Identity and Access Management Standard

Version No	3.3
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 & 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	22 January 2025
Approval Date	17 January 2025
Next Review Date	31 December 2026

Table of Contents

Version Control Table (Latest Changes)

Document Author	Changes made	Materiality	Approved by	Version number
Katarzyna Wencka [ICS Standards]	Administrative changes introduced to update document template, references, roles and ownership.	Non-material	Jamie Cowan Head, ICS Risk Framework & Governance	3.3

The full version history is included in *Appendix A*.

1 INTRODUCTION AND PURPOSE

This Information and Cyber Security Standard defines Identity and Access Management [IAM] requirements for the Information Assets, Information Systems and Technology Infrastructure owned and used by the Group.

Identity and Access Management provides controlled access allowing Staff, Customers and Vendors to carry out their business whilst protecting Group Information Assets, Information Systems and Technology Infrastructure from unauthorised and inappropriate access.

IAM defines the lifecycle required around Staff User identities and accounts associated with those identities and the permissions and entitlements given to those accounts. The Standard also defines requirements to manage access such as Privileged Access Management according to business need and the need to have segregation of controls for certain duties.

This Standard is important as it is a key control in protecting the Group's Information. It sets out control requirements to ensure that Users are identified, authenticated, the correct permissions are allocated and that the User is authorised to access the Information they need according to business requirements.

The Standard also ensures that Access Management is carried out on an on-going basis.

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. Policy 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].

TAM covers all Applications and user entitlements where supporting processes, processes with their activities, string of processes and user entitlements fulfilling the roles:

1) are GRAM rated level 4 [L4] & level 5 [L5];

2) have a potential of impact propagation, leading to L4 or L5 impact (i.e. target process activities are rated <L4, but when combined can lead to L4 or L5 impact);
3) could result in L4 or L5 impact propagation when exposed by identified threat profile.

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 in line with applicable ICS controls defined in ICS Standards.

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 Information Systems and Technology Infrastructure.

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.

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

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

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

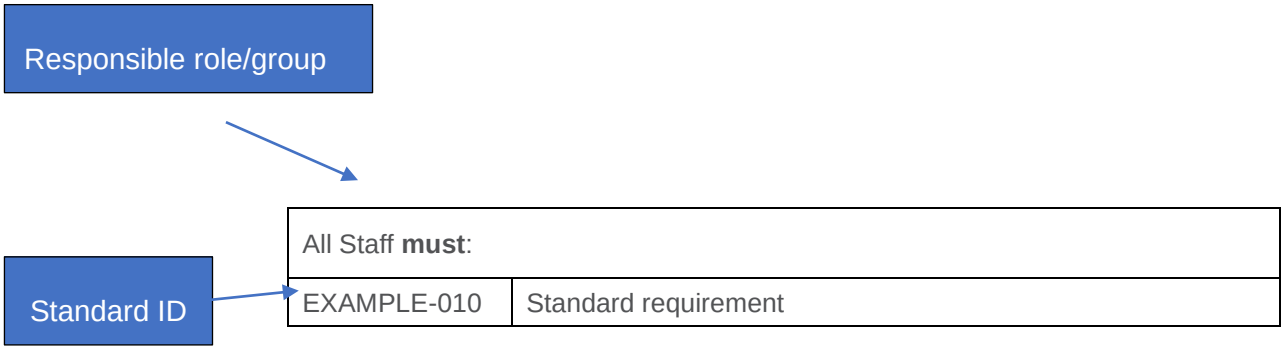
CISO ICS Standards & Controls
The CISO is the owner of this Information Security Standard and will ensure the document is updated to an agreed schedule.

***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: Access Control Governance

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-010	Document and review annually the following IAM requirements for each Information System and Technology Infrastructure: a) Information System Owner/Technology Infrastructure Owner *Note: This is required by Information Classification Standard.* b) Description of the Information System *Note: This is required by Information Classification Standard.* c) Identity and Access security controls (including but not limited to authentication mechanism) d) Roles & entitlements including privileged attributes e) Segregation of Duties [SoD] – Toxic Access Management [TAM] f) Data sovereignty restrictions (Reference: Data Sovereignty Standard) g) Individual Account details: • User ID [Bank ID] • User. h) Generic Accounts details: • Default • Non-Default i) All Accounts attributes details: • Account Owner • Individual/Generic • Privileged (including Emergency) • Interactive or Machine/Non-Interactive • Third Party • Domain • Local • Production • Non-Production • Dormant • Orphan • Service

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-020	Carry out an annual review of the Access Matrix (SoD – TAM) and assigned entitlements.
IAM-030	Document and review annually additional requirements for each Information System and Technology Infrastructure hosted by Third Parties: a) Types of external connections. *[Reference: IAM-010]*
IAM-040	Document and review annually the following procedures for each Information System and Technology Infrastructure: a) Change to entitlements b) Requesting, provisioning, de-provisioning and reviewing of all Account Types c) Password management d) Access Matrix (including SoD – TAM)
IAM-050	Ensure that Identity and Access security controls mandated in this Standard are embedded at design stage, tested for conformance, and then onboarded.
IAM-060	Ensure that any Staff, using or owning Accounts with privileged attribute, are trained to assure that they are aware of their responsibilities and accountabilities.
IAM-065	Document and maintain an accurate and up to date exempt list of applications and systems allowed during Staff long-term leave, including the justification and valid approval for allowing them. *[Reference: IAM-870]*

3.2 Control Area: Account Types

3.2.1 Requirements Applicable to All Accounts

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-130	Ensure all accounts ownership is assigned to Account Owner (Staff identified by a User ID [Bank ID]). *[Reference: IAM-090]*
IAM-135	Document and record all accounts in Information Systems and Technology Infrastructure with the following: a) Creation date and creator details b) Where the account is used (in which Information System or Technology Infrastructure) c) The Account Owner (including User ID [Bank ID]) d) Purpose of the account e) The associated access role (preferred) or entitlements of accounts. (reference IAM-211). f) For Generic Account - list of authorised Staff that can use the Account
IAM-440	Implement effective process for terminating and purging sessions initiated by unsuccessful/failed logon attempts.

3.2.2 Individual Accounts

3.2.2.1 User ID [Bank ID]

Information System Owner [Human Resources Manager] **must**:	
IAM-070	Establish the identity of each Staff before assigning them a unique identifier which will be the User ID [Bank ID].

Information System Owner [Human Resources Manager] **must**:	
IAM-080	Ensure that each Staff has signed the Contract and Terms of Employment prior starting employment to assure that Staff is contractually bound to comply with the ICS Policy and ICS Standards.
IAM-100	Document and record the following for each Staff: a) unique User ID [Bank ID] b) Full name c) Employment status

3.2.2.2 User Account

No specific control requirements for this type of Account in this section.

3.2.3 Generic Accounts

3.2.3.1 Requirements Applicable to All Generic Accounts

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-150	Allow usage of Generic Accounts only if an Individual Account creation is not technically feasible or practically justified and document the exception (including risk assessment). *Note: Generic Accounts can only be used for one purpose and have access only to one Information System or to one Technology Infrastructure.* *[Reference: IAM-190i]*
IAM-250	Identify ownership, authorised user and the entitlements required for Generic Accounts and ensure that they are approved by Information System Owner or Technology Infrastructure Owner.

3.2.3.2 Requirements Applicable to Default Generic Accounts

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-120	Disallow usage of Default Generic Accounts through disabling/locking them and creating equivalent accounts. *Exception: If disabling/locking is not technically feasible then the default password of such Account must be changed in line with requirements defined in Identity and Access Management Standard.* *[Reference: IAM-115]*

3.2.3.3 Requirements Applicable to Non-Default Generic Accounts

No specific control requirements for this type of Account in this section.

3.2.4 Account attributes

3.2.4.1 Privileged (including Emergency)

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-190	Establish a documented process for managing Accounts with Privileged attribute in Information Systems and Technology Infrastructure (including Local Accounts with Privileged attribute) which adhere to the following: a) Technique for controlling Account (with Privileged attribute) access and use for each Information System and Technology Infrastructure must be determined: Account escalation (Individual Account) or account sharing (Generic Account); b) Privileged entitlements for each account must be identified, approved, and recorded c) Every usage must be directly associated with defined, planned, and approved security or administrative activity [For example: Change Request or Incident]. This must be ensured through implementation of a Just-In-Time Access control model (if not technically feasible then exception must be documented [including risk assessment]). "Broker and remove access" type is preferred and recommended d) Password for Account with Privileged attribute must be securely vaulted when not in use e) Password for Account with Privileged attribute must be changed after each usage f) Access to Account with Privileged attribute must have an identified Owner and be restricted to Staff authorised by Information System Owner or Technology Infrastructure Owner g) Controls must be in place to ensure that identification of authorised Staff, using Account with Privileged attribute at any time, is possible. (This must include full auditing and non-repudiation mechanisms) h) Must be recertified every six months i) Staff having access to any Information System or Technology Infrastructure with the usage of any Generic Account with Privileged attribute cannot have access to such Information System or Technology Infrastructure with the usage of any Individual Account. j) Staff having access to any Information System or Technology Infrastructure with the usage of any Individual Account with Privileged attribute cannot have access to such Information System or Technology Infrastructure with the usage of any other Individual Account. *[Reference: IAM-135]*
IAM-200	Maintain a register of individuals/delegates who can approve granting privileged entitlements to any Account in owned Information Systems and Technology Infrastructure. *[Reference: IAM-190f]*

3.2.4.2 Third Party

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-195	Establish a documented process for managing accounts with Third Party attribute to access, support, or maintain Group's Information System and Technology Infrastructure via remote (external) access or On-Prem, which adhere to requirements defined in this Standard and also in addition: a) Third Party Account should always be of a Generic Type (if not technically feasible then exception must be documented [including risk assessment]) b) Password for a Third Party Account must not be revealed through automatic granting secure access using Third Parties' own credentials c) if Single Sign-On [SSO] is used then it must be performed by injecting the required credentials as the connection request passes through Group's proxies d) Third Party Account access (including Emergency Privileged) should be restricted to specific time windows or granted for the minimum period required to perform expected activities e) Read-only access control should be considered for Third Party Accounts to complement the restricted write/modify access f) All Third Party Account access must be recorded for each session g) Third Party Account must be granted with minimum role-based entitlements required to perform expected activities *Note for Third Party Accounts with Privileged entitlements IAM-190 must be followed.* *[Reference: IAM 3.2.1 Requirements Applicable to All Accounts]* *[Reference: IAM-390 (Exception: subpoint c) is not applicable to Third Parties Accounts)]* *[Reference: ICS Standard - Security in Interaction with Third Parties]*

3.2.4.3 Domain

No specific control requirements for this type of Account in this section.

3.2.4.4 Local

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-140	Allow usage of Local Accounts only if a domain account creation is not technically feasible and document the exception (including risk assessment).

3.2.4.5 Production

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-110	Disallow usage of Production Accounts in Non-Production Environments.

3.2.4.6 Non-Production

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-115	Disallow usage of Non-Production accounts in Production Environments.

3.2.4.7 Dormant

Reference IAM-720

3.2.4.8 Orphan

Reference IAM-720

3.2.4.9 Service

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-160	Ensure that only Non-Interactive Service Accounts are used for System-to-System Authentication and Interactions.

3.3 Control Area: Approving, Granting and Provisioning Access

3.3.1 Approving Access

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-230	Ensure that any Account creation or any modification in owned Information Systems and Technology can only be performed if approval has been obtained from: a) People Leader / Information System Owner or Technology Infrastructure Owner for Individual Account b) Information System Owner or Technology Infrastructure Owner for Generic Account *Note: For Privileged Emergency Account creation or enablement there must exist a valid corresponding incident ticket.*
IAM-205	Maintain a register of individuals/delegates who can approve Staff assignment to Generic Account in owned Information Systems and Technology Infrastructure.
IAM-210	Identify and approve Staff ('Authorised Staff') assignment for the use of any Account as needed by their Job Role and based on the 'Least Privilege' Principle.

3.3.2 Provisioning Approved Access

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-211	Create any Account which adhere to the following: a) Entitlements must be assigned to Role and then Role to an Account b) Accounts (identifier/login/Account name) must be unique (if technically feasible) and follow naming convention that enables differentiating them between Production and Non-Production *Note: Assigning entitlements directly to an Account is not allowed (if not technically feasible then exception must be documented and risk assessed, then assigning entitlements directly to an Account is allowed).*
IAM-212	Ensure any Account created with Privileged attribute adheres to the following: a) Password for Account must be securely vaulted when not in use b) Password for Account must be changed after each usage c) Access to Account must be restricted to Staff authorised by Information System Owner or Technology Infrastructure Owner d) Controls must be in place to ensure that identification of authorised Staff, using Account with Privileged attribute at any time, is possible. This must include full auditing and non-repudiation mechanisms
IAM-090	Create a unique User ID (identifier) which will be [Bank ID] which adhere to the following: a) must be in 'disabled' status until the new joiner or Non-Employed Worker [NEW] is onboarded b) must be issued with one-time login password securely provided to People Leader *Note: The User ID [Bank ID] cannot be a reassigned ID with the exception of re-hires.* *Note: User ID [Bank ID] must be stored in the People Management System.*

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-310	Create any Individual Account which adhere to the following: a) Forces Individual Account Owner to change any initial password. *Note: Any Account for new joiner or NEW can only be created after the issuance of the User ID [Bank ID].* *[Reference: IAM-090]*
IAM-155	Ensure all Generic Account adhere to the following: a) Password for Generic Account must be securely vaulted when not in use b) Password for Generic Account must be changed after each usage c) Access to Generic Account must be restricted to Staff authorised by Information System Owner or Technology Infrastructure Owner d) Controls must be in place to ensure that identification of authorised Staff, using Generic Account at any time, is possible. This must include full auditing and non-repudiation mechanisms
IAM-240	Provide authorised Staff with login details of Generic Accounts and grant access to vault. *[Reference: IAM-155]*

3.3.3 Authentication at Logon

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-340	Apply approved authentication methods for each Account usage. All Accounts must be authenticated at least once before being allowed to access to an Information System or Technology Infrastructure.
IAM-350	Ensure in Information System and Technology Infrastructure that if SSO is used then Account credentials must be protected with strong authentication. For Example: where SSO has Multi-Factor Authentication [MFA] enabled. *Note: Shared usage of SSO between Production and Non-Production environments is not allowed.*
IAM-360	Apply MFA commensurate with Information System and Technology Infrastructure S-BIA Rating. *Note: In line with Table "Multi Factor Authentication" MFA implementation must include at least 2 of 3 Authentication Factors.* *[Reference: Tables: "Authentication Requirements Matrix Table" and "Multi Factor Authentication"]*
IAM-370	Ensure that usage of an MFA solution is assessed for security aspects and approved by the Group. *[Reference: Table: "Multi Factor Authentication"]*
IAM-390	Ensure that remote access to Group Information Systems and Technology Infrastructure must: a) Be documented and Group approved b) Use MFA for Authentication c) Use Group approved solutions to verify that the IT Equipment being used by Staff is Group owned and/or managed *Note: Remote access excludes customer access to Group Information Systems and Technology Infrastructure.* *[Reference: Network Security Management NSM-210]* *[Reference: IAM-450]*

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-400	Design and implement password (including passphrase) and PIN management controls for Information Systems and Technology Infrastructure which follow the required complexity (as set out in Table 7.1) and in addition: a) Ensure that initial password (including passphrase) and PIN for any Account must be different from the associated Account identifier (Account Name/login) b) Enable Individual Account Owners to change their password (including passphrases) and PINs c) Mask any Account's password (including passphrases) and PIN characters when they are being entered d) Ensure that only holders of Accounts with Privileged attribute can access files containing passwords (including passphrases) and PINs e) Encrypt all Accounts passwords (including passphrases) and PINs at-rest (with strong encryption) and in-transit f) Ensure passwords (including passphrases) and PINs are never hardcoded *[Reference: Tables: "Authentication Requirements Matrix Table" and "Multi Factor Authentication"]* *[Reference: Cryptography Standard]*
IAM-410	Ensure that, if Digital Certificates are used for the purpose of authentication, then solutions must be designed and implemented to carry out a Digital Certificates validation. *[Reference: Digital Certificate Management Standard].*
IAM-450	Implement session idle and absolute timeouts in line with the following 1) User sessions a) S-BIA 4-5 systems must have • Idle Session Timeout <= 15 minutes • Absolute Session Timeout <= 60 minutes. b) SBIA1-3 systems must have • Idle Session Timeout <= 15 minutes • Absolute Session Timeout <= 120 minutes Machine – Machine internal systems a) S-BIA 4-5 systems must have: • Idle Session Timeout <= 30 minutes • Absolute Session Timeout <= 12 hours b) SBIA 1-3 systems must have • Idle Session Timeout <= 30 minutes • Absolute Session Timeout <= 18 hours 2) Applications using modern protocols such as OAuth 2.0 can use Refresh Tokens to keep sessions alive while adhering to 1) and 2). Session must be terminated and purged after reaching above timeouts and reauthentication enforced to login again. *Note: Implement appropriate notifications for expiring sessions.*
IAM-455	Implement a minimum of 30 minutes account lockout duration of the user ID or until administrator enables it.
IAM-470	Ensure that Information Systems and Technology Infrastructure do not display redundant Information (especially last login) on logon screen.
IAM-480	Ensure that direct access to databases with S-BIA rating 4-5 is limited to Accounts with Privileged attribute only.

3.3.3.1 Authentication – Password

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-490	Ensure that during the logon process Information System and Technology Infrastructure must: a) Prevent concurrent session logons of same Individual Account for Web Application only b) Advise Web Application Users of the date and time of their last successful login c) Notify Users that access to Information Systems / Technology Infrastructure / Application is permitted for authorised use only

3.3.3.2 Authentication – Token/PIN

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-500	Ensure the controls related to the use of token and PIN authentication must: Include a documented process for registering Users' tokens including request and approval requirements: a) Manage lifecycle of tokens and token access including secure destruction of tokens when no longer active or needed b) Ensure delivery is to the authorised requestor c) Issue token and PIN separately d) Be restricted to hardware and software tokens approved by the Group e) Include a process to authenticate the Staff if the token authentication fails f) Include awareness procedures for the Staff that at a minimum cover: • protecting the token against loss, theft, and misuse • changing of the PIN • credential sharing is forbidden • reporting any actual or suspected loss, theft, misuse, or tamper of the token • return of the token when it is no longer needed or before leaving the Group g) Ensure token management is configured as per the ICS Security Configuration Management Standard
IAM-510	Apply only Group approved cryptographic algorithms to generate One-Time Passwords [OTP]. *[Reference: Cryptography Standard]*
IAM-520	Ensure that OTP tokens consist of at minimum 6 characters.
IAM-525	For time-based OTPs ensure that validity period is as short as practicable to lower the risk of a stolen OTP being used for fraudulent transactions.

3.3.3.3 Authentication – Biometrics

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-530	Establish a documented process for using biometric Authentication which adhere to the following: a) An appropriate biometric mechanism should be selected b) Staff's unique biometric details must be registered (this must require direct Staff involvement and physical presence for the registration) c) Staff's unique biometric details, that are stored in the form of electronic data, must be encrypted and protected from unauthorised access, modification or deletion d) Staff's unique biometric details must be processed, stored, transferred, or removed in compliance to applicable privacy, regulatory requirements e) Include a process to reauthenticate the Staff when the biometric Authentication fails f) Include awareness procedures for the Staff that at a minimum cover: • protecting biometric Authentication details from loss, theft, and misuse • reporting any actual or suspected loss, theft, misuse, or tamper of the biometric Authentication details *[Reference: NIST Special Publication 800-76-2]*

3.3.4 Secure Handling of Credentials

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-540	Ensure that distribution of passwords for User ID [Bank ID] complies with: a) when sent via post then address must be verified, envelop must not include associated User ID [Bank ID and must not indicate the content b) delivering of password and associated User ID [Bank ID] be sent separately and in a secure manner viz., encrypted channels using secure protocols, sealed/tamper resistant envelopes and similar.
IAM-550	Ensure that distribution of tokens for User ID [Bank ID] complies with: a) when sent via post then address must be verified, envelope must not include associated User ID [Bank ID] and must not indicate the content.
IAM-560	Maintain an up-to-date inventory of tokens which includes the following Information (including destroyed tokens): a) The Device ID b) Details of Staff the token is allocated to c) The date the token was allocated *Note: A review of token allocation must be conducted at least every twelve months.*

3.3.5 Preventing Unauthorised Access

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-660	Verify and Validate the User's identity when unlocking an account or changing a forgotten password. *[Reference: Tables: Authentication Requirements Matrix and Multi Factor Authentication]*
IAM-670	Reset Account's password if: a) The request has been made by the Account Owner; b) The requestor's identity has been verified.

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-680	Authenticate all tokens prior to unlocking them by either: a) Calling Staff back on their listed or registered phone number b) In person with Staff c) Contacting People Leader if Staff does not have a phone number registered in Group's People Directory *[Reference: AUS-570]*

3.4 Control Area: Revoking / De-Provisioning Access

People Leader **must**:	
IAM-690	Register a request for moving Staff to ensure: a) Removal of no longer needed logical access to Information Systems and Technology Infrastructure held by moving Staff in current role b) Recovery or return of no longer needed Group owned IT equipment [including: Cryptography Keys or Physical Tokens] held by the moving Staff c) Reassigning of Generic Accounts owned by moving Staff (no longer needed in a new role) to the appropriate new Account Owner d) Provision of needed access to Information Systems and Technology Infrastructure in moving Staff's new role e) That movers process is concluded before moving Staff starts new role or as per mover process SLA.
IAM-700	Register a request for leaving Staff to ensure: a) Notification to HR or update of HR record with 'Last Working Date' details b) That leaving Staff's logical access Information Systems, Technology Infrastructure is removed before or on the Last Working Day or as per leaver process SLA c) Reassigning of Generic Accounts owned by leaving Staff to the appropriate new Account Owner d) Verification that any Group owned IT Equipment [including: Cryptography Keys or Physical Tokens] held by leaving Staff is recovered or returned to the Group before or on the Last Working Day.

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-710	Remove Account entitlements in case of: a) Request from Account Owner, People Leader, Information System Owner or Technology Infrastructure Owner b) Account expiry c) Lack of possibility to disable/lock Account *[Reference: IAM-720]* *Note: In case that Account won't be used anymore, or it expired then at first the Account must be disabled/locked in line with IAM-720 (if technically feasible, if not then only the entitlements must be removed).* *[Reference: For Accounts with Third Party attribute follow IAM-195d]*

Information Asset Owner and/or Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-720	Disable/lock any Account in case of: a) Account was not used for more than 90 calendar days [Dormant Account] in all Information Systems and Technology Infrastructure with S-BIA rating 4-5 b) Account was not used for more than 180 calendar days [Dormant Account] in all Information Systems and Technology Infrastructure with S-BIA rating 1-3 c) Account has no Account Owner [Orphan Account]; d) request from the Account Owner, People Leader, Information System Owner or Technology Infrastructure Owner e) Account expiry f) Individual User Account / Customer Account initial password has not been changed within 3 days *Exception: If disabling/locking is not technically feasible then all entitlements of such Account must be removed. Reference: IAM-710.* *[Reference: For Accounts with Third Party attribute follow IAM-195d]*

3.5 Control Area: Entitlements Review

3.5.1 Preventing Inappropriate Access

Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-725	Ensure that Information Systems and Technology Infrastructure with S-BIA rating 5 are onboarded to Group's entitlement review platform.
IAM-850	Initiate Access Reviews every 6 months once in accordance with the Access Review Certification (ARC) process and provide People Leader with the required reports. *[Reference: IAM-840]*
IAM-880	Review and endorse the results of owned Information Systems and Technology Infrastructure Access Review reports.
IAM-890	Prepare completion rates reports of Access Reviews and any access discrepancies in owned Information Systems and Technology Infrastructure.

Information System Owner and/or Technology Infrastructure Owner and/or Application Owner **must**:	
IAM-840	Ensure that the access reports from their owned Technology Assets contain the following: a) All Access roles/entitlements & associated permissions (e.g., in a Security Access Matrix report) b) Staff's Accounts (including assigned Individual Accounts and/or Generic Accounts (e.g., in a User Access List report) with the following minimum fields for access reviews: • User ID [Bank ID] • Account Owner • Account Roles/Entitlements • Last Logon Date • Status • Report generation date and time stamp (where technically feasible) • Last password change date & time (where Authentication is via password and it's technically feasible)

People Leader **must**:	
IAM-790	Report an incident in case of any issue identified during Access Reviews.

People Leader **must**:	
IAM-860	Complete all Access Review Certification (ARC) every 6 months to ensure that access for managed Staff is the minimum required to carry out their Job Roles. The review includes: a) Confirmation that managed Staff is in fact direct subordinate and an active employee b) Validation of Staff's each Account (both Individual and assigned Generic) entitlements c) Confirmation that SoD – TAM and 'Least Privilege' principles are applied d) Identification of any Staff's Account that is no longer required (as a result of mover/leaver process) and ensuring that they are disabled/locked e) Identification of Dormant and Orphan Accounts and ensuring that they are disabled/locked if no longer needed f) Retaining evidence that the ARC are completed on time. *[Reference: IAM-720 a) & b) & c) - guidance for 'Dormant Accounts' and 'Orphan Accounts']* *[Reference: IAM-710 - removal of entitlements]*
IAM-870	Request disabling/locking of Staff's Individual Accounts in Information System and Technology Infrastructure when Staff is for whatever reason on a long-term leave (30 calendar days or above). *Exception: Disable/locking of Information System access excludes an exempt list of applications and systems.* *[Reference: IAM-720, IAM-710, IAM-065]*

3.6 Control Area: Remote (External) Access

Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-910	Ensure that all requests for remote (external) access with the usage of any Accounts with Third Party attribute to owned Information Systems and Technology Infrastructure are reviewed and approved before granting such access.
IAM-920	Define remote (external) access security requirements and document all remote (external) access requests, together with the details of used account and its entitlements.
IAM-930	Review remote (external) access at least every six months.

3.7 Control Area: Requirements for Non-Employed Workers [NEW]

Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-950	Disable external email and printer access for NEW by default. Access can be enabled if approved by Managing Director or above.

3.8 Control Area: Customer Access

Information System Owner and/or Technology Infrastructure Owner **must**:	
IAM-960	Document and implement procedures for the provision of access to the Group's Information Systems for customers which cover: a) actions to be performed before granting access to customer (including customer identification and secure credentials provisioning); b) access control requirements that should include: • effective customer authentication method (through applying a risk-based approach and implementing an appropriate risk-based or adaptive authentication that presents customers with authentication options that commensurate with the risk level of the transaction and sensitivity of the information) • assigning to customers unique IDs • strength of the password including a Personal Identification Number (PIN) • forcing customers to change their initial password when it is first used • masking the password characters when they are being entered • enabling customers to change their password • encrypting passwords (including passphrases) and PINs at-rest (with strong encryption) and in-transit • disabling customer access if the initial password has not been changed within three days • assuring that customers are authenticated using Group approved Authentication or as per applicable regulations • assuring that only authorised customers are permitted to have access • assuring that customer account Information is updated only when the customer has been authenticated • protection against automated brute-force attacks, repeated logon attempts and concurrent logons • assuring that customer account must be protected from unauthorised access and modification • periodical password change • restricting access only to Information based on 'Need to know' principle • SoD - TAM and security measures to ensure any password generated, re-issued, or reset by Group would not be disclosed or leaked during the generation and delivery • configuring session idle timeout • not displaying, storing and/or transmitting in clear text any passwords (including passphrases) or any PIN's or any such Authentication values • not displaying any specific error or help messages that would facilitate an unauthorised access to succeed • notifying customers of the date and time of their last successful login. c) customer access arrangements including periodical review (as per applicable regulation or at least annually) d) managing security incidents related to customer access e) legal, regulatory, and mandatory requirements
IAM-995	Ensure that for high-risk activities (including high-risk transactions) MFA of customers is implemented.

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 Authentication Requirements Matrix Table

In case that any Account is holding more than one attribute then the strictest requirements should be applied.

Authentication Requirements								
Requirements / **Categories**	**Multi Factor Authentication (MFA) MFA =** **1. What I know 2. What I have 3. Who am I**	**Minimum Password/ PIN Length**	**Maximum Password Change Cycle**	**Password Reuse/history Prohibited**	**Password/PIN Uniqueness**	**Password/PIN Complexity**	**Lockout after number of Incorrect Attempts**	**Vaulting**
1. Information Systems & Technology Infrastructure of S-BIA 4-5 2. Internet Facing & External Accessed (e.g., Third-Parties, Regulator, On-line Banking) Information Systems & Technology Infrastructure	Yes	12 Characters	180 days	Last 10	Must not be User ID [Bank ID], Client ID Number or equivalent.	Minimum must: 1. Contain Numbers 2. Be a combination of Upper and Lower cases letters. 3. Include special characters/symbols (e.g., &"%). 4.Not be sequential (ascending or descending)	3	N/A
Information Systems & Technology Infrastructure of S-BIA 1-3	No	8 Characters	90 days	Last 8	Must not be User ID [Bank ID]	Minimum must: 1. Contain Numbers 2. Be a combination of Upper and Lower cases letters. 3. Include special characters/symbols (e.g., &"%). 4.Not be sequential (ascending or descending)	6	N/A
Laptops and other similar devices access Group Data	Yes	12 Characters	AUS-460 or 180 days	Last 10	Must not be User ID [Bank ID], Client ID Number or equivalent.	Minimum must: 1. Contain Numbers 2. Be a combination of Upper and Lowe cases. 3. Include special characters/symbols (e.g., &"%). 4.Not be sequential (ascending or descending).	6	N/A

						5. Not be an 'illegal patterns' i.e., patterns based on ordinary words / Password Dictionary.		
Personally owned [All] and Group owned Mobile Devices (Smartphones and Tablets iOS/Android) access and/or hold Group Data		6-digit PIN	AUS-460	Last 8	Must not be User ID [Bank ID] [Reference AUS-470 for All Staff	1. Numbers must not be sequence in both orders (e.g., 345678 or 876543) 2. Must avoid repeat of same number (e.g., 333333)	6	N/A
Accounts with Privileged attribute	Yes	25 Characters Note: Requirement satisfies the SWIFT requirement as mandated in CSF as 15+ characters	IAM-212 b) or 180 days	Last 10	Must not be User ID [Bank ID]	Minimum must: 1. Contain Numbers 2. Be a combination of Upper and Lower cases letters. 3. Include special characters/symbols (e.g., &"%). 4.Not be sequential (ascending or descending)	3	IAM-212 a)
Service Accounts	No	25 Characters	180 days	Last 10	Must not be User ID [Bank ID]	Minimum must: 1. Contain Numbers 2. Be a combination of Upper and Lower cases. 3. Include special characters/symbols (e.g., &"%). 4.Not be sequential (ascending or descending)	3	Yes
Generic Accounts	No	18 Characters	IAM-155 b) or 180 days	Last 10	Must not be User ID [Bank ID]	Minimum must: 1. Contain Numbers 2. Be a combination of Upper and Lower cases letters. 3. Include special characters/symbols (e.g., &"%). 4.Not be sequential (ascending or descending)	3	IAM-155 a)

7.2 Multi Factor Authentication [MFA]

Authentication Factor	Attributes	Approved Method
Something you Know	This is something known only to the User and can be recorded or allocated to their User ID [Bank ID]	• Password / PIN • Pre-shared secret or Private Information
Something you Have	This is something that is known to or belong to the User and can be authenticated or tracked to their User ID [Bank ID]	• Smart Card/Digital Certificate • Token [with OTP] • Badge • Security Keys • Smartphones/Mobile Devices
Something you Are	This is something assumed to be a unique part of that User.	• Fingerprint/Hand Scans/Hand Geometry/Finger Vein Sensing Technology • Retinal Pattern/Scans • Customer's Voice/Voice Scans/Voice Recognition • Face Geometry/Facial Scans/Face Feature • Iris Pattern • Signature Scans

APPENDIX A - Version Control Table

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISRO Policy	All previous versions are migrated to ERMF template and the Standard version is reset to v1.0 in ERMF template.	-	Gareth Carrigan, Global Head of Information & Cyber Security Policy, Governance & Risk	Up to 3.3	18-Jun-2019	-
CISRO Policy	This uplifted IAM Standard has replaced the existing Access Control Management and Governance [ACMG] Standard and a few other controls documents.	-	Liz Banbury	1.0	06-Nov-19	15-Feb-20
CISRO Policy	IAM-490 Changed the scope of points b) and c) to Web Applications only to align with OWASP and NIST requirements [ICSCR-16Nov2019-2] Definition included in Glossary for Application/Web Applications.	Non-material	Liz Banbury, Head of ICS Policy	1.1	10-Feb-20	15-Feb-20
CISRO Policy	A note added to IAM-720 and IAM-730 as approved in ICS Change Request [CR] Forum – *ICSCR-24Mar2020-1*.	Non-material	Liz Banbury, Head of ICS Policy and Risk	1.2	17-Jun-20	17-Jun-20
CISRO Policy	Removal of 90 days Password Change Cycle for Personally Owned [All] and Group owned [Android] Mobile/Smartphones/Tablets in Appendix 6.2.1. This was approved in ICS Change Request [CR] Forum – *ICSCR-22Jun2020-1 & ICSCR-23Jun2020-1.*	Non-material	Liz Banbury, Head of ICS Policy and Risk	1.3	04-Sep-20	04-Sep-20
CISRO Policy	Annual Review	Material	Liz Banbury [delegate of Group CISRO]	2.0	15-Jan-21	01-May-21
CISRO Policy	Annual Review. TAM definition added to Scope; **New Controls**: IAM-065, IAM-455;	Non-material	Samantha Finan, Global Head, ICS Policy, Standards and Reporting	2.1	15-Dec-2021	01-Jan-22

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	Removed Controls: IAM-600, IAM-650; **Updated Controls**: IAM-680, IAM-870, Updated Table 7.1					
CISRO Policy	**Updated Controls:** IAM-690, IAM-700, IAM-840, IAM-450, IAM-010	Material	Samantha Finan, Global Head, ICS Policy, Standards and Reporting	3.0	22-Jun-22	01-Jul-22
CISRO Policy	1. Template updated to ERM Standard template v5.6 2. Changes made w.r.t ICS Policy Changes Requests: a. ICSCR-16Dec2022-1 – Updated - IAM-660 b. ICSCR-19Dec2022-6 – Updated – IAM-010, IAM-060, IAM-250, IAM-420, IAM-160, IAM-190 & IAM-720 c. ICSCR-25Jul23-1 – Updated – Table 7.1 for Laptop Password length. d. ICSCR-26Jul23-1 – Updated – Table 7.1 for Laptop Password Complexity. e. ICSCR-26Jul23-4 – Updated – Table 7.1 for Mobile Devices lock out attempts. f. ICSCR-26Jul23-5 – Updated – Table 7.2 for Approved MFA methods. g. ICSCR-30Jan2023-1 – Updated - IAM-135, IAM-155, IAM-211, IAM-212, IAM-540,	Non-Material	Paul Hoare, Head ICS Policy & Best Practice	3.1	13-Nov-23	14-Nov-23

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	IAM-840, IAM-850, IAM-860. h. ICSCR-18Feb2022-1 – Removed as covered in Acceptable Use Standard - IAM-570, IAM-580, IAM-590, IAM-610, IAM-620, IAM-640, IAM-996. 3. People Manager to People Leader 4. Updated IAM-680 by replacing referenced INH-500 with AUS-570.					
CISRO Policy	1. Included with entries of versions 1.2 & 1.3 in Version Control table. 2. Correction made to IAM-155 by removing word 'which'.	Non-Material	Paul Hoare, Head ICS Policy & Best Practice	3.2	08-Dec-23	14-Nov-23
Katarzyna Wencka [ICS Standards]	Administrative changes introduced to update document template, references, roles and ownership.	Non-material	Jamie Cowan Head, ICS Risk Framework & Governance	3.3	17-Jan-25	22-Jan-25