Applications Security Standard

Version No	2.3
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	Arti Singh
Document Contact Job Title	Assoc Dir, ICS Standards
Business Scope	All Businesses
Function Role	All Functions
Geography Scope	GLOBAL
Approval Date	15/11/2024
Effective Date	25/11/2024
Next Review Date	24/11/2025

Table of Contents

Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Arti Singh	Applications Security Standard	Non-Material	Jamie Michael Cowan	2.3	15/11/2024	25/11/2024

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

1. INTRODUCTION AND PURPOSE

This Information Security Standard defines the minimum-security requirements for the Group Applications.

Defining security requirements is a critical part of an Application development in order to prevent insecure solutions from being deployed to Production. The security requirements along with any Privacy specific requirements are generally a part of both functional and non-functional requirements and they need to be integrated and verified in different stages of the development lifecycle.

Without the early integration of the security requirements, an organisation will have to undergo a significant expense at a later stage for remediation of any security and/or privacy lapses.

Applications developed and deployed with an early integration of these requirements are less susceptible to security vulnerabilities and hence a secure Application is put in place, reducing the Group exposure to threats.

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 internal or external threats ,
- Disclosure of Information caused by internal or external threats
- Disruption to business operations caused by internal or external threats .

1.2. Scope

This Standard must be read, and controls deployed in conjunction with all other applicable ICS Standards.

The Standard is mandatory and applies to the Group businesses, functions, countries, and regions except where explicitly prohibited by local Law or Regulation [assessed as per section 4.2. Reporting Non-Compliance].

Note: *In case of any Country specific LRM requirement, the approach defined in ERMF (Chapter Eleven, Part B, section 4.2 "Country-level Host Regulatory Obligations") must be followed.*

The Standard covers all Group Information Assets which are processed and or used by the Group's Information System [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 [SBIA] ratings, they are applicable only to those rated Systems. All other Control Statements apply to all Systems regardless of ratings and hosted environments [Production or Non-Production unless stated otherwise].

The Systems owned and or managed by the Third Parties [including Cloud Systems, Vendor Systems, Regulatory Systems, Self Service Terminal [SST] and similar], must additionally refer to the ICS Standards for Security in Interactions with Third Parties and Secure Configuration Management.

Please note, any Systems which are deemed as 'Standalone Machines' must be assessed using the Security – Business Impact Assessment [S-BIA] and controls must be applied accordingly as per the applicable ICS Standards

2. ROLES AND RESPONSIBILITIES

All Staff

All Staff are responsible for the safety of Group Technology Assets under their care, the security of Group Information allowed for accessing via the Technology Assets and for compliance with the applicable Control Statements defined in this Standard.

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.

CISO ICS Standards & Controls

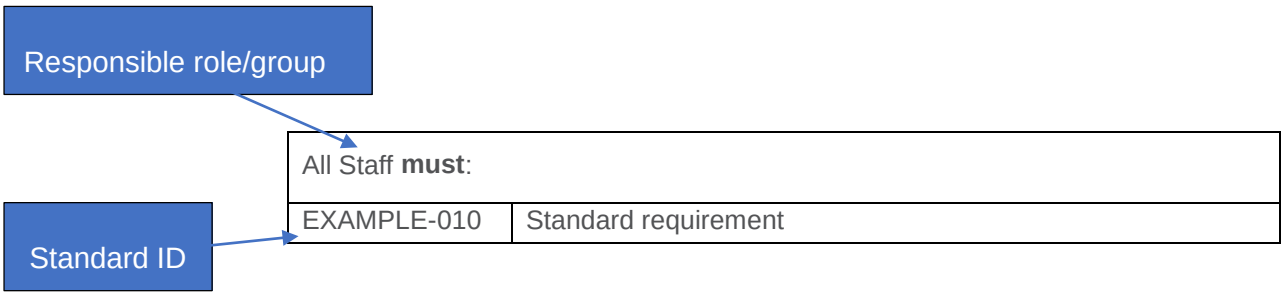
The CISO is the owner of this Information Security Standard and will ensure the document is updated at least annually.

***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 - On-boarding

Information System Owner **must**:	
AS-010	Ensure that Applications and Information Systems onboarded to the Group inventory have documented: a) types and classification of Information Assets that will be handled by them; b) types of System that will handle Information Assets; c) physical environments and locations where they are located. physical environments and locations where they are located.
AS-020	Ensure their Applications are security assessed for criticality and assigned

	ratings. *[Reference: Security Business Impact Assessment [S-BIA] Methodology Definition & Scope]*

3.2. Control Area - Secure by Design

Information System Owner and/or Technology Infrastructure Owner **must**:	
AS-030	Design the Applications in conjunction with Group's ICS Standards requirements (including but not limited to Legal, Regulatory and Mandatory [LRM], Privacy protection requirements) during all stages of the Application lifecycle.
AS-040	Document and maintain the following for all Application types: a) security solution architecture including all connection points; b) non-functional security requirements; c) minimum security baseline requirements; d) security specific contractual requirements, if any; and e) business requirements from Information Asset/System Owner.

3.3. Control Area - Security Architecture

Information System Owner and/or Technology Infrastructure Owner **must**:	
AS-050	Follow architecture principles such as: a) Resilience to common & well-known Application attacks/threats. b) Granting only the minimum privileges necessary to a user or function (Principle of least privilege); c) All Application and data access events should be traceable to an initiator (Accountability); d) No single security component failure should result in the compromise of an entire environment (Defence in depth); and e) Failure of a component must not lead to a lower state of security (Fail securely). *Note: Security components e.g., Authentication, Authorisation, Logging.*
AS-060	Enable Applications with the following protection measures: a) Spoofing Protection; b) Tampering Protection; c) Repudiation Protection; d) Information Disclosure Protection; e) Denial of Service/Distributed Denial of Service [DoS/DDoS] Protection; f) Elevation of Privileges Protection; and g) Key threats. *[Reference: Appendix Additional Protection measures]*
AS-070	Use the Group approved technology products and components in development to minimise security risks. *[Reference: Technology products and components inventory]*

AS-080	Ensure the underlying Technology Infrastructure of the Applications is securely configured and hardened. *For Example, Technology Infrastructure is configured secure and placed in a secure zone especially for external facing Applications. [Reference: ICS Network Security and ICS Secure Configuration Standard]*
AS-090	Ensure that Non-Production environment: a) is separated from Production environment; b) is impact assessed through S-BIA; c) has relevant (corresponding with its classification/impact rating) ICS controls deployed; d) does not contain a source of any content or objects that are migrated to production environments. *Note: In the case the impact is not evaluated independently for the non-prod environment, the environment inherits the rating from current or target production instance.* *Note: For Vulnerability Identification Frequency and Vulnerabilities Classification and Remediation (all in Calendar Days) refer to ICS Vulnerability Identification and Management Standard.*

3.4. Control Area - Build and Development

3.4.1 Baseline Security Requirements

Information System Owner and/or Technology Infrastructure Owner **must**:	
AS-100	Ensure Staff involved in Application development have the knowledge required to develop securely. *[Reference: Information Security Awareness and Training Standard]*
AS-110	Ensure development in Production is prohibited.

Information System Owner **must**:	
AS-140	Ensure that for acquired software: a) security requirements are identified; b) suppliers provide assurance that they can meet security requirements (for example: by producing results of penetration tests, Code Security Review and Vulnerability Identification and Management [VIM], demonstrating adherence to standards, and providing an effective method for delivering software patches/fixes); c) a high priority is placed on reliability in the selection process; d) contractual terms are predefined in line with identified ICS requirements, agreed with suppliers and made formally binding. *[Reference: ICS Standard Security in Interactions with Third Parties]*

Information System Owner **must**:	
AS-150	Reduce the risk of potential security weaknesses in Software by: a) obtaining and reviewing external assessments from trusted sources (for example: external auditor's opinions and specified security criteria, such as the Information Technology Security Evaluation Criteria [ITSEC], Common Criteria [CC] and Federal Information Processing Standards [FIPS]); b) identifying security deficiencies (for example: by detailed inspection, Malware testing, Vulnerability scanning, reference to published sources, or by participating in user/discussion groups); c) if possible, addressing any security weakness found, by applying a countermeasure and raising a request/support ticket with vendor; d) providing security requirements for the delivery Process to ensure that Software cannot be compromised during delivery; e) considering implementation of alternative (equivalent) controls or methods to ascertain the required level of security (for example: an alternative method of authentication or additional Application and system monitoring). *[Reference: ICS Standard Security in Interactions with Third Parties]*
AS-160	Ensure that when designing and building Applications or Information Systems: a) development tools help enforce the creation of secure code; b) a section of code incorporated into the Application, including Third Party [TP] components are maintainable, tracked and originate from proven, reputable sources; c) source code reviews or application level security scans are performed to limit the likelihood of introducing security weaknesses; d) a fall-back process is in place in the event of security relevant features failing to function as intended. e) Security Issues are recorded, tracked, and managed in a timely manner;
AS-170	Include potential Threats (often referred to as Threat modelling) and review industry standards at the Information System design phase to help determine: a) significant Threats (including those that are adversarial, accidental, or environmental), such as nation states, organised criminal groups, inexperienced developers or poorly informed contractors. b) Threat events common to most development projects that should be defended against (for example. by leveraging lists such as OWASP Top 10 Most Critical Web Application Security Risks and CWE/SANS Top 25 Most Dangerous Software Errors); c) Vulnerabilities that must be avoided (for example: by leveraging lists such as OWASP Top 10 Most Critical Web Application Security Risks and CWE/SANS Top 25 Most Dangerous Software Errors); d) the priority of Threat events in terms of the risk they pose. e) appropriate measures to reduce the level of Threat and Vulnerability. *[Reference: Table: "Additional Protection Measures"]* *[Reference: OWASP Top 10 Web Application Security Risks]* *[Reference: OWASP Top 10 Mobile Risks]* *[Reference : OWASP Top 10 for LLM/AI Applications]*

Information System Owner **must**:	
AS-175	Ensure that security-related best practices and principles are embedded in the development methodology, tailored to the application's architecture, functionality and intended use including: a) a security architecture (for example: 'secure by design', 'defence in depth', 'secure by default', 'default deny' and 'fail secure'); b) secure coding guidance (for example: by leveraging lists such as OWASP Top 10 Most Critical Web Application Security Risks and CWE/SANS Top 25 Most Dangerous Software Errors); c) secure Application Programming Interface [API] guidance (for example: by leveraging list such as OWASP API Security Top 10 and NIST Security Strategies for Microservices-based Application Systems) ; d) an operational security directive (for example: which events to log and where, documentation to produce and instructions to be provided to the Information security team); e) a consistent and intuitive view of the data and how it is managed (for example: avoidance of redundant, unused interfaces, Information hiding, avoidance of semantic overloading of interfaces or their parameters). f) a review of designs to ensure security controls are specified and meet security requirements and are documented if they do not fully meet requirements. *[Reference: Group "Secure Coding" guideline]* *[Reference: OWASP Top 10 Web Application Security Risks]* *[Reference: OWASP API Security Project]* *[Reference: NIST SP 800-204: Security Strategies for Microservices-based Application Systems]* *[Reference: NIST SP 800-53: Security and Privacy Engineering Principles]* *[Reference: Appendix - Additional Protection measures]* *[Reference : OWASP Top 10 for LLM/AI Applications]*
AS-180	Ensure Applications have integrity checks built-in (for example: Checksum, Reconciliation, File Integrity Monitoring).

Information System Owner and/or Application Owner **must**:	
AS-185	Ensure that (owned) Applications do not store or cache sensitive information locally at client side/on Endpoint Devices. *[Examples:* *Sensitive information that cannot be stored locally:* - *User identification related: User names, IDs, bio-metric data, etc.* - *User authentication related: Passwords, Passphrases, PIN, OTP, etc.* - *Password reset / recovery related: Security questionnaires, answers, phone numbers, email addresses, etc.* - *Client Secret (reference Auth2.0)* - *Encryption keys]*

	[Notes: Endpoint Device includes mobile phones and tablet devices, laptops, desktops, etc. *Auto-complete feature must be disabled for the above user-entry fields]* *[Reference: Appendix Mobile Applications Security Requirements]*

Information System Owner **must**:	
AS-190	Ensure no proprietary uncompiled source code (or related Information) is stored in the Production environment.
AS-200	Ensure access control checks are performed for each object access. *Note: Code review of Application is recommended to identify presence of such vulnerabilities.*
AS-210	Ensure Applications involving batch input or batch interfaces (financial data) have capability to carry out Reconciliation.
AS-220	Include in the Information System build and development analysis of: a) the applicable security controls required to protect Information and Systems in line with ICS Standards requirements, assigned classification (impact rating) and identified threat profile; b) the effectiveness of specific implementation of security controls in terms of preventing, detecting or reacting to security events; c) specifics of security controls adoption in terms of information processing context, scope and architecture required by particular business Processes supported by systems under development (for example: encryption of Sensitive Information, Integrity checking and digitally signing Information); d) where and how security controls are to be applied; e) how individual security controls (manual and automated) work together to produce an integrated set of controls. *Note: Cryptography controls must be embedded to protect the Confidentiality and Integrity of Information Assets rated 5 or 4 in transit and at rest.* *[Reference: ICS Cryptography & ICS Information Handling Standard]*
AS-230	Ensure session management follows the minimum Session Management Requirements. *[Reference: IAM-450, IAM-490]*
AS-240	Follow the minimum secure techniques for Cookie Management. *[Reference: Appendix Secure Cookie Management technique]*
AS-250	Enable logging to the minimum requirements set within Group ICS Standard. *[Reference: ICS Security Logging and Monitoring Standard]*

3.4.1.1 Client Based Applications

Information System Owner **must**:	
AS-260	Ensure Application clients are securely authenticated by the Application server. *[Reference: ICS Identity and Access Management Standard]*

AS-270	Ensure Application clients are allowed by the server to access only the authorised services.

3.4.1.2 Browser Based/Web Applications

Information System Owner **must**:	
AS-280	Develop browser and Web Applications with the following minimum requirements: a) The authorised client list is to be defined at the Web or Application server (for example: in a system-to-system communication); b) Information Assets rated 5 or 4 are not stored in the browser's history; c) Changes to authorisation levels must be prevented during transaction sessions; d) Log and system report such attempts.
AS-290	Ensure Information Assets rated 5 or 4 are transmitted securely between Web application server and users. *[Reference: ICS Cryptography Standard Table for secure protocols]*
AS-300	Ensure Multi Factor Authentication [MFA] is implemented in an internet banking Application development and is in line with activities addressed by the Identity and Access Management Standard. *[Reference: IAM-350, IAM-360, IAM-370, IAM-390, IAM-660, IAM-995]*

3.4.1.3 Mobile Applications

Information System Owner and/or Technology Infrastructure Owner **must**:	
AS-310	Define and document a secure User access provisioning and de-provisioning process for Mobile Applications.

Information System Owner **must**:	
AS-320	Ensure security requirements are included in Mobile Application development. *[Reference: Appendix Mobile Applications Security Requirements]*
AS-330	Ensure the Mobile Application detects a rooted or jailbroken device.
AS-340	Enable access authorisations and Information protection measures when the Mobile Application processes Information Assets rated 5 or 4. *[Reference: ICS Information Handling Standard]*
AS-350	Ensure access to Information Assets and Information Systems are commensurate with its ratings. *[Reference. ICS Identity and Access Management Standard]*
AS-360	Ensure Mobile Application detects the presence of reverse engineering tools. *For Example: code injection tools, hooking frameworks, debugging servers.*
AS-370	Configure secure communication between the Application server and the client end. *For Example: The latest TLS version should be deployed.*

3.4.1.4 Third Party Applications

Information System Owner and/or Technology Infrastructure Owner **must**:	
AS-390	Screen all packaged Applications for any malicious code prior to distribution and installation in the Group.
AS-400	Ensure any modification to the base code of a pre-packaged Application is conducted without impacting the built-in security controls of the Application.

3.5. Control Area - Security Assessment

Information System Owner **must**:	
AS-420	Ensure that: a) Information risks associated with new Information Systems have been identified, assessed and treated (for example: mitigated, avoided, transferred or accepted); b) selected security controls (to mitigate identified Information risks) have been reviewed, built into new Information Systems and operate as expected; c) key performance indicators [KPIs] have been used to report the effectiveness of security approaches used in development (for example: the adoption of security techniques; the number of approved deviations from security policy; the reduction in overall number and severity of security Vulnerabilities; and the cost of security breaches caused by Vulnerabilities in the Information System); d) outstanding security issues have been or are being addressed.

3.6. Control Area - Implementation

Information System Owner and/or Technology Infrastructure Owner **must**:	
AS-490	Ensure the installation of new Information Systems in Production environments is: a) agreed with and communicated to impacted stakeholders; b) following a documented installation Process; c) restricted to authorised individuals and applies the principle of Least Privilege; d) carried out from authorised logical locations (for example: properly connected to secure network); e) feasible to be paused or revoked if required, in line with predefined, documented and tested roll-back procedure(s); f) performed within agreed time frames; g) (if required) supported by experts or vendor support teams (in the case the solution / technology implemented is new to the Group).
AS-500	Carry out checks to ensure that: a) the Application code (or equivalent) has been digitally signed to protect its Integrity;

Information System Owner and/or Technology Infrastructure Owner **must**:	
	b) developer's digital signature is verified before the Application is in use; c) all necessary patches and updates have been tested and successfully applied; d) any remaining technical security Vulnerabilities do not exceed approved impact assessment for security Vulnerability rating systems; e) there will be no adverse effects on existing Production systems; f) LRM requirements are fulfilled. *[Reference: ICS Security Patch Management Standard]*
AS-510	Remove sample or unused Application scripts.
AS-520	Use secure services (ports) and ensure communication of Information Assets rated 5 or 4 between different Application architecture tiers are encrypted. *Note: From Web service to Middleware and vice-versa. Middleware to database and vice-versa.* *[Reference: ICS Secure Configuration Management and ICS Cryptography Standard]*
AS-530	Ensure developers and testers access rights are revoked and any test data is securely removed before deploying to Production.

3.7. Control Area - Post Implementation

Information System Owner and/or Technology Infrastructure Owner **must**:	
AS-540	Only grant developers time-limited access to the relevant Production Application (for example: on an incident ticket basis) and ensure activities are logged and monitored without reducing the security of the Application.
AS-550	Maintain backup copy of configuration files separately from the Production Application configuration settings in the event of corruption and the same must be access restricted.

3.8. Control Area - Secure Decommission

Information System Owner and/or Technology Infrastructure Owner **must**:	
AS-560	Decommission the Application as per the Group's IT decommissioning process and securely destroy the Application data subject to applicability and fulfilment of the data retention period. *[Reference: ICS Secure Decommissioning and Destruction Standard sec 3.1 & 3.2., Data Retention period is as per the Group Record Management Policy].*

4. INFORMATION AND SUPPORT

4.1. General Information and Support

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

Reporting Non-Compliance

4.2. Reporting Non-Compliance

As a general guideline, any non-compliance against the Applications and underlying Technology Infrastructure in CMDB should follow the ICS Non-Compliance Register (ICS NCR) process. Further assessment of these non-compliance should follow the issue management process, i.e., iTrack for issues with remediation plan or ICS Dispensation when there is an explicit decision not to remediate the issue.

4.3. Breach of this Standard

- Failure to comply with this Standard may result in formal action under the Group Disciplinary Standard, that for serious breaches could include termination of employment.
- Any actual or suspected breaches must be reported immediately to your People Leader or to your Compliance representative from the Group.
- All breaches of this Standard must be reported to the Document Owner of the Standard.

5. GLOSSARY

The ICS Standards Glossary has been defined and is available via the *GovPoint* – see the *Technology Glossary* via the *GovPoint Glossary* reference.

6. REGULATORY OR INDUSTRY REFERENCES

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

7. APPENDIX

7.1. Table 1 - Additional Protection Measures

Threat	Description	Protection Measures
Spoofing	To protect against impersonation of Users/Systems, when dealing with Application processes and Users/Systems accessing the Application.	Basic authentication Digest authentication Cookie authentication Windows authentication Kerberos authentication PKI systems such as TLS and certificates IPSec Digitally signed packets To authenticate code or data: Digital signatures Message Authentication Codes Hashes
Tampering	To protect against modification of data or code through integrity protection, while dealing with data flows, data stores and Application processes.	Windows Mandatory Integrity Controls ACLs Digital signatures Message Authentication Codes Cookie authentication Basic authentication (to include CAPTCHA)
Repudiation	To protect against claims to have not performed an action, while dealing with Users/Systems and Application processes.	Strong Authentication Secure logging and auditing Digital Signatures Secure time stamps Trusted third parties
Information Disclosure	To protect against authorisation exposure of information, while dealing with data flows, data stores and Application processes.	Encryption Access control lists [ACLs]
Denial of Service [DoS] Distributed Denial of Services [DDoS]	To protect against denial or degraded service to Users, when dealing with data flows, data stores and Application processes. To apply bank's solutions for protecting critical Internet facing Applications.	DoS ACLs Filtering Quotas Authorisation High availability designs DDOS Web Application Firewalls (Akamai KONA) to protect against directed layer 7 web Application DoS attacks Routed 'On-Demand' Network DDoS

Threat	Description	Protection Measures
		protection (Akamai Prolexic) to protect against large scale layer-4 network DDoS attacks. External facing applications MUST have preventive measures such as routing traffic using network tools (e.g., firewall, IDS and IPS, WAF) and by placing them in effective locations, thereby aiding in preventing DoS / DDoS attacks.
Elevation of Privileges/Privilege Escalation	To protect against gaining capabilities without proper authorisation, when dealing with Application processes.	ACLs Group or role membership Privilege ownership Permissions Input validation
Key Threats	To protect against existing/emerging application relevant threats which could possibly exploit unaddressed vulnerabilities.	Forgery Attacks OWASP Top 10 vulnerabilities SANS Top 20 Programming Errors

7.2. Session Management Requirements

1. Delete session files upon session termination.
2. Session ID:
    a. To be at minimum length of 128 bits [preferred 256 bits].
    b. Not to be exposed in the URL rewriting options.
    c. To timeout after 15 mins of inactivity & MUST be invalidated when the user logs out. *Note: Where the 15 minutes Idle-time is set at Group Operating Systems/Platform level, the Group's internal facing applications cannot exceed Session time-out of 60 minutes.*
    d. To be changed after successful login/re-authentication.
    e. To be generated at random and unique.
    f. Generated by Application framework MUST only be recognised as valid by Application.
3. Restrict multiple concurrent sessions from same Session ID.
4. Do not embed Web session ID as part of URL [GET] or hidden fields [POST].
5. Protect securely the session data stored in the Application server memory [or disk].

7.3. Secure Cookie Management techniques

1. The entire cookie MUST be encrypted if sensitive data is persisted in the cookie (e.g. authentication cookies).
2. Secure flag MUST be set to prevent accidental transmission over 'the wire' in a non-secure manner.
3. Cookie parameters, values and their purpose MUST be documented in the Web Application design document.

4. Secure communication channel MUST be used to protect authentication credentials or cookies.
5. HTTPS MUST be implemented to protect transmission of login information and/or authentication cookies.
6. Cookies MUST be configured to expire without divulging the expiry date by addressing item (a) above.
7. Cookies MUST be configured for only its targeted specific domain by validating and specifying the domain attribute.
8. Encrypt Information Assets rated 5 or 4 passed in the cookies.
9. Ensure that cookie-based authentication is implemented using one-time encrypted session tokens.

7.4. Mobile Applications Security Requirements

1. Manage sessions as per Session Management Requirements in Appendix 6.2
2. Use random access tokens for client authentication without sending user's credentials.
3. Biometric authentication must be based on unlocking the keychain/keystore.
4. Users must be informed about all logging activities relevant to them.
5. Users must be able to view and manage their trusted/registered Mobile Devices having Group/Bank Mobile Applications installed.
6. Users login or access from an unregistered device must be verified with the user.

   [User profile and Device registration process exists as part of user on-boarding]
7. Use a valid certificate and the same must be signed by the Group Certification Authority [CA] or an equivalent as allowed by the Group.
8. Ensure the deployable Application
   a) Is not in debugging mode.
   b) Enable verbose logging or debugging messages.
9. Set the Application in denied access by default. Memory used by unmanaged code must be used securely. After usage the memory must be freed accordingly.
10. Not enable debugging by default in the context of protection scheme, this will enable adversaries to invest significant effort to enable debugging. All available debugging protocols must be covered.
11. Ensure Information Assets rated 5 or 4 such as passwords and credit card numbers, are not;
    a) Exposed through the Inter Process Communication [IPC] or user interface or leaks to screenshots.
    b) Included in backups.
    c) Kept in memory longer than necessary and memory must be cleared explicitly after use.
12. Remove Information Assets rated 5 or 4 from views when back grounded.
13. Ensure JavaScript is disabled in WebViews unless explicitly required. WebViews are configured to allow only the minimum set of protocol handlers required (ideally, only https). Potentially dangerous handlers, such as file, tel and app-id, must be disabled.
14. Ensure Webviews do not allow import/export of user data through any channel (through browser or network file share, etc).
15. Ensure;

a) If java objects are exposed in a Webview then only the JavaScript functionality should be rendered or utilised.

b) Object serialisation, if any, is implemented using safe serialisation Application Programming Interfaces [APIs].

16. Ensure the Mobile Application must:

a) Detect and respond to tampering with executable files and critical data along with any modifications of process memory, including relocation table patches and injected code.

b) Detect being run in an emulator using any method.

17. Validate authenticity of client certificate before allowing access.

18. Ensure the Mobile Application has the capability for Certificate pinning with the trusted server and deny requests from untrusted servers (applicable to Internet-facing and Customer application).

8. Appendix A - Version Control Table

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISO Policy	Annual review incudes: 1. Initial Draft in new ERMF Template. 2. Consolidated following existing Standards a) Security in Application Development b) Application Security Standard c) Mobile Application Security Standard d) Securing Sensitive Data during Application Development e) Application relevant controls from various other existing Standards. Consultation feedback, corrections incorporated	-	Liz Banbury	1.0	19-Dec-2019	26-Dec-2019

Document Author Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISRO ICS Policy	1. Removed 'should not' from Appendix Section 6.4: Point 18 [ICSCR-9Jan2020-1]	-	Liz Banbury	1.1	10-Feb-2020	14-Feb-2020
CISRO ICS Policy	Based on Change Requests and roles updated, IC removed: **New**: AS-175 (split of AS-170)	-	Samantha Finan, Global Head, ICS Policy,	1.2	22-June-2022	29-June-2022
	Administrative update: AS-040, AS-090, AS-140, AS-150, AS-160, AS-170, AS-220, AS-230, AS-300, AS-420, AS-440, AS490, AS-500 **Removed**: AS-120, AS-130, AS-380, AS-410, AS-430, AS-450:480		Standards and Reporting			
CISRO ICS Policy	Document template updated as per the ER STD Template for Group Standards v5.6 AS-185 added and AS-280 amended in line with the ICSCR6Dec2022-1	-	Paul Hoare Head, ICS Policy and Best Practice	2.0	27-Apr-2023	02-May-2023
CISRO ICS Policy	Editorial changes introduced: 1) AS-440 removed in line with the ICSCR-9Dec2022-1 (as the requirement is already covered in the ICS controls from the Vulnerability Management area)	-	Paul Hoare Head, ICS Policy and Best Practice	2.1	03-Oct-2023	07-Oct-2023

9. Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Arti Singh **[ICS Standards]**	Administrative and editorial changes: 1. Document template updated 2. ICS risks in section 1.1 updated in line with definition from ERMF 3. References / Links in section 4 , 5 and 6 updated 4. Scope section updated 5. Section 2. ROLES & RESPONSIBILITIES - Group Chief Information Security Risk Office (Group CISRO) Updated Review of standard from Bilennial to at least Annual	Non - Material	Jamie Cowan Head, ICS Risk Framework & Governance	2.2	15-Nov-2024	25-Nov-2024