640	Implement access management to Network Devices diagnostic ports.
NSM-660	Ensure administration of Network Devices is carried out through an out-of-band management network. *For example: Firewall, IDS/IPS, Switches, Routers, SAN, NAS.* *Exception: Not applicable to Network Devices connected only to Group internal network.*
NSM-665	Ensure the administrative access over the internal or external network is encrypted using Group approved Cryptographic algorithms. *[Reference: Cryptography Standard]*
NSM-670	Ensure out-of-band management network is not connected to untrusted networks or Internet.
NSM-680	Configure Network Devices so that they do not respond to external Simple Network Management Protocol [SNMP] strings. *[Note: Only SNMPv3 is allowed for usage in the Group’s network.]* *[Reference: Appendix: Secure Communication Protocols]*
NSM-690	Deploy and maintain secure router configurations between the start-up and running of configuration files.

4. INFORMATION AND SUPPORT

4.1. General Information and Support

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

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 OR INDUSTRY REFERENCES

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

7. APPENDIX

7.1. Secure Communication Protocols

S. No	NAME
1	Transport Layer Security [TLS] v1.2 or 1.3
2	Internet Protocol Security [IPSEC]
3	Simple Network Management Protocol [SNMP] v3
4	Secure Real Time Protocol [SRTP]
5	Cipher Block Chaining Message Authentication Code Protocol [CCMP-AES]
6	Wi-Fi Protected Access 2 [WPA2]
7	Enhanced Interior Gateway Routing Protocol [EIGRP]
8	Border Gateway Protocol [BGP]
9	Intermediate System-to-Intermediate System [IS-IS]
10	Open Shortest Path First [OSPF]

8. 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 Network Security Management Standard, Firewall Standard, Intrusion Detection Standard, Wireless Networks Standard, Remote Environments Standard, Web Application Firewall Standard, Network Devices HLSTS and Network Services Application HLSTS documents have been consolidated in this standard. Consultation feedback, Corrections incorporated.	N/A	Gareth Carrigan, Global Head, ICS Governance, Policy and Risk	1.0	11-Jul-19	11-Jul-19
CISRO ICS Policy	To align with recent Org change, reference to CISO amended to CISRO accordingly within the document.	Non-material	Liz Banbury, Head, ICS Policy	1.1	30-Dec19	30-Dec19

CISRO ICS Policy	Annual Review	Material	Liz Banbury, Head, ICS Policy	2.0	13-Oct20	13-Oct20
CISRO ICS Policy	Note added to control NSM300; Duplication removed from NSM630.	Non-material	Liz Banbury, Head, ICS Policy	2.1	15-Jan21	31-Jan21
CISRO ICS Policy	Annual review: Risks, Roles and Responsibilities alignment to RTF. Controls updated: NSM130, NSM-340, NSM-51	Material	Samantha Finan, Global Head, ICS Policy, Standards and Reporting	3.0	14-Dec21	01-Jan22
CISRO ICS Policy	Based on Change Requests and additional standard review, IC role updated: NSM-035, NSM-060, NSM-320, NSM-330, NSM-340, NSM-371, NSM-490, NSM510, NSM-570, NSM-600	Non-material	Samantha Finan, Global Head, ICS Policy, Standards and Reporting	3.1	22-Jun22	01-Jul-22
CISRO ICS Policy	Modification of: NSM-540 in line with ICSCR-9Mar2022-1, NSM-141 in line with ICSCR-26Jan2022-1	Non-material	Paul Hoare Head, ICS Policy and Best Practice	3.2	08-Mar23	29-Mar23
ICS Standards	Editorial: 3. Document template updated 4. References uplifted in line with organisational changes New controls: 2. NSM-061 & NSM-241 added in line with ICSCR16Aug23-6: Establish a DNS process	Material	Jamie Cowan Head, ICS Risk Framework & Governance	4.0	15-Nov2024	15-Feb2025

9. Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
ICS Standards	Editorial: 1. Document template updated 2. References uplifted in line with organisational changes New controls: 1. NSM-061 & NSM-241 added in line with ICSCR16Aug23-6: Establish a DNS process	Material	Jamie Cowan Head, ICS Risk Framework & Governance	4.0	15-Nov2024	15-Feb2025