Acceptable Use Standard

Version No	1.2
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	Katarzyna Maria Wencka
Document Contact Job Title	Director, ICS Standards
Business Scope	All Businesses
Function Role	All Functions
Geography Scope	GLOBAL
Approval Date	04/12/2024
Effective Date	16/12/2024
Next Review Date	30/06/2026

Table of Contents

1. INTRODUCTION AND PURPOSE....................4

1.1. Risks....................4

1.2. Scope....................4

2. ROLES & RESPONSIBILITIES....................5

3. STANDARD REQUIREMENTS....................5

3.1. Control Area- General Provisions....................5

3.2. Control Area- Information Security & Handling Requirements....................8

3.3. Control Area- Secure Working Practises....................13

3.4. Securing Access to Group's Information Technology resources....................14

3.5. Control Area- Acceptable Use of Group Information Technology Resources....................17

3.6. Control Area- Secure Disposal of Group Information & Devices....................22

3.7. Control Area- Incident reporting & handling....................24

4. INFORMATION & SUPPORT....................24

4.1. General Information and Support....................24

4.2. Reporting Non-Compliance....................24

4.3. Breach of this Standard....................24

5. GLOSSARY....................25

6. REGULATORY INDUSTRY REFERENCES....................25

7. APPENDIX....................25

7.1. [AUS-AP-010] Table 1 – Confidentiality Classification Labels....................25

7.2. [AUS-AP-020] Table 2 – How to Classify the Information....................26

7.3. Handling Non-Electronic and Electronic Information....................27

7.4. Appendix A – Version Control Table....................31

....................31

8. Version Control Table....................32

Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Katarzyna Maria Wencka	Acceptable Use Standard	Non-Material	Jamie Michael Cowan	1.2	04/12/2024	16/12/2024

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

1. INTRODUCTION AND PURPOSE

The Group provides access to Information Technology resources, including computers, services, applications and peripheral devices[1], to support its mission and business objectives. Group's Information and Information Technology ("IT") resources must be used in an approved, ethical and lawful manner to avoid any adverse impact, including loss or damage to the Group's operations, reputation and financial interests and to comply with applicable regulations.

In order to prevent Staff from increasing the information and cybersecurity risk to Information and Information Technology resources, the Acceptable Use Standard ("AUS") establishes Rules of Behaviour, i.e. the Group expects all Staff to follow, when using Group's Information Technology resources and handling Group's Information.

The Rules of Behaviour drive a healthy Risk Culture as applied to ICS through the development of interventions such as: ensuring clarity of roles and responsibilities in ICS risk management processes, provisioning of behavioural guidance to enable employees to do the right thing, uplifting ICS risk management knowledge to strengthen conduct and behaviour of all staff. Regardless of your role in the Bank, upholding the Confidentiality, Integrity and Availability of the Group Information Technology resources and Information is vital for:

- Supporting Group's business strategy and objectives,
- Ensuring compliance with applicable laws and regulations,
- Mitigating various ICS threats specific to end-user activities.

In addition to the above, AUS also defines the activities which are strictly prohibited as posing direct or indirect ICS risk and increasing ICS threat exposure. The control statements of this Standard also aim at increasing Staff understanding of their role in effective ICS risk management.

1.1. Risks

Failure to adopt and implement this Information and Cyber 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

The Standard is mandatory and applies to all **Standard Chartered PLC** (the "Group") entities, except where explicitly prohibited by local Law or Regulation [assessed as per section 4.2 Reporting Non-Compliance].

The control statements of the Standard:

- apply to All Staff,
- cover general, BAU All Staff activities, i.e. this Standard does not define requirements for security controls definition, implementation and maintenance for Information and Information Technology resources (where applicable ICS Standards must be followed),
- apply in the context of handling Group's Information or interacting with Group's Information Technology resources.

[1] such as keyboards, mice, docking stations, etc.

***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".*

Requirements of this Standard apply to all Information Assets and Technology Assets in the Group regardless of the environment (e.g. End user, Prod, Test).

2. ROLES & RESPONSIBILITIES

All Staff

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

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.

CISO ICS Standards & Controls

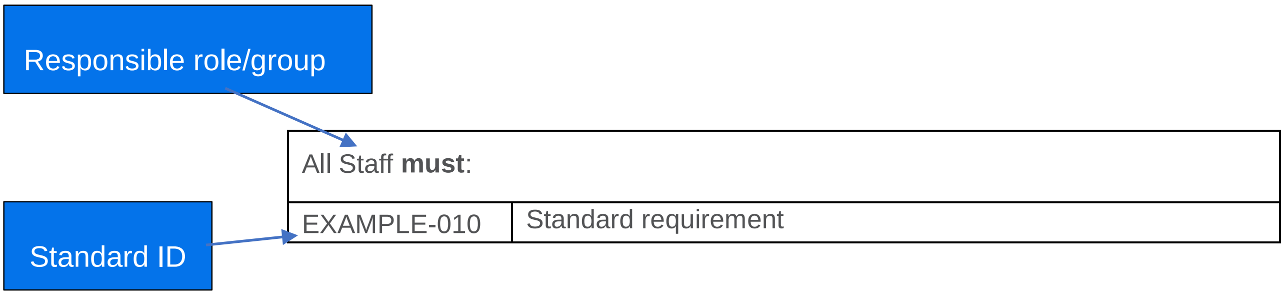
The CISO is the owner of this Information Security Standard and will ensure the document is updated to an agreed schedule.

***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 the minimum mandatory requirements that apply to this Standard. The requirements are set out in the following format:



3.1. Control Area- General Provisions

3.1.1 People Leaders oversight & responsibilities

All People Leaders **must**:	
AUS-010 *[new]*	With immediate effect, inform the Staff under their supervision about Acceptable Use and Rules of Behaviour requirements (i.e. applicable controls of this Standard).
AUS-020 *[prev. ISA-071]*	Ensure that Staff under their supervision understands the Acceptable Use and Rules of Behaviour requirements by, if required, providing them with guidance

	regarding the applicable controls of this Standard.
AUS-030 *[new]*	Report any identified non-compliance with Acceptable Use and Rules of Behaviour requirements in line with existing Group procedures. *[Reference: Sections 4.2 "Reporting Non-Compliance" & 4.3"Breach of this Standard".]*

3.1.2 General Provisions for All Staff

All Staff **must**:	
AUS-040 *[new]*	Read and comply with Acceptable Use and Rules of Behaviour requirements (i.e. applicable controls of this Standard) and always follow Group Code of Conduct when using Group's Information Technology resources and handling Group's Information. *[Reference: Group Code of Conduct]* *[Important notice: Breach of the Code of Conduct and/or the policies and procedures may lead to disciplinary action under relevant procedures and may result in dismissal without notice or compensation.]* *[Keynote: Compliance with this Standard is vital for driving healthy Risk Culture. Please refer to paragraph 2 of ERMF.]*
AUS-050	Exercise good judgment regarding appropriate use of Group's resources in accordance with Group's policies, standards, and guidelines.
AUS-060 *[new]*	Promptly report suspicion or occurrence of unauthorised activities breaching the Acceptable Use and Rules of Behaviour requirements (i.e. requirements of this Standard) following the incident reporting guidance. *[Reference: Staff must report any loss, compromise, or unauthorized use of information and other Group's resources immediately upon discovery or detection, in accordance with Guide: How to report an incident.]* *[Keynote: For more information regarding Personal Data Breach incidents, please refer to Group Privacy Standard.]*
All Staff **must**:	
AUS-070 *[new]*	Be accountable for any use made of their accounts, logon IDs, tokens or Group devices under their care (unless a compromise of aforementioned asset(s) is reported or identified). *[Keynote: Any suspicious activity or misuse (once identified) of the account(s), logon credentials, Group devices, etc. must be reported without undue delay, in line with the instructions from AUS060 or section 3.7 "Control Area: Incident reporting & handling"]*
AUS-075 *[prev. multi.* *ISA-081]*	Complete all mandatory Information and Cyber Security trainings as assigned (via elearning or other Group learning solutions) in line with defined schedule and: 1) communicated by People Leader OR 2) via Groups communication channels (such as email communication).

3.1.3 Monitoring Practises

All Staff **must**:	
AUS-080 *[new]*	Consider they may be monitored, recorded, and audited while accessing Group computers, networks, e-mail, or any other IT Resources. *[Key information:* *For security, Compliance, Investigatory, Legal and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic as per applicable policies and standards.* *Monitoring includes the monitoring of electronic communications such as emails and instant messages whether sent from fixed or mobile equipment and including communications over third party instant messaging programmes, social media services or any other services which enable employees and contractors to send and receive electronic communication, internet access/use, telephone monitoring which includes listening in to calls in real time and reviewing call logs for traffic data and location data, numbers dialled and time spent on calls, monitoring of the use of printers, scanners or similar devices, video and audio monitoring, CCTV and monitoring of access to buildings through access cards or similar devices and mechanisms, in-vehicle monitoring or monitoring through information obtained from third parties.* *Monitoring and recording may take place without further notice or warning and consider any use of the Group's Systems for the purpose set out in the Notice on the Monitoring of Staff Electronic Communications, ensuring that such Group Systems are being used lawfully and appropriately and that the Group's policies and procedures are being complied with.]* *[Reference: Group Privacy Standard.]*
AUS-090 *[new]*	Use Group's Information Technology resources with the understanding that such use may not be private, is not anonymous, and may be subject to disclosure under the applicable regulation of legal authority. *[Key information: Group security monitoring systems and their authorized personnel have the right to monitor, audit, review, block, and log All Staff activities.]* *[Reference: Group Privacy Standard.]*

All Staff **must**:	
AUS-100 *[new]*	Never execute any monitoring or recording activities (such as casual reading of email messages to other recipients or recording conversations) except: 1) as authorised in the official duties and with formal agreements, for example. monitoring and reviewing other Staff activities in the context of internal of external investigations, Legal Investigations or recording conversations or meetings by appointed Staff members,
All Staff **must**:	
	2) recording the meetings with the use of available tools and solutions (such as an option to record Teams meeting) if with prior notification (i.e. mentioning the recording at the start of the call/meeting).

	[Keynote: Recording meetings, conversations and other Staff activities with the use of unsolicited devices or software is strictly prohibited.]

3.2. Control Area- Information Security & Handling Requirements

3.2.1 General Information on key controls objectives

Information classification is a fundamental step for accurate and effective information protection. By classifying and labelling Information, we ensure adequate protection mechanisms during the whole information lifecycle.

Information must be labelled with a 'classification' based on levels of Confidentiality, to determine how to handle that Information accordingly. There are four Confidentiality Classifications labels: Restricted, Confidential, Internal, Public. Details on the classification labels are outlined in section 7.1 "[AUS-AP-010] Table 1 – Confidentiality Classification Labels".

Information classification (as based on the classification labels) cannot be confused with Technology Assets and Information Assets classification, which is Group Risk Assessment Matrix aligned and defined by the respective Owners with the use of applicable methodologies

3.2.2 Information classification & labelling

All Staff **must**:	
AUS-110 *[prev. INC-170]*	Classify and label all Group Information (includes: all types of electronic and nonelectronic Information, for example: emails, files, paper documents) in line with their sensitivity level and with the use of the Group approved labelling scheme as defined in section 7.1 "[AUS-AP-010] Table 1 – Confidentiality Classification Labels". *[Note: Information classification must be defined in line with the guidelines defined in sections 7.1 "[AUS-AP-010] Table 1 – Confidentiality Classification Labels" &* 7.2 *"[AUS-AP-020] Table 2 – How to Classify the Information".* *Every document and email message must be classified and labelled. Pre-embedded tools must be used to select and apply required label. In cases where the tools cannot be used, a label can be added manually (as a watermark or tag in the document footer/header).]*
AUS-120 *[prev. INC-190]*	Review all classified and labelled Information they are responsible for, and reconsider if its classification and label is still appropriate: 1) when the document change (including change of its contents or type of the Information included), 2) upon a change of the Information classification.
AUS-130 *[new]*	Take due care and consult People Leaders regarding any doubts or difficulties when assessing the sensitivity of Information, to ensure the Information is classified and labelled correctly.

All Staff **must**:	
AUS-140 *[new]*	Act with integrity, by never intentionally applying incorrect classification labels to Information they handle. *[Note: Incorrect classification labels may be applied in an attempt to circumvent data protection mechanisms or avoid applying required controls when handling the Information. Such activities, however, are in scope of data leakage prevention monitoring and may be investigated when identified.]*

3.2.3 Information protection & handling requirements

All Staff **must**:	
AUS-150 *[prev. INH-060* *DLP-360]*	Understand and be aware of the classification of all Information that is being processed, stored, transferred, or removed, i.e. ensure that: 1) it is labelled correctly and in accordance with AUS-110 and AUS-120, 2) it is protected and handled securely by applying controls corresponding with the Information classification, as per the requirements of this Standard, 3) all doubts and concerns regarding the Information classification and handling are discussed with People Leader. *[Reference: AUS-110]*
AUS-160 *[prev. INH-100* *INH-120* *INH-150* *INH-160]*	Protect Group's Information regardless of media or format, from disclosure to unauthorised persons or groups. This includes, but is not limited to: 1) encrypting electronic Information: a. at rest (stored on laptops or other computing devices) and b. during transit (transmitted via email, attachments, uploading information to websites, media, etc.) in line with its classification label, as defined in section 7.3.2 "[AUS-AP-040] Table 4 – Electronic Information protection requirements", 2) encrypting or digitally signing information in cases when its Integrity must be protected, 3) handling information in line with its classification label, as defined in section 7.3.1 "[AUS-AP-030] Table 3 – Non-Electronic Information Protection & Handling Requirements", 4) secure disposal of electronic media and papers when no longer needed, in accordance with the Group Record Keeping Standard requirements, 5) only providing Group Information to those with a Business 'Need to Know', i.e. the information is essential to discharge their duties and whose possession of such information will not give rise to a conflict of interest or appearance of misuse of the information. *[Keynote: If Information or document is a subject to the Preservation Holds ("PHs"), as per the Group Record Keeping Standard, it cannot be destroyed, or modified and must comply with the direction given by the Function issuing the preservation holds (such as Group Legal, Tax, etc.)].* *[Reference: Group Record Keeping Standard]*
AUS-170 *[prev. DLP-*	Use only Group's approved encryption mechanisms (i.e. solutions and software available on end-user devices) to ensure required protection is applied for

360]	Group electronic Information (see AUS-160). *[Important note: Pre-embedded tools must be used to select required label and apply encryption. In cases where the tools cannot be used to encrypt Information, Information can be protected via password protected file or archive (such as zip, rar, etc) – see* AUS-350*].* *[Reference: Encryption Guide in Handling Information.]*

All Staff **must**:	
AUS-180 *[INH-365]*	When protecting files with password (see AUS-170), use passwords that, at minimum: 1) are at least 12 characters long, 2) contain numbers, 3) contain lower case letters, 4) contain upper case letters, 5) include special characters like “+”, “#”, “$” or others, 6) are not sequential (ascending or descending), 7) are not dictionary words, 8) are different from the passwords already used (for protecting other files). *[Example of files: Word, Excel, PDF, zip.]*
AUS-185 *[new]*	When protecting files with password supply the password upon request of authorised personnel (e.g Group Legal). *[Note: Authorised personnel is any personnel approved or assigned by the Group to perform a specific type of duty or duties such as monitoring and reviewing other Staff activities in the context of internal of external investigations, Legal Investigations, etc.]*
AUS-190 *[new]*	Always disseminate passwords (used for information protection – see AUS-170) and encryption keys through off-channel communication/media (e.g., via text message, in person, or phone call – a different channel than the channel used to send the information protected with the key/password) AND store password and encryption keys separately from encrypted files, devices and data when sending or transporting encrypted media. *[Note: encryption is considered an effective protection measure only if the password/key used for this encryption is not disclosed. Keeping encryption keys/passwords together with the encrypted Information or sharing them using the same communication channel (as for encrypted message) is considered as a negating the encryption. Keys could be intercepted together with the encrypted Information and used for decrypting it.]*
AUS-200 *[new]*	Only access Information necessary to perform job functions and only use such Information for the purposes for which it was collected and in accordance with all applicable handling and protection requirements. *[Keynote: Please refer to Group Conflicts of Interest Policy for further content*

	regarding information segregation and physical segregation and Information Walls.]
AUS-210 *[prev. INH-080* *INH-090]*	Always process, store, or transfer any Group Information with the use of Group approved Information Technology resources (such as systems, devices, communication channels, software & services). *[Keynote: Group approved/authorised Information Technology is any software, device or solution which Group provides to Staff by either:* - *deploying those on Group issued devices (such as laptops, PCs and other Mobile Devices),* - *delivering though Group web-services,* - *providing based on Staff request as per the Service Catalogue defined, including BYOMD.]*
AUS-220 *[prev. UDS-150]*	Store documents and other files in Storage Elements that provide access only to authorized Staff/users, i.e. if a document is not intended to be shared widely, make sure that the Storage Element access is restricted the users authorised to access the document. *[Note: Storage Elements is an unstructured Information container (as delivered thought group IT Resources, such as shared network drive or SharePoint folder/list, Teams channels, etc.]*
All Staff **must**:	
AUS-235 *[prev. PCD115]*	Never store customer payment card information e.g. Primary Account Number (PAN) locally in their Mobile Devices. *[Note: Includes the mail pst files.* *PAN stands for **p**rimary **a**ccount **n**umber assigned to payment card, simply the card number.]*
AUS-240 *[prev. INH-070* *INH-075]*	Never: 1) process, store, or transfer any Group Information, classified: ‘Restricted’, ‘Confidential’ or ‘Internal’, outside the Group without obtaining prior authorisation from People Leader or without authorisation in the formal duties, 2) store Group Information in unauthorised devices/services (i.e. other than devices issue by Group) or other unsecure physical or electronic locations or external public folders, 3) take pictures or recordings of other than Public Group Information without obtaining prior authorisation from People Leader. *[Note: this requirement is applicable to both Electronic and Non-Electronic Information and all communication channels.* *Information can only be stored with onboarded third parties or other authorised external bodies that are cleared to hold our data.]*
AUS-245 *[prev. INH-390]*	Never access any electronic Group Information from personally owned devices or personal Information from Group IT equipment without your People Leader approval. *[Reference: BYOMD – see section* 3.5.4 *“Employee owned Mobile Devices used for business purpose (BYOMD)”]*

All Staff **must**:	
AUS-250 *[new]*	Never knowingly or willingly conceal, remove, mutilate, obliterate, falsify or destroy Group Information. *[Important note: Information removal/destruction in the context of this control considers the removal of the information other than authorised or in cases when the information must be destroyed as no longer needed or removal is mandated by applicable regulations]*
AUS-260 *[prev. DLP-360]*	Never attempt to access or access any Group's Information for which they do not have express authorisation.

3.2.4 Information sharing

All Staff **must**:	
AUS-270 *[prev. INH-280]*	Verify an identity of external recipient of Group Information classified as 'Restricted' or 'Confidential' through off-channel communication/media. *[Note: Off-channel communication refers to a separate communication channel, i.e. channel other than the one used for communication initiation. The objective is to mitigate the risk of information disclosure to unauthorised parties due to phishing or other types of social engineering attacks. Such communication must be via authorised channels, not private communication.]* *[Example:* *Request to provide 'Restricted' documents is received via email from external email address. Even if the request comes from a 3rd party authorised to receive the information, the accuracy of the contact details should be verified via separate channels, such as:* • *Official company web site or address book,* • *Over the phone inquiry/verification (with the prone number obtained from other sources than the email with the request.* *By simply replying to such a request, the Group could be exposed to data leakage risk, if the request was forged (to look like it came from the legitimate source.]*
AUS-275 *[prev. DLP-370]*	Prior to sharing, inspect documents, files and email threads for any information or metadata not intended for sharing and remove it. *[Note: This step is of critical importance to ensure that too much information is not shared. The most common cases of such unwanted information sharing consist of:* • *Forwarding email threads/chains with sensitive information not eligible for sharing,* • *Sending document templates with data/information not removed,* • *Sending documents such as excel files of word documents with metadata*

	(such as changes tracking or notes) or information that should be removed before sharing (such as information about clients being sent to other clients).]

All Staff **must**:	
AUS-280 *[new]*	Never share or disclose Group's Information, except as authorized in the official duties and with formal agreements ensuring all authorised third parties will adequately protect the Group information.
AUS-290 *[new]*	Never share, store or disclose Group's Information with third-party organizations or use third-party applications (e.g. DropBox, Evernote, iCloud, Gmail, WhatsApp, SFTP/FTP based solutions, etc.) unless authorised and with formal agreement (as communicated in the Group Electronic and Voice Communication Standard). *[Note: SFTP/FTP refers to (**s**ecure) **f**ile **t**ransfer **p**rotocol, i.e. any solution that uses this protocol for file exchange/sharing]* *[Reference: Group Electronic and Voice Communication Standard.]*
AUS-295 *[new]*	Never forward Group Information to their personal emails or other external recipients unless authorised by People Leader.

3.3. Control Area- Secure Working Practises

3.3.1 General Requirements

All Staff **must**:	
AUS-300 *[prev. INH-520]*	Never discuss Group Information classified as 'Restricted', 'Confidential' or 'Internal' in places where you may be overheard.
AUS-310 *[prev. INH-330]*	Properly secure all assets, including laptops, mobile devices, portable storage devices and other equipment that store, process, and handle Group information, when leaving them unattended either at the office and other work locations, such as home, hoteling space, etc. and while on travel. This includes: 1) locking workstations, laptops, placing information in locked drawer, or cabinet when leaving office desk, 2) keeping laptops and other mobile devices with you all time when in public locations, 3) closing down or hibernating laptops rather than suspending them when travelling.
AUS-320 *[prev. INH-540]*	Ensure that Digital Assistants (e.g. Amazon Alexa, Google Assist) are not present or are switched off on any Group owned or personally owned (BYOMD) IT equipment while in the office or when working and discussing Group related matters (also when working from home).
AUS-330	Never take or process photos, videos or images showing restricted office areas

[new]	or any other Group related content or Information unless considered public or authorised in the formal duties.
AUS-340 *[new]*	Never post photos, videos or images showing restricted office areas or any other Group related content or Information unless considered public or authorised in the formal duties on postable Media or other public services (such as online drives, email services, chats, etc.). *[Reference: Please review the "Employee Communication Standards" for more details regarding social media use.]*

3.3.2 Working from the Office

All Staff **must**:	
AUS-350 *[prev. INH-170* *INH-180* *INH-190]*	Ensure that Group Information is securely handled in line with applicable requirements defined in section 7.3 "Handling Non-Electronic and Electronic Information". *[Reference: 7.3* "Handling Non-Electronic and Electronic Information*]*
AUS-360 *[new]*	When working in the office, use only Group provided wire or wireless network connections.

3.3.3 Working from Home or co-working spaces

All Staff **must**:	
AUS-370 *[prev. INH-130]*	Follow the requirements for secure Information handling, as defined in section 7.3 "Handling Non-Electronic and Electronic Information" (Storage & handling outside Group premises) always when working from home or co-working spaces. *[Reference:* 7.3 "Handling Non-Electronic and Electronic Information*]*
All Staff **must**:	
AUS-375 *[new]*	To avoid the risk of session/connection hijacking, never use unsolicited or unknown opened wireless network connections/Wi-Fi spots. *[Keynote: when working outside Group premisses trusted and protected Wi-Fi connections should be used. Special caution should be executed for open and unknown Wi-Fi hotspots as they may pose certain cybersecurity threats to anyone connecting (to them)].*

3.4. Securing Access to Group's Information Technology resources

3.4.1 General Information on Access Control measures and their objectives

To ensure accountability of activities, every individual accessing the Group's IT resources must have an individual account (except in special cases such as shared/generic accounts for the operation of special services supported by a team of people). Another key important aspect is, that access to Group's IT resources must reflect one's needs based on the business duties and 'need-to-know' basis. The above objectives can only be met if:

1) access to the Group IT resources is requested and granted in line with the Group access management process and standard,
2) the account/access credentials are kept secure – in the case of unauthorised account sharing, all of the actions conducted with the account will be attributed to the individual who owns the account,
3) individuals always use access they are authorised to.

IMPORTANT NOTE: The control statements of this section refer to 'individual/personal accounts', i.e. accounts allocated to individual users. This section does not cover the special requirements for generic/shared accounts (which are defined in the Identity and Access Management Standard).

Access credentials is a combination of unique identifier and secret used to validate and prove one's identity when accessing Group's IT resources. Access credentials are issued to the authorised users to allow them accessing Group's IT resources. The identifier is usually User ID, the 'secret' could be one or combination of the below:

1) Passwords or passphrases, one-time passwords,
2) PINs or access tokens,
3) Digital certificates,
4) Digital cards or devices,
5) Biometrics,
6) Other factors, such as location or behavioural patterns.

3.4.2 User Access & Digital Identity

All Staff **must**:	
AUS-380 *[prev. IAM-570]*	Never allow others to use their account, digital identity, access credentials (such as passwords, passcodes, access cards, biometrics or digital certificates) provided by the Group to perform their official work duties. *[Note: this includes not sharing with anyone: any Individual Account's access credentials and any Generic Account's password (this includes Default and Non-Default Accounts)]*
All Staff **must**:	
AUS-390 *[new]*	Never access other users' accounts, digital identity, access credentials (such as passwords, passcodes, access cards, biometrics or digital certificates) provided by the Group to perform their official work duties; OR use credentials for which they are not explicitly authorized, attempt to capture or guess credentials, in any way attempt to gain access to an unauthorized account.
AUS-400	Always:

[prev. INH-340]	a) supervise any access to owned or under their care Group's Information Technology resources, b) ensure that such access is based on a legitimated and authorised business need, c) report any case of factual or suspected access to such resources, which does not meet the conditions as above. *[Note: Such access includes, but is not limited to: workstation (desktop, laptop), smartphone, tablet, or any other Group device.]*

3.4.3 Passwords, PINs and other Access Credentials

All Staff **must:**	
AUS-420 *[prev. IAM-580]*	Never store/safe keep/keep records of any access credentials: a) in IT resources, software, services or devices which are not Group approved, b) in a manner that may led to their exposure or misuse by unauthorised individuals. *[Note: Examples of insecure access credentials storing:* • *writing down passwords,* • *storing password or other access credentials on personal devices,* • *storing password/access credentials in external password management solutions,* • *storing passwords/access credentials in Group's IT resources not authorised for such purposes (text files kept on shared drives, MS Teams catalogues, MS Outlook archives, etc.)* • *downloading and using unauthorised software, such as password managers.]*
AUS-430 *[prev. IAM-590]*	Never reuse passwords (including passphrases) and PINs used in Group's Information Technology resources anywhere else.
AUS-440 *[prev. IAM-610]*	Report without undue delay any actual or suspected loss, theft, misuse, compromise or tampering of any access credentials. *[Reference:* Guide: How to report an incident
AUS-450 *[prev. IAM-620]*	Change any password (including passphrase) and any PIN in line with the requirements defined in Authentication Requirements Matrix Table. *[Reference: Section 7.1 "Authentication Requirements Matrix" –* Identity and Access Management Standard] *[Exception: AUS-180]*
All Staff **must:**	
AUS-460 *[prev. IAM-640]*	Ensure that: login, password (including passphrase), PIN or token is changed or reset if there is an actual or suspected loss, theft, misuse, compromise, or tamper of these credentials; initial password is changed or reset password (including passphrase); PIN or token is changed or reset in line with the

	requirements defined in Authentication Requirements Matrix Table *[Reference: Section 7.1 “Authentication Requirements Matrix” – _Identity and Access Management Standard]* *[Exception: AUS-180]*
AUS-470 *[prev. IAM-966]*	Ensure that Non-Account password used for access to Group’s Information, Information Technology resources (including IT Equipment) [for example but not limited to: password to Mobile Devices (Smartphones and Tablets only) or BitLocker] must at minimum be in line with requirements defined in Authentication Requirements Matrix Table. *[Note: Maximum Password Change Cycle is never unless you suspect a breach or breach has been confirmed.]* *[Reference: Section 7.1 “Authentication Requirements Matrix” – _Identity and Access Management Standard]*

3.4.4 Digital Certificates

Digital certificate is a form of electronic credential that proves authenticity of a user, device or service through the use of cryptography (by proving the ownership of the public key). The digital certificate is always linked to a key pair (as defined in the Public Key Infrastructure technology).

In the case that no Certificate Authority proved the authenticity of the digital certificate (by signing it) we consider such certificate as self-signed.

All Staff **must**:	
AUS-480 *[prev. DCM010]*	(When requesting a Digital Certificate) have a business need as authorised in the official duties and with formal agreements or authorised by People Leader AND Follow the applicable requirements of the Digital Certificate Management Standard. *[Reference: Digital Certificate Management Standard.* *Please note that Digital Certificates are issued for certain organisational roles, such as system administrators or developers]*
AUS-490 *[new]*	Never generate, install or use Digital Certificates without verification and approval from the Group Approved Internal Certificate Authority [ICA] team. *[Keynote: This applies to self-signed certificates or certificates issues or signed by external authorities.* *Please refer to Digital Certificate Management Standard for more details, if required.*

3.5. Control Area- Acceptable Use of Group Information Technology Resources

3.5.1 Portable Storage Devices

All Staff **must**:	
AUS-500 *[prev. INH-140 INH-310 INH-380]*	Use only Group issued, approved and encrypted Portable Storage Devices for processing Group Information.
AUS-510 *[new]*	Never: 1) copy/transfer Group information to the Portable Storage Devices except as authorised in the official duties and with formal agreements or authorised by People Leader, 2) download or transfer Group information to any non-authorised device.
AUS-520 *[new]*	Ensure that Group Information transferred to portable Storage Device is always encrypted.
AUS-540 *[new]*	Never use the Group's Portable Storage Devices for personal use.

3.5.2 Voice and Verbal Communication & Telephony and VoIP

All Staff **must**:	
AUS-550 *[prev. INH-530]*	Use telephones, conferencing, and speaker phones securely i.e. take reasonable measures to ensure you are not overheard.
AUS-560 *[prev. INH-510]*	Never leave Group Information classified as 'Restricted', 'Confidential' or 'Internal' on an answering machine or voicemail.
AUS-570 *[prev. INH-500]*	Verify the Identity of a Caller when being asked for any Group Information. *[Note: verification should be conducted though out of the band channel or with the use of challengeresponse questions/information assuring the identity of the caller.* *Upon identification of any malicious attempt an incident must be immediately reported – see* Guide: How to report an incident*.]*
AUS-580 *[prev. INH-490]*	Ensure, when sharing Group Information, that all recipients [Internal and External] of Voice and Verbal Group Information classified as 'Restricted' or 'Confidential' are only ones intended to receive such Information.

3.5.3 Group Information Systems & Group Issued Devices

All Staff **must**:	
AUS-590 *[prev. SAM236]*	If applicable, comply with any detailed or system specific directions from People Leaders and system administrators concerning access to and use of Information, Information Systems and Group owned devices.
AUS-600 *[prev. AM-260]*	Only access system utilities that are made available due to a legitimate business case.
All Staff **must**:	
AUS-610	Request any software or device:

[prev. AM-260 *SAM-234]*	1) only through the Bank's Technology Service Catalogue and Service Request Management system, 2) based on their authorised and intended business use.
AUS-620 *[new]*	Never download, install or use any unauthorised software (i.e. software other that the one mentioned in AUS-610) on Group issued Devices.
AUS-615 *[new]*	In order to ensure accuracy of the IT resources records, verify and acknowledge Group issued devices (assigned to them) as requested by People Leader or authorised Group personnel.
AUS-630 *[prev. AM-260* *SPM-240]*	Ensure that the Group IT Equipment assigned to them is available for timely deployment of relevant software updates and Software Patches by the Group. *[Note: Timely, i.e. as communicated/requested by authorised Group personnel. For cases, where deployment by Group is not possible, ensure that Software Patches are timely deployed on IT Equipment assigned to them.* *In cases where required updates or patches are not deployed in a timely manner, the device is disconnected from the Group network.]*
AUS-640 *[prev. AM-260* *SAM-230]*	Report all lost or stolen devices (or any other malicious activity suspected related to owned devices) through communicated channels and in line with the communicated operational procedures. *[Reference:* Guide: How to report an incident]
AUS-650 *[prev. SAM232]*	Ensure the corporate devices are returned upon their contract termination or when no longer in use.

All Staff **must**:	
AUS-660 *[prev. AM-260]*	Never use: 1) nonstandard software or equipment, 2) unapproved and unprotected non-Group devices, such as mobile phones that have not been officially onboarded in accordance with the Mobile Device Policy, to conduct Group business or process Group Information.
AUS-670 *[prev. AM-260]*	Act with integrity and never make unauthorized changes to information or information systems or exceed access beyond their authorisations.
AUS-680 *[prev. AM-260]*	Never insert an unauthorised Portable Storage Devices into a Group owned device.
AUS-690 *[prev. AM-260]*	Act with integrity and never circumvent (or attempt to circumvent) security measures. This includes (but is not limited to): 1) downloading, installing or executing utilities such as password crackers, packet sniffers, or port scanners that reveal or exploit security weaknesses, 2) accessing system utilities to change or disable security components (such as

	DLP or AM agents, local firewall settings) of the Information System or device.

3.5.4 Employee owned Mobile Devices used for business purpose (BYOMD)

All Staff **must**:	
AUS-700 *[prev. MDS-220]*	Prior to using personally owned Mobile Devices to access Group's Information or Information Systems: 1) obtain the approval of your People Leader, 2) request device enrolment for the corporate services via formal Service Request. 3) enrol the Mobile Device in line with the instructions provided. *[Reference: Bring Your Own Device (BYOMD) – Technology Catalogue Request]* *[Note: Mobile Devices – devices include, but are not limited to Laptops, Tablets, Smartphones, Wearable Technology.* *Not all countries and Mobile Devices are eligible for enrolment.]*
AUS-710 *[prev. MDS-230]*	Protect personally owned Mobile Devices from malware and clean any malware found on the Device. *[Note: This requirement is applicable only to BYOMD laptops.]*
AUS-720 *[prev. MDS240]*	To avoid Group's Information disclosure or unauthorised use, never allow others to access or use your Mobile Device. *[Note: this applies only to the devices which are considered BYOMD]*
AUS-730 *[prev. MDS250]*	Apply Software Patches in line with manufacturer and software authors recommendations and without undue delay. *[Note: Unless explicitly dissuaded doing so by Group Technology via official communication.]*
AUS-740 *[prev. MDS260]*	Request that Group Information is wiped securely from the BYOMD by unenrolling it, before the device is transferred of out their control, for example is disposed or sold or returned to a supplier under warranty, lease, maintenance or failure, or when you plan to replace, upgrade, decommission or re-use. *[Reference: BYOMD.]*
AUS-750 *[prev. MDS270]*	Not jailbreak (IOS) or root (Android) [for smartphones and tablets] or tamper with Operating System or security configuration [for laptops, smartphones and tablets].
AUS-760 *[prev. MDS280]*	Immediately report any loss, theft of, or unauthorised access to the Mobile Device in accordance with the Group's Information Security Incident reporting procedure. *[Reference: Guide: How to report an incident]*
AUS-770 *[prev. MDS290]*	Immediately report to the Group (in accordance with the Group's Information Security Incident reporting procedure.) if a Mobile Device becomes subject to any court proceedings (whether related to the Group or not) or if a Mobile Device is required to be accessed or confiscated by any legal requirement, governmental or regulatory body. *[Note: Unless prevented from doing so by any legal requirement, governmental*

	or regulatory body.] *[Reference:* *Guide: How to report an incident]*

3.5.5 Email, Internet, Instant Messaging & Other communication channels

All Staff **must**:	
AUS-780 *[prev. INH-290* *INH-440]*	Prior to sending emails and electronic messages ([Internal and External] classified as 'Restricted' or 'Confidential' or containing any Group Information classified as 'Restricted' or 'Confidential'): 1) review the list of recipients to ensure it includes only ones intended to receive such emails, 2) verify the recipients added through the auto-fill option to ensure the correct names were selected. *[Keynote: It is recommended to add the recipients individually – avoid using email distribution lists or shared mailboxes, to ensure the recipients list explicit.]*
AUS-790 *[prev. INH-300]*	Ensure encryption is in place for sending emails and other electronic messages internally and externally, where required, i.e. according to the classification of the Information contained. *[Reference:* 7.3.2 *"[AUS-AP-040] Table 4 – Electronic Information* protection *requirements"].* *[Note: In cases where encryption cannot be applied, different communication channel should be used.]*
AUS-800 *[prev. AM-260]*	To minimise the risk of successful phishing attempt or malware infection, assess possible threats and exercise caution when receiving unsolicited emails (or other electronic messages) from both external and internal senders, by: 1) verifying the sender address and validity, 2) avoiding clicking links or opening/downloading attachments, 3) proactively and promptly reporting any suspicion of malicious attempt by using the 'Report as Phishing' button in the MS Outlook client. *[Note: Phishing attempts are becoming more sophisticated. It is important to keep learning about emerging phishing methods and staying vigilant to avoid falling prey. Visit CyberSpace for more information and useful tips.]*
AUS-810 *[prev. AM-260]*	To minimise the risk of successful phishing attempt, malware infection, data exfiltration and data loss, execute caution when browsing internet sites by: 1) avoiding visiting unknown sites or sites to which references were provided in unsolicited emails or messages, 2) limit the usage of internet to work related purposes, 3) avoiding downloading, installing or executing files downloaded from external sites.

3.5.6 Personal Use

All Staff **may**:	
AUS-820 *[new]*	Occasionally and incidentally use (for personal purposes) Group email, internet or instant messaging) if it does not: 1) interfere with their work or IT resource's ability to perform Group's objectives and mission, 2) breach the requirements of this Standard, 3) breach Group's internal regulations (including Code of Conduct), 4) breach relevant regulations and applicable laws. *[Note: Personal activity (on the Group's Information Technology resources), will be processed in line with the Groups Privacy notice and may be subject to monitoring or legal disclosure – see AUS-080 for more details.]*

3.5.7 Prohibited Use

All Staff **must:**	
AUS-830 *[new]*	Never use Group's IT resources to access, share, store or process any information or conduct any activity that: 1) violates internal regulations or applicable laws, 2) is considered as obscene, discriminatory, harassing, embarrassing or offensive to other Staff members, individuals or the Group, 3) is considered pornographic, racist or malicious, 4) promotes or maintains private or personal business, 5) support unlawful or unethical activities, such as gambling, fraud or hacking, 6) may degrade the performance of Group's IT resources, deprive an authorized user access to resources (or interferes with the legitimate activities of the user), or obtain extra resources beyond those allocated, 7) cause congestion, delay, or disruption of service to information resource (such as sending chain letters via email, playing streaming videos, games, music, etc.) 8) violates other persons rights or privacy, 9) involves using, storing or distributing unauthorized, copyrighted or other intellectual property in a manner that could be considered intellectual property infringement. *[Exception: Does not apply to activities if conducted in line with definition as per AUS-100, point (1).]*

3.6. Control Area- Secure Disposal of Group Information & Devices

3.6.1 Information Disposal

All Staff **must**:	
AUS-840 *[prev. INH-200]*	Securely dispose Group Information classified: 'Restricted', 'Confidential' or 'Internal' commensurate with its classification. *[Keynote: If Information or document is a subject to the Preservation Holds*

	("PHs"), as per the *Group Record Keeping Standard, it cannot be destroyed, or modified and must comply with the* *direction given by the Function issuing the preservation holds (such as Group Legal, Tax, etc.)].* *[Reference: Group Record Keeping Standard]* *[Reference: AUS-850 to 860].* *[Reference: 7.3 "Handling Non-Electronic and Electronic Information]* *[Note: If Information is no longer required, it must be permanently deleted.]*
AUS-850 *[prev. SDD220]*	Never dispose of paper wastes outside the Group offices. *[Keynote: This also applies when working from home or non-Group owned sites, such as coworking spaces. Bank printed materials used outside of Group offices, are required to be brought back into the Group Offices for disposal in line with AUS-860.]* *[Reference: AUS-860]*
AUS-860 *[prev. SDD-230* *SDD-240]*	Always dispose printed documents/hard copies with the confidential waste bins located in the office and use: 1) the confidential waste bins or shredders provided when disposing of printed documents containing Internal or Confidential information, 2) a cross-cut shredder when disposing of printed documents containing Restricted information. *[Reference: AUS-840]*

3.6.2 Disposal of Group Issued Devices

All Staff **must**:	
AUS-870 *[prev. INH-410* *SDD-120]*	Ensure that all Group owned IT equipment is returned to local technology / IT Support team if it is not to be reused, i.e.: 1) upon contract termination, 2) in the case of the equipment's malfunction or failure, 3) when the equipment is required to be replaced, 4) in cases where the equipment is to be handed over to other Staff member(s). *[Keynote: If Information or document is a subject to the Preservation Holds ("PHs"), as per the Group Record Keeping Standard, it cannot be destroyed, or modified and must comply with the direction given by the Function issuing the preservation holds (such as Group Legal, Tax, etc.)].* *[Reference: Group Record Keeping Standard]* *[Note: The requirement refers to all type of electronic devices, such as laptops, PCs, Portable Storage Devices and other Mobile Devices.* *It is of a key importance ensuring that unused devices and IT equipment is handed back to respective technology departments so they can be handled with all relevant ICS requirements applied.* *Such devices disposal cannot be under Staff members discretion, as this may lead to significant ICS risks, such as information leakage, identity misused, etc.]*

AUS-880 *[prev. SDD130]*	Only reuse Portable Storage Devices and IT equipment when all data have been securely erased by relevant technology department.

3.7. Control Area- Incident reporting & handling

All Staff **must**:	
AUS-890 *[prev. SIR-060]*	Immediately report any actual or suspected Information and cyber security incidents once an individual becomes aware of them or suspect any abnormality in line with the Group approved Process. *[Reference: Guide: How to report an incident]*
AUS-900 *[prev. DLP-370]*	Take timely actions, as requested and instructed by People Leaders or individuals representing Group cybersecurity incident response functions, to ensure appropriate and timely response to ICS events and incidents.

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. [AUS-AP-010] Table 1 – Confidentiality Classification Labels

7.1 [AUS-AP-010] Table 1 – Confidentiality Classification Labels

Confidentiality Labels	Criteria and Examples
Restricted Note: This would usually but not always be Information rated as a '5'for Confidentiality in the Information Asset Register	This is Information which if disclosed the consequences to the Group, its Clients, Customers, Business Partners and Staff would be 'Severe'. Distribution is only allowed for named individuals and groups. For Example: • Strategic plans • Board papers • PINs and passwords Restricted Information includes inside Information. This is Information which • is of a precise nature • not generally available • relates, directly or indirectly, to one or more issuers or to one or more financial instruments; and would, if generally available, be likely to have a significant effect on the price of those financial instruments or on the price of related derivative financial instruments *Note: Employees must contact the Group Company Secretary immediately if they think they are in possession of inside information relating to the Group.*
Confidential Note: This would usually but not always be Information rated as a '4' For Confidentiality in the Information Asset Register	This is Sensitive Information which should be protected from public disclosure, because if disclosed the consequences to the Group are likely to be at a minimum 'Material'. Confidential Information is considered sensitive within the company and is intended for use only by a limited number of Group Staff, and only be sent externally upon authorisation. Sensitive Information: Information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction. For Example: • Product Design & Development Details • Bank Statements/Investment & Transaction Details Example Scenarios: 1. Financial Crime Risk (FCR) information collected about potential regulatory breaches or criminal offences by customers or staff (e.g.

	money laundering or insider dealing, business plans); 2. Information subject to the Transactional Conflicts and Information Wall (TCIW) procedures which are a subset of the Group's conflicts of interest policy; 3. Details of non-public contractual arrangements between the Group and a supplier subject to a non-disclosure or confidentiality agreement relating to the provision of products and services to the Group (e.g. pricing information or business plans); 4. Commercially sensitive Information which is proprietary and valuable information not available in the public domain, such as consultancy tools and methodology, information subject to licensing restrictions on use and disclosure by the Group and price/customer lists.
Internal Note: This would usually but not always be Information rated as a '3' or a '2' for Confidentiality in the Information Asset Register	This is information which should be protected from public disclosure, because if disclosed the consequences to the Group are likely to be at a minimum 'Moderate'. It should be accessible only by Group Staff who have a legitimate reason to access the information, and only be sent externally upon authorisation. For Example: • Internal business plans • Newsletters • Internal policies & procedures • User manuals • Business Continuity plans
Public Note: This would usually but not always be Information rated as a '1' for Confidentiality in the Information Asset Register	This is information which is intended for distribution outside the Group with no legal restrictions on access or usage or Information which is already in the public domain (as either coming from external sources or already authorised to be in the public domain). Unauthorised disclosure of the data would result in a 'Low' or no impact to the Group. For Example: • Press releases • Advertisements • Job Postings [once finalised and posted]

7.2. [AUS-AP-020] Table 2 – How to Classify the Information

If the Answer is 'Yes' to the following Questions:	Confidential Classification
Is the Information suitable for posting to a public website?	Public
Is the Information suitable for internal websites [the Bridge]	Internal
Does the Information contain Personal or other Business sensitive Information that is intended for a limited audience?	Confidential
Does the Information contain sensitive data that if disclosed would cause an impact to the share price?	Restricted

7.3. Handling Non-Electronic and Electronic Information

7.3.1 [AUS-AP-030] Table 3 – Non-Electronic Information Protection & Handling Requirements

Information medium and activity	Internal	Confidential	Restricted
Printed Information sent inside the Group	• Seal in packaging /envelope. • Label the classification: Internal. • Address to a named person. • Send via the internal mail system.	• Seal in packaging /envelope. • Label the classification: Confidential. • Address to a named person. • Send via the internal mail system.	• Do not use the internal mail system. • Hand-deliver or send using an approved courier and confirm receipt.
Printed Information sent outside the Group	• Seal in packaging which is nontransparent. • Address to a named person. • Include return address.	• Seal in packaging which is non-transparent and tamper evident. • Do not indicate the classification or the nature of the information on the outer packaging. • Address to a named person. • Include return address. • Use an approved courier	• Seal in packaging which is non-transparent and tamper evident. • Do not indicate the classification or the nature of the information on the outer packaging. • Address to a named person. • Include return address. • Use an approved • courier and confirm receipt. • The delivery must be able to be tracked (e.g. sent by registered

			mail). • Process must be • in place if the delivery is unsuccessful, tamper seal is broken, and/or the asset is missing/stolen.
Storage and handling within Group premises	• Remove the Information from whiteboards and flipcharts when no longer needed. • Collect all Group Information from photocopiers and printing machines immediately after printing. • Securely store the Information in locked storage and never leave it unattended whether this is inside or outside Group premises.		• Limit printing the Information and collect all Group Information from photocopiers and printing machines immediately after printing. • Lock away in a secure location when not in use • Securely destroy hard copies (by using cut shredders) immediately when no longer needed • Avoid placing on whiteboards and flipcharts and remove Information when no longer needed
Storage and handling outside Group premises	• Keep with you at all times in public places and lock away in a secure location when not in use. • Do not read in public places where you can be overlooked.	• Do not access Information in public that could lead to unauthorised disclosure. • Do not print when outside Group workspaces or with the use of non-authorised printers, such as printers directly connected to the user device or printers not connected to the Group's networks and printing services, (upon review and approval of the request by the HICS for exceptions to the standard). • Segregate Group Information from your personal Information on your personal portable and handheld devices.	

		• Do not copy Group Information to a personal portable and hand-held device or use removable media without authorization. • Do not dispose of Group Information outside of Group Premises. • Ensure that Digital Assistants (e.g. Amazon Alexa, Google Assist) are not present or are switched off.
Faxing	• Confirm validity/accuracy of the fax number using out of band channel. • Verify that the recipient can receive the fax prior to sending Group Information, i.e. can collect the information immediately after receiving. • Ensure that the Confidentiality label and Information recipients are on the cover page.	• Prohibited

7.3.2 [AUS-AP-040] Table 4 – Electronic Information protection requirements

Information Confidentiality Classification	Electronic Data Transfer (All Staff Only)		
	At Rest (user applied*)	In Transit Internal (user applied*)	In Transit External (user applied*)
Restricted	Encrypt	Encrypt	Encrypt
Confidential Personal Data & PCD	Encrypt	Encrypt	Encrypt
Confidential	Encrypt	Encrypt	Encrypt
Internal	Encryption not required	Encryption not required	Encryption not required
Public	Encryption not required	Encryption not required	Encryption not required

In the case of document/data handling through Group provided Information System the above can be delivered by the Information System functionality. In such case please follow specific requirements/guidance provided by
the Information System Owner.

The above requirements can be replaced by target solution providing equivalent data protection. In such case
T&E/CSS shall be contacted to explore possible options.

*Encryption as added/applied by user:

1) via embedded toolset, such as outlook email encryption

2) via Group approved solutions, such as office documents Information Rights Management, encrypted zip archives, etc.

Important note: Embedded solutions are mandated for use in email and web.

Personal Data – as defined by Group Privacy.

PCD – Cardholder Data/ Payment Card Data is all personally identifiable data about the cardholder (i.e. account
number, expiration date, data provided by the cardholder, other electronic data gathered by the merchant/agent, etc.).

7.4. Appendix A – Version Control Table

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISRO ICS Policy	First release (ICSCR-18Feb2022-1): 1. All Staff & People Leaders related controls relocated from applicable ICS Standards: 2. New control areas covered	Material	Paul Hoare Head, ICS Policy and Best Practice	1.0	25-Jul-23	31-Jul-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	1.1	04-Dec24	16-Dec-24

8. 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	1.1	04-Dec24	16-Dec-24