Standalone Machine Management Standard

Version No	**4.1**
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	16 December 2024
Approval Date	4 December 2024
Next Review Date	30 November 2027

Table of Contents

Version Control Table

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Katarzyna Wencka **[ICS Standards]**	Administrative changes introduced to update document template, references, roles and ownership.	Non-material	Jamie Cowan Head, ICS Risk Framework & Governance	4.1	04-Dec-24	16-Dec-24

1 INTRODUCTION AND PURPOSE

1.1 Purpose

This Security Standard defines the target control requirements for all Information Systems and Technology Infrastructure within the Group which are not connected to the Group network and are therefore termed 'Standalone Machines'.

Standalone Machines can be deployed on Information Systems & Technology Infrastructure and managed by the Group Technology but can also be deployed and managed by departments other than Group Technology.

Standalone Machines are used for various functions within the Group and the usage and type of the technology architecture (together with the non-standard maintenance approach) will determine the level of risk that the Machine presents to the Group in terms of the type of data entering and leaving the Machine.

Below is a list of some of the key use cases, where a Standalone Machine would be required.

Standalone Machine Usage (examples):
• Customer Internet Access • Marketing/Telesales • On-Line Execution of Trades • Payment Instruction to Third Parties • Physical Security Controls [i.e. CCTV] • Regulatory Related [but not report submissions] • Regulatory Reporting Submissions • Retail Branch Technology [Q-Ticketing] • Staff Internet Access [or Copy Shop] • Telephony System Administration • Specific data processing context (such as pentesting and forensic labs, sandboxing solutions, etc.)

The ideal for the Group is to have no Standalone Machines; however, there are legitimate reasons why some Standalone Machines are needed such as:

- a Regulator requiring specific software to be installed on a Standalone,
- increased risk of certain types of data processing, for example malware sandboxes.

Standalone Machines are often used to either transfer important data externally or to carry out business-critical activities and these Machines therefore pose a significant risk. It is therefore imperative that all Standalone Machines are identified, classified, risk assessed and secured to ensure the overall data protection and security of the Group.

This Standard sets out the minimum Information and Cyber Security [ICS] requirements to be adhered to whilst engaging Third Parties who have access to Group Information during the provision of contracted services to the Group.

Note: *Where a Third Party requires access to Group Information or Group Information is to be shared applicable requirements of Security in Interactions with Third Parties Standard must be followed.*

The Group relies on the Confidentiality, Integrity and Availability of its Information to deliver its services. It is therefore vital that Group Information is protected both on premises and with any Third Party [TP] which processes and/or manages Group Information.

TPs form part of the Group's network and this Standard defines the way in which we assess the security controls of our Third Parties and the security control requirements that we impose on them via contractual agreements.

This Standard is important as TP compliance to our security controls reduces the risk of Security Incidents and helps ensure that the Group maintains the trust of all relevant stakeholders. It also helps to identify areas where these TPs do not meet our requirements so that appropriate risk assessments can be carried out for a risk decision.

1.2 Risks

The Standalone Machine Management Standard mandates that adequate controls are implemented and that the Machines are protected and secured to a level equivalent to the Information Systems and Technology Infrastructure connected to the Group network and managed under Group Technology processes.

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.

1.3 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.

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.

A Standalone Machine is a type of an Information System or Technology Infrastructure all applicable controls from ICS Standards applicable to Information Systems and Technology Infrastructure must be deployed.

Standalone Machine can either operate: (1) in isolation, i.e. not connected to any external network, or (2) be connected to external network (internet or 3rd party network).

The network isolation can be either physical (i.e. no physical connection) or logical (placement is in dedicated VLAN or network segment).

2 ROLES & RESPONSIBILITIES

Information Asset Owner
Information Asset Owners are responsible for granting permissible use of the owned IA, i.e. approving the IA processing on the Standalone Machine(s).

Information System Owner
Information System Owners are responsible for complying with the control areas of this Information Security Standard which are applicable to them and for the protection of Standalone Machines as part of their overall information asset portfolio. They are also accountable for ensuring that the Technology Infrastructure Owners correctly apply the controls as set out in this Standard. As first line role holders they must also have in place a model for validation of control existence and effectiveness.

Technology Infrastructure Owners
Technology Infrastructure Owners are responsible for complying with the control areas of this Information Security Standard which are applicable to them and must ensure that Information processed by the Standalone Machines under their custody are adequately secured. As first line role holders they must also have in place a model for validation of control existence and effectiveness.

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.

Process Owner (PO)
The PO must embed the applicable requirements of this Standard within their process(es) and within any suppliers, joint ventures and outsourced/off-shored activities for which they are responsible.

PO must ensure that information processed by the Standalone Machines supporting their process(es) is adequately secured.

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.

Group Chief Information Security Office (**CISO**)
The CISO support the Information Asset and System Owners for their area by cascading changes to the ICS Policy and Standards to them and to other required business stakeholders ensuring that the changes are understood.

CISOs are responsible for complying with the control areas of this Information Security Standard which are applicable to them.

Group Technology (Technology)
Technology is responsible for complying with the control areas of this Information Security Standard which are applicable to them.

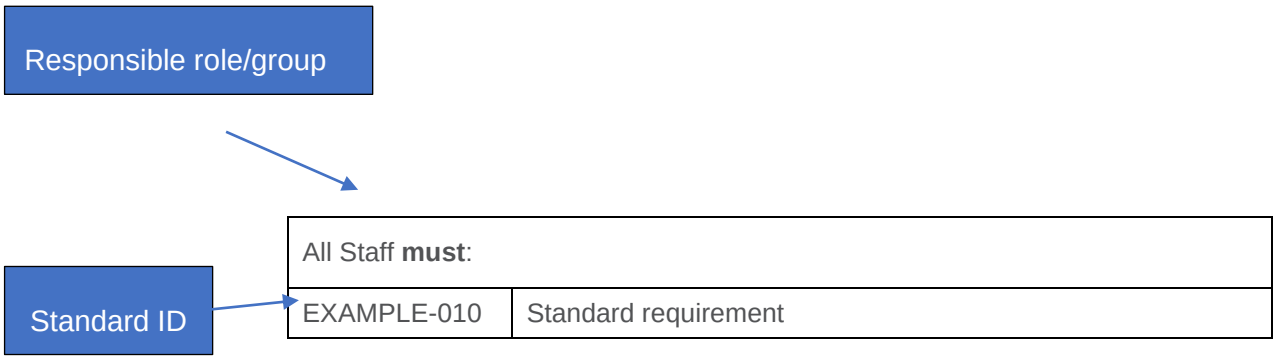
CISO ICS Standards & Controls
The CISO is the owner of this Information Security Standard and will ensure the document is updated to an agreed schedule.

***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: Technical Controls

3.1.1 Technical Controls: Secure Configuration

Technology Infrastructure Owner **must**:	
SMM-010	Ensure the technology used for Standalone Machine deployment is Group approved and, where available, based on a standard build.
SMM-020	Ensure the technology used for Standalone Machines deployment is licensed and vendor supported (where applicable) and not obsolete.
SMM-040	Ensure that, where a standard approach to security controls deployment cannot be followed (such as globally forced password policy), an equivalent solution is identified, assessed, tested, implemented, and documented.
SMM-110	Ensure that network access and allowed traffic (to and from the Standalone Machine) is defined and controlled, with the approach and its deployment reviewed at least every 6 months.
SMM-120	Ensure only encrypted and authorized Portable Storage Devices are used for data transfers. *[Note: Exceptions must be tracked, reviewed periodically, and reported to appropriate country risk committee(s).]*
SMM-121	Limit the software used and data processed on the Standalone Machine strictly to the business use case the Machine supports: 1) any software, services or add-ons not required must be disabled or removed; 2) Information volume, scope and attributes processed must be strictly limited to the business use-cases the Machine Supports – data no longer required must be securely removed/destroyed; 3) recertification of software, services, or add-ons to ensure timely removal and disablement.
SMM-122	Ensure required data retention and availability (in the scope of Standalone Machine data processing).

3.2 Control Area: Operational Controls

3.2.1 Operational Controls: Secure Handling & Maintenance

Information System/Technology Infrastructure Owner **must**:	
SMM-130	Limit the use of the Standalone Machine to those requirements determined by the Process it supports.
SMM-140	Only install Group approved Third Party software that is licensed, sourced from Group approved, legitimate repositories and required to support the Machine operations.
SMM-150	Ensure that data processed is adequately secured in line with the Group ICS Standards. *[Note: The processing and transfer of data is acceptable as long as it meets the required standards.]*
SMM-160	Ensure that Standalone Machines are on-boarded into the Group's centralised IT inventory and the information is managed up to date.
SMM-161	Ensure that Information Asset Owner consent is obtained before processing Information Assets on the Standalone Machine(s). *[Note: Information Assets processed must be secured in line with the applicable standards and assigned criticality.]*
SMM-162	Ensure that owned Standalone Machines are classified through S-BIA. *[Reference: Security BIA methodology]*
SMM-163	Ensure that Standalone Machines are secured in line with the ICS approach and control statements defined for Information Systems or Technology Infrastructure by: • Identifying and deploying relevant baseline controls, • Identifying and applying additional controls in line with the impact rating assessed, • Applying equivalent solution (i.e. at least of the same effectiveness and meeting the control objectives), in the case that certain control cannot be deployed, due to specifics of Standalone Machines in line with SMM-040.

3.2.2 Operational Controls: Reviews

People Leaders **must**:	
SMM-170	Ensure that access reviews are carried out every six (6) months to ensure: 1. Only authorized users are granted access, 2. No generic accounts can be used, except privileged accounts used for maintenance purposes, 3. Only authorized users have a privileged account. Evidence of access reviews must be retained for Audit. *[Reference: Identity and Access Management Standard for the activities and roles required to extract the data for review]*

Technology [Country Technology Managers or equivalent role] **must**:	
SMM-180	Support: • an annual review is conducted to ensure all Standalone Machines are identified and that they are still required and relevant,

	• classification through the S-BIA process is undertaken, to ensure that where high-risk Machines occur, all controls are applied, • verification of the Standalone Machine compliance with the controls imposed by the Standard is completed.
SMM-190	Grant endorsement for the usage of each Standalone for one year based on the Annual Review process.

3.2.3 Operational Controls: Secure Asset Management

All Process Owners **must**:	
SMM-200	Identify, register, and appoint owners for Standalone Machine(s) supporting owned Process(es).
SMM-205	Consult with T&I about the use of the Standalone Machines including the scope and permissible use of the Standalone Machines under their remit.
SMM-210	Approve the scope and permissible use of the Standalone Machines under their remit.
SMM-220	Carry out an annual review to ensure all Standalone Machines are identified and that they are: • still required and relevant; • classified through S-BIA; • compliant with the Standard; • supported with business or technical rationale; • unregistered and applied for removal when not used or no longer required; • assigned to a valid owner.

Technology **must**:	
SMM-230	Provide capabilities to allow registration or deregistration of the Standalone Machines.
SMM-240	Advise Process Owners, Information System Owners and Technology Infrastructure Owners if the Standalone Machine(s) can be replaced by an equivalent solution supported by the standard T&I processes.

Information Asset Owner **must**:	
SMM-250	Ensure Information System/Technology Infrastructure Owner is informed of: 1. Information Asset(s) classification and (potential) restrictions and limitations of their processing on Standalone Machines; 2. Any prerequisites that must be met (processing or scope limitations); 3. Grant or deny any approval requests for Information Asset processing on the Standalone Machine.
SMM-260	Inform Information System/Technology Infrastructure Owner about any changes to the information listed in the SMM-250.

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*

Appendix A – Version Control Table

Document Author 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 Minimum Control Requirements for Standalone Systems and Secure Standalone Systems Support - Guidelines documents have been consolidated and uplifted into this standard. 3. Consultation feedback, corrections incorporated.	Material	Gareth Carrigan, Global Head, ICS Governance, Policy & Risk	1.0	03-Jun-19	03-Jun-19
CISRO Policy	Re-allocation of SMM-190 to the Heads of Information & Cyber Security	Material	Liz Banbury, Head, ICS Policy	2.0	09-Sep-19	09-Sep-19
CISRO Policy	To align with recent Org change, reference to CISO amended to CISRO accordingly within the document.	Non-material	Liz Banbury, Head, ICS Policy	2.1	30-Dec-19	30-Dec-19

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISRO Policy	Annual Review - The following statements have been amended. Major – SMM-110 Minor – SMM-020, SMM-030, SMM-040, SMM-150 Administrative – SMM-010, SMM-070, SMM-090, SMM-100, SMM-120, SMM-140, SMM-160, SMM-190	Material	Liz Banbury, Head, ICS Policy	3.0	16-Apr-20	16-Apr-20
Katarzyna Wencka **[CISRO Policy]**	Out-of-the cycle uplift aimed at assuring consistency in the approach to ICS of various IT assets including CR ICSCR-7Jun2021-1. Updated Risks & paragraph 4. The statements amended: 1) **Administrative**: Information Custodian role replaced with Technology Infrastructure Owner; 2) **Editorial**: 1.1 'Purpose', 1.2 'Risks', 1.3 'Scope', SMM-010, SMM-020, SMM-130,	Material	Liz Banbury, Head, ICS Policy	4.0	10-Nov-21	15-Nov-21

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	SMM-140, SMM-170, SMM-180, 3) **Minor**: 2. 'Roles & Responsibilities', SMM-150, SMM-190; 4) **Major**: SMM-040; 5) **New**: SMM-121, SMM-122, SMM-161, SMM-162, SMM-163, SMM-200 to 260, 6) **Removed**: SMM-030, SMM-050 to SMM-100					
Katarzyna Wencka **[ICS Standards]**	Administrative changes introduced to update document template, references, roles and ownership.	Non-material	Jamie Cowan Head, ICS Risk Framework & Governance	4.1	04-Dec-24	16-Dec-24