

Title:	ICT Acceptance Use Standard
Owner:	Lead: ICT Service Management
Document No:	SS-STD-ICT-018
Effective date:	November 2014
Next Review:	Every Three Years
File Plan No:	(For completion by CSIRIS only)


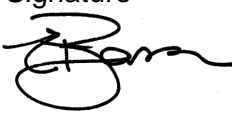

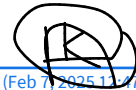
Document Approval			
Approved by:	Manager: Infrastructure and Service Management Lawrence Moeng	Signature 	Date 06/02/2025
Approved by:	Manager: Solutions Development: Eric Basson	Signature 	Date 06/02/2025
Approved by:	Manager: Strategy and Demand Management Darryl Rondganger	Signature 	Date 06/02/2025
Approved by:	Chief Information Security Officer Kweku Arthur	Signature  <small>Kweku Arthur (Feb 7, 2025 12:47 GMT+2)</small>	Date 07/02/2025

Table of Contents

1 DOCUMENT CHANGE HISTORY	3
2 STANDARD TITLE	3
3 PURPOSE	3
4 SCOPE	3
5 STANDARD	4
5.1 General Use and Ownership	4
5.2 Security and Proprietary Information	4
5.3 Unacceptable Use.....	5
6 ENFORCEMENT	6
7 OWNERSHIP AND RESPONSIBILITIES	6
7.1 Owner	6
7.2 Responsibilities	7
8 RECORDS	7

1. DOCUMENT CHANGE HISTORY

PUBLICATION DATE	AUTHOR	REVISION NO.	CHANGE DESCRIPTION
November 2011	Carl Grundling	00	New
March 2013	Carl Grundling	01	General revision of terms
November 2014	Leon du Preez	02	Reviewed stakeholders and review period
August 2015	Leon du Preez	03	Reviewed content
December 2024	Eugene Goqo	04	Reviewed content

2. DEFINITIONS

Term	Definition
Access Control	A process or control through which access is restricted to authorised individual users, applications, third parties or information systems.
Availability	Ensuring timely and reliable access to and use of information.
Best Practice	Recommendations, solutions, or practices considered the most desirable, preferred or widely used in a specific industry.
Classification	The act or process by which data and/or information is determined to be of a particular category or class.
Confidentiality	The principle is that information is not made available or disclosed to unauthorised individuals, entities or processes.
Data	A set of values, numbers, characters, words or other elements that may be interpreted or processed to produce information.
Event	An occurrence of or change in a particular set of circumstances.
Guideline	A document that provides recommended but not mandatory advice regarding practices in a given situation, scenario or topic.
ICT Asset	Any resource, tool, infrastructure, or hardware and software owned, controlled, or utilised by an organisation to process, store, and communicate information.
ICT Service	A means of delivering value to the business by facilitating the achievement of the business's outcomes and objectives. These are typically provisioned through ICT infrastructure and business application systems.

Incident	An identified occurrence of an adverse event indicating a possible breach of policy, failure of controls, or previously unknown situation that may impact the organisation's information security and privacy responsibilities.
Information Asset	An information asset is a valuable or useful object which includes: <ul style="list-style-type: none"> • Technology assets (databases, data files, electronic documents, software, development tools and utilities); & • Physical assets (computer equipment, communications equipment, or computer media).
Information Resource	Any data/information in electronic, physical, verbal or audio-visual form or any hardware, software or information processing facilities that makes possible the use, handling, transfer and/or storage of data/information.
Information System	An application, service, information technology asset, or any other information handling component.
Information Owners	A CSIR employee is ultimately responsible for establishing the rules for the appropriate use and protection of an Information Resource.
Integrity	The property of information that describes its accuracy, reliability and completeness, especially as impacted by unauthorised modification.
Least Privilege	Giving an employee only those essential privileges for the employee's role/function.
Management	Employees responsible for managing the organisation and/or functions or people within the organisation. These individuals are often responsible for setting the organisation's strategy or function and for coordinating the efforts of its employees to accomplish its objectives through the application of available resources, such as financial, natural, technological, and human resources.
Personal Device	Electronic equipment that has a processing capability and is owned by an individual/employee and is not owned by the CSIR often

	refers to a desktop, laptop, tablet, cell phone, smartphone, wearables, or portable storage device.
Procedure	A set agreed or approved series of activities or tasks that contribute to fulfilling a task.
Risk	A measure of the extent to which a potential circumstance or event threatens an entity.
Standard	A measure, often documented that, provides specific mandatory controls that help enforce and support policies.
Third-party	A person or entity other than the CSIR and its employees with whom the CSIR has a legal, transactional or stakeholder relationship.
Threat	A circumstance, entity or event that can potentially exploit vulnerabilities and violate information security.
Transfer	The sending and/or sharing of information.

3. LIST OF ABBREVIATIONS

Abbreviation	Full term
AUS	Acceptable Use Standard
CSIR	Council for Scientific and Industrial Research
ICT	Information and Communication Technology
IP	Intellectual Property
IS	Information Security
ISO	International Organisation of Standardisation
ITIL	Information Technology Infrastructure Library (IT Service Management Framework)
MISS	Minimum Information Security Standards
POPIA	Protection of Personal Information Act 4 of 2013
PRDC	Policy Review and Development Committee
OPCO	Operations Committee
RICA	Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002
SLA	Service Level Agreement

4. STANDARD TITLE

ICT Acceptable Use Standard.

5. PURPOSE

This standard aims to protect the image and reputation of the CSIR and promote the integrity, availability, and confidentiality of the CSIR's systems, network and data contained therein. It informs the user of the prevailing rules and prohibitions that define and govern acceptable use of such systems and facilities and outlines the possible results of violation of this standard.

CSIR's ICT comprises the vast and growing array of computing and electronic data communications facilities and services utilised daily to create, access, examine, store, and distribute material in multiple media and formats. ICT plays an integral part in the fulfilment of CSIR's research function. Users of CSIR's ICT resources have a responsibility not to abuse these resources and to respect the rights of the members of the community and the CSIR itself. The CSIR AUS provides guidelines for the appropriate use of CSIR's ICT resources and for the CSIR's access to information about and oversight of these resources.

6. SCOPE

This standard applies to employees, contractors, consultants, temporary workers, and all personnel affiliated with third parties. It also applies to all ICT systems and services owned or leased by the CSIR.

This standard defines the boundaries for the "acceptable use" of the CSIR's resources, including software, hardware devices, and network systems. Hardware devices, software programs, and network systems purchased and provided by the CSIR are to be used only for creating, researching, and processing CSIR-related materials. Using the CSIR's hardware, software, and network systems, the employee (user) assumes personal responsibility for their appropriate use and agrees to comply with this standard, other applicable CSIR policies, and laws and regulations.

All the following are included whether they are owned or leased by the organisation or are under the organisation's possession, custody, or control:

- All computer-related equipment, including desktop personal computers, laptops, tablets, smartphones, wireless computing devices, telecommunication equipment, networks and networking equipment, databases, printers, servers and shared computers, and all networks and hardware to which the equipment is connected.
- All software, including purchased or licensed business software applications, organisational-written applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on organisationally owned equipment.
- All IP and other data stored on organisational equipment.

7. STANDARD

The acceptable use of information resources in CSIR is critical to the organisation's success and must be protected against misuse.

7.1. CSIR Information Resource for Personal Use

- 7.1.1 The use of CSIR-provisioned Information Resources for purposes that are not part of the employee's duties and not within the course and scope of such employee's work (personal use) must be restricted to when the employee has no other option and cannot wait until the employee can use their personal information resources (reasonable use).
- 7.1.2 Each user assumes responsibility for exercising good judgement regarding their reasonable personal use of CSIR ICT infrastructure, such as the Internet, storage, streaming and/or downloading of data, etc.
- 7.1.3 Each user recognises that the personal use of CSIR-provisioned Information Resources may constitute fruitless and wasteful expenditure, which in turn constitutes misconduct. Users must consult the Manager: ICT Infrastructure and Service Management if uncertain.
- 7.1.4 Personal software installed on any CSIR ICT Asset must adhere to the terms of the applicable license agreement
- 7.1.5 The CSIR does not guarantee the confidentiality of any private information stored on its information resources.
- 7.1.6 The CSIR reserves the right to have authorised ICT Services personnel audit ICT systems and services at any time.

7.2 The Use of Personal Devices or Information Resources

- 7.2.1 All personal devices used by employees to access CSIR Information Resources, including connecting to the CSIR network, must:

- Continuously execute an approved internet security suite with the latest signatures.
- Encrypt all CSIR Information using a suitable encryption.
- Ensure that any personal data storage device containing sensitive and/or confidential information is always kept secure.
- Adhere to CSIR policies and standards.

7.2.2 The loss of any personal device or information resource with CSIR information must be reported using the same process to report the loss of a CSIR computing asset.

7.2.3 For security or operational purposes, the CSIR reserves the right to have authorised ICT Services personnel audit any personal device or information resource connected to the CSIR network.

7.2.4 ICT Services does not support personal devices or information resources; any assistance is on a 'best effort' basis.

7.3 ICT Information Asset Management

7.3.1 ICT Services must facilitate the acquisition of all IT assets (hardware and software, including licenses) following the CSIR Procurement Policy.

- This includes all computing devices, peripherals, networking equipment, network cabling and wireless infrastructure, storage devices, software, and subscription licenses, irrespective of the field of application.
- Depending on the IT asset to be procured, ICT Services will either directly facilitate, participate or provide requirement specifications for acquiring IT assets.
- Technical, support and integration requirements set by ICT Services are mandatory if the information asset is used, hosted, or integrated with CSIR's current ICT Infrastructure.

7.3.2 Regardless of ICT Services' level of involvement in the process to select or procure a CSIR Information Asset, ICT Services must be allowed to review the selection of any non-specialised RD&I ICT information asset or provide requirements before its acquisition to ensure the information asset is compatible with the CSIR's ICT ecosystem and complies with applicable governance requirements (standards, policies, etc.) in the CSIR. Suppose ICT Services deems that the selected information asset is not sufficiently compatible, does not comply with the applicable governance requirements in the CSIR, or both. In that case, ICT Services may prohibit the acquisition thereof.

- 7.3.3 Regardless of ICT Services' level of involvement in the procurement process, ICT Services must be consulted and support contracting ICT-related third-party services before they are procured and contracted.
- 7.3.4 Regardless of ICT Services' level of involvement in the contracting process, ICT Services must be consulted and support the inclusion of any CSIR ICT services, ICT Services' resources and the use of CSIR information assets as part of a contract with a client or a supplier.
- 7.3.5 Users must submit a service request to ICT Services to seek approval for and facilitate the procurement of all CSIR Information Assets.
- 7.3.6 The ICT Services must be allowed to manage all ICT information assets centrally.
- 7.3.7 Software installed on any CSIR ICT Asset must adhere to the terms of the applicable license agreement.
- 7.3.8 Specialised RD&I Information Assets are exempted from the central control
- 7.3.9 For security or network maintenance purposes, the CSIR reserves the right to audit ICT systems and services by authorised ICT Services personnel at any time.
- 7.3.10 ICT Services employees may restrict a host's network access if the host disrupts or threatens to disrupt production services.
- 7.3.11 Passwords are kept secure and are not shared. Every user assumes responsibility for the security of their passwords and accounts.
- 7.3.12 All PCs, laptops and workstations must be secured with a password-protected screen saver and have the automatic activation feature turned on at all times.
- 7.3.13 All employees' hosts connected to the CSIR's Internet/Intranet/Extranet (or used in an 'off-line' state) must continually execute approved virus-scanning software with a current virus database.
- 7.3.14 Each user should exercise extreme caution when opening e-mail attachments received from unknown senders, as they may contain viruses.
- 7.3.15 Care is taken to ensure that any data storage device with sensitive and/or confidential information is always kept secure.
- 7.3.16 Do not leave your laptop unattended unless it is physically secure. Secure your laptop when you are not in your office. Lock your door and/or secure your laptop to the desk with a laptop cable. If you take your laptop home, be sure to keep it in a secure location. For example, don't leave your laptop in your car.

7.4 Specialised RD&I Information Assets

Regarding CSIR ICT information asset management, specialised RD&I information assets are exempted from central control. However, the asset management of specialised RD&I information assets must comply with the following:

- 7.4.1 Depending on the IT asset to be procured, ICT services must participate in or provide requirement specifications for acquiring IT assets.
- 7.4.2 Technical and support requirements provided by ICT services are mandatory if the information asset will be used or hosted on CSIR's current ICT Infrastructure or if any form of integration is required with current CSIR systems.
- 7.4.3 Specialised RD&I information asset owners must register the assets and report on the use and maintenance of such assets to the ICT Services Centre.
- 7.4.4 Specialised RD&I information asset owners must inform ICT Services if the asset owner changes.
- 7.4.5 Unless decommissioned, specialised RD&I information assets must remain fully supported by the original equipment manufacturers through warranties and maintenance/support contracts, including software assurance, to remain eligible for the latest version of any software that forms part of or is used by the specialised RD&I information asset
- 7.4.6 Specialised RD&I information assets, whether CSIR or not, that store or have access to CSIR information or business services must have the necessary information protection controls (such as access control and encryption) to safeguard the information.
- 7.4.7 Privileged or administrative rights to specialised RD&I Information Assets must comply with the 'least privilege' principle.
- 7.4.8 Specialised RD&I information assets used to provide anything as a service (XaaS) are subject to the CSIR Change Management and Release Management controls.
- 7.4.9 Specialised RD&I information assets must be securely backed up at appropriate intervals according to the applicable backup and retention policies/requirements.
- 7.4.10 XaaS provisioned/hosted on Specialised RD&I information assets must comply with the CSIR's overall Business Continuity plans and processes.
- 7.4.11 Specialised RD&I information asset owners must apply measures to protect data integrity, confidentiality, and availability.
- 7.4.12 All non-CSIR information systems or ICT services to be hosted at, managed and/or operated by the CSIR are subject to a feasibility assessment under the oversight of ICT Services and a signed contract(s).

7.4.13 Using cloud-based services as part of specialised RD&I information assets is subject to ICT oversight, and ICT Services must contract and manage such a cloud-based service.

7.4.14 Consider the generally good administration practices and adopt the relevant practices.

7.5 Privileged or Administrative Rights

7.5.1 Where privileged or administrator rights are required, the user must

- Must log a service request with ICT.
- Complete the application for the elevated privilege access.
- Obtain approval from the relevant management structures.

7.5.2 Such rights and entitlements

- Are reviewed annually and removed when no longer required.
- May be removed in the event of misuse or perceived threat.

7.6 Protection of Information

7.6.1 Security breaches include, but are not limited to:

- Accessing data of which the employee is not the intended recipient or does not form part of the employee's duties and is not within the course and scope of such employee's work.
- Logging into a server or account that the employee is not expressly authorised to access unless these duties are within the course and scope of such employee's work.

7.6.2 Organisational confidential information may not be shared outside the organisation without authorisation unless a contractual relationship specifically governs the sharing.

7.6.3 All devices, whether CSIR or personally owned, that store or have access to CSIR information or business services must have the necessary information protection controls (such as access control and encryption) to safeguard the information. Where this is a CSIR-owned device, the ICT Services Centre must implement and manage these safeguards.

7.6.4 Data and information assets must be stored securely relevant to their classification. Primary storage should be in a secure CSIR-managed network environment.

7.6.5 Information Owners must classify data based on its sensitivity and importance, and appropriate security measures must be implemented for each classification level.

7.6.6 Information Owners must apply measures to protect data integrity, confidentiality, and availability.

7.6.7 Each user assumes responsibility for ensuring that visitors who bring their own removable storage devices onto the CSIR campus are always supervised while the device is connected to CSIR equipment.

7.6.8 Whenever possible, only connect to wireless networks that require a network security key or have some other form of security, such as a certificate. The information sent over these networks is encrypted, which can help protect your computer from unauthorised access.

7.6.9 Before connecting to a network provided by a wireless Internet service provider (ISP), such as a public network in a coffee shop or airport, read the privacy statement carefully and make sure that you understand which files, if any, are saved to your computer and what type of information the network provider collects from your computer.

7.7 General Use and Ownership

7.7.1 The following considerations apply to social media:

- Be responsible in what one writes
- Remember to protect CSIR's confidential & proprietary information
- Respect copyrights
- Authenticity
- Consider your audience
- Exercise good judgement
- Understand the concept of community.

7.7.2 Postings by employees from a CSIR e-mail address to newsgroups contain a disclaimer clearly stating that the opinions expressed are strictly their own and not necessarily those of the CSIR.

7.8 Software Development

7.8.1 Register in-house developed software in the CSIR Software Asset register.

7.8.2 Update the CSIR Software Asset Register when the ownership changes.

7.8.3 All software developed in-house must comply with the CSIR's overall business continuity plans and processes.

7.8.4 All software development must comply with applicable CSIR Standards.

7.8.5 Consider the generally good software development practices and adopt the relevant practices.

7.9 Unacceptable Use

The following activities are prohibited:

- 7.9.1 Breaching the security of any CSIR information asset.
- 7.9.2 Organisational confidential information may not be shared outside the organisation without authorisation unless a contractual relationship specifically governs the sharing.
- 7.9.3 The transmission, storage or distribution of any material or content where such action would violate any South African or other applicable laws prohibiting child pornography; obscenity; discrimination (including racial, gender or religious slurs) and hate speech; or speech designed to incite violence or hatred, or threats to cause bodily harm.
- 7.9.4 The transmission, storage or distribution of any material or content where such action is intended to defame, abuse, stalk, harass or physically threaten any individual in the Republic or beyond its borders, including any attempt to link to, post, transmit or otherwise distribute any inappropriate or defamatory material.
- 7.9.5 The transmission, storage and distribution of any material or content where such action violates any IP laws, including laws concerning local and international copyright, trademarks and trade secrets.
- 7.9.6 Any effort to use the CSIR's ICT systems and services in a way that circumvents or would circumvent the user authentication or security of any host, network or account ("cracking" or "hacking"). In instances where this is a requirement, ICT Services should be notified of the intention via the Cluster or Portfolio manager.
- 7.9.7 Any attempt to use the CSIR's ICT systems and services in a way that breaches or would breach the security of another user's account or that gains or would gain access to any other person's computer, software, or data or otherwise threaten another person's privacy, without the knowledge and consent of such person.
- 7.9.8 Any activity which threatens to disrupt the CSIR's systems and services through "denial of service attacks", flooding of a network or overloading a service, or any unauthorised probes ("scanning" or "nuking") of other networks.
- 7.9.9 Any activity that threatens the security of ICT systems and services by knowingly posting, transmitting, linking to or otherwise distributing any information or software that contains a virus, trojan horse, worm, lock, mail bomb, or other harmful, destructive or disruptive component.

- 7.9.10 Any unsolicited mass mailing activity, including direct marketing, spam, and chain letters for commercial or other purposes, without the prior consent of the recipients of those e-mails.
- 7.9.11 Unauthorised use, or forging, of e-mail header information.
- 7.9.12 Creating or forwarding "chain letters" or other "pyramid" schemes.
- 7.9.13 The installation of any computing device on the CSIR's network without prior approval from ICT Services is strictly prohibited. This includes PCs, laptops, servers, routers, mobile devices, and switches. It excludes providing guest network access to visitors and their specific computing devices via the CSIR Guest Network for Internet Access initiative.
- 7.9.14 The use of any portable storage devices to store sensitive, confidential or personally identifiable information without prior authorisation by their manager.
- 7.9.15 The storing of any CSIR sensitive or confidential information on social networking sites such as Facebook, WhatsApp, Instagram, X (formerly known as Twitter), Telegram and others.
- 7.9.16 Employees are prohibited from using forensic software or other tools that may attempt to defeat or circumvent controls or otherwise destroy CSIR information stored on a CSIR-owned device.
- 7.9.17 Contracting for any ICT Service that binds the CSIR as a whole.

7.10 Enforcement

- 7.10.1 The CSIR reserves the right to audit networks and systems periodically to ensure compliance with this standard. The Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) no 70 of 2002 came into effect in 2005. This act requires written consent from each employee to agree to the interception of any communication and related information (expressly, but not limited to, communication using telephone/modem, telefax, Internet or e-mail).
- 7.10.2 Any employee found to have violated this standard may be subject to disciplinary action, up to and including termination of employment.
- 7.10.3 All users must report all suspected cases of violation to their appropriate Business Services Manager and the Chief Information Officer.

7.10.4 The Manager: Infrastructure and Service Management will collect the facts (after approval from the CIO, of the case and identify the offender. If, in the opinion of the CIO, the alleged violation warrants further action, the relevant HR Manager will be contacted to initiate the appropriate action.

7.11 Physical and Environments

7.11.1 All CSIR's information resources and all information systems must be installed within an appropriate facility that meets the requirements of that information system. The management of physical access to ICT Resources will be managed in line with the Physical Access to ICT Services Centre (Data Centres) Application procedure

8. OWNERSHIP AND RESPONSIBILITIES

8.1 Owner

Chief Information Officer.

8.2 Responsibilities

The Chief Information Officer retains all levels of authority for ICT Risk and Compliance.

The Manager: ICT Infrastructure and Service Management owns the documented standard and is responsible for ensuring that it is followed, regularly reviewed, and updated.

9. RECORDS

Description	Location	Responsibility	Retention Time	Disposal Method
ICT Acceptable Use Standard	ICT Website	Chief Information Officer.	Indefinitely	Normal waste
ICT Policy	ICT Website	Chief Information Officer.	Indefinitely	Normal waste
ICT Investigations and Surveillance Procedure	ICT Website	Chief Information Officer.	Indefinitely	Normal waste

ANNEXURE A Generally Good Administration Practices

General Best Practices:	Application Administration:
Change Management: Implement a robust change management process, ensuring changes are tested, approved, and documented.	Regular Updates: Update applications regularly, especially for security patches.
Incident Management: Have a well-defined process for handling incidents, ensuring timely response and recovery.	User Management: Manage user roles and permissions diligently. Only grant access as needed.
Training: Continuously train administrators on new technologies, security threats, and best practices.	Monitoring and Logging: Monitor application performance and user activities. Ensure logs are comprehensive, but avoid logging sensitive information.
Vendor/Original Equipment Manufacturer Management: Review and communicate regularly with vendors about patches, updates, and known vulnerabilities.	Performance Tuning: Monitor application performance and fine-tune configurations to ensure optimal performance.
Automation: Wherever possible, automate repetitive tasks to reduce human errors.	Backup and Recovery: Regularly backup application data and configurations. Test recovery processes.
Auditing and Compliance: Regularly audit system and user activities. Ensure compliance with industry standards and regulations.	Security: Implement security measures like HTTPS, input validation, output encoding, and secure session management.
Principle of Least Privilege: Only give users and processes the permissions they need to perform their tasks.	Configuration Management: Store configurations securely, preferably outside the codebase. Avoid hardcoding sensitive data.
	Testing: Regularly test the application for vulnerabilities and performance issues. If possible, implement continuous integration and development/deployment (CI/CD) pipelines.
	Documentation: Maintain updated documentation about the application's architecture, dependencies, configurations, and customisations.
Database Administration:	Server Administration:
Regular Backups: Ensure databases are backed up regularly and test the restoration processes.	Regular Updates and Patching: Ensure that the OS and software are updated with the latest patches and updates.
Performance Tuning: Monitor query performance, optimise indexes, and fine-tune configurations to ensure optimal performance.	Monitoring: Use tools to monitor server health, performance metrics, and potential security threats.
Security: Use strong authentication methods, encrypt sensitive data, and regularly audit access and actions.	Backup: Implement regular backups and test the restoration process to ensure data integrity and availability.
Data Integrity: Implement data validation checks, constraints, and referential integrity rules.	User Management: Only grant necessary permissions and privileges. Use the principle of least privilege.
Monitoring: Monitor database health, transaction rates, and error logs.	Security: applying the principle of Least Privilege,
Updates and Patching: Keep the database management system (DBMS) updated with the latest patches.	Perimeter Security: Using a firewall to regulate incoming and outgoing traffic, Limiting open ports to only those necessary for your application, using SSH Key, and implementing 2FA where feasible, especially for administrative access.
Disaster Recovery: Implement and test disaster recovery plans and high-availability setups like replication or clustering.	Hardening: Disable unused services, ports, and protocols. Configure firewalls and intrusion detection systems.
Documentation: Document database schemas, relationships, stored procedures, and custom configurations.	Documentation: Maintain updated documentation regarding server configurations, installed software, and changes.

ANNEXURE B Generally Good Software Development Practices

Requirements and Design	Approach
Understand the business problem/opportunity, objective(s), alternatives, risks and constraints, and the URS and FRS documentation where available.	Break down the project into clearly defined iterations with regular feedback and adjustments,
Unless prescribed, please select the most appropriate technologies by assessing their technical, operational, and financial feasibility to identify potential risks and challenges early. First, choose from available technologies.	Focus on delivering the most valuable features first.
Formulate a conceptual solutions design.	Develop a functionality release roadmap.
Coding Standards	Code Reviews
Follow and adhere to consistent coding standards and style guides to ensure maintainability.	Regularly review code with peers to catch potential issues, ensure the code meets quality standards, and share knowledge among team members.
Use consistent naming conventions, formatting, and structure throughout the codebase.	Provide helpful and respectful feedback during reviews to foster a positive and productive team environment.
Write code that is easy to understand, avoiding complex logic where possible.	Accept feedback constructively, focusing on improving the code and being open to exploring alternative approaches.
Use Linters and Formatters to automate coding standards enforcement and ensure consistency.	Utilise pull requests for code reviews to provide a formal process for merging changes into the main branch.
Continuously improve code by refactoring to reduce complexity, improve readability and enhance maintainability without changing external behaviour.	Automated Code Review Tools: Integrate automated code review tools to ensure adherence to coding standards and detect common issues.
Break down the code into smaller, reusable modules or components that make the code easier to maintain, test, and extend.	
Avoid duplicating code by reusing functions, classes, and modules wherever possible.	
Version Control	Testing
Maintain code versions to track changes to the codebase, ease rollbacks, and provide a clear history of the project's evolution.	Conducting unit, integration, and end-to-end tests to ensure that the code works as expected and that code changes do not introduce regressions.
Preferably use version control systems (VCS) like Git to manage code versions, collaborate with team members, and enable the segregation of duties when moving projects between environments.	Write tests before writing the actual code to ensure that functionality meets the requirements from the start and that all features are covered and work as expected.












ICT Acceptance Use Standard

Final Audit Report

2025-02-07

Created:	2025-02-06
By:	Eugene Goqo (egoqo@csir.co.za)
Status:	Signed
Transaction ID:	CBJCHBCAABAArVOyktyve9Tx1t7TMRT7ngM5X2mmv40R

"ICT Acceptance Use Standard" History

-  Document created by Eugene Goqo (egoqo@csir.co.za)
2025-02-06 - 07:09:28 GMT- IP address: 41.150.217.219
-  Document emailed to Lawrence Moeng (lmoeng@csir.co.za) for signature
2025-02-06 - 07:11:32 GMT
-  Email viewed by Lawrence Moeng (lmoeng@csir.co.za)
2025-02-06 - 07:31:03 GMT- IP address: 146.64.81.209
-  Lawrence Moeng (lmoeng@csir.co.za) authenticated with Adobe Acrobat Sign.
2025-02-06 - 07:31:41 GMT
-  Document e-signed by Lawrence Moeng (lmoeng@csir.co.za)
Signature Date: 2025-02-06 - 07:36:32 GMT - Time Source: server- IP address: 146.64.81.209
-  Document emailed to Eric Basson (ebasson@csir.co.za) for signature
2025-02-06 - 07:36:33 GMT
-  Email viewed by Eric Basson (ebasson@csir.co.za)
2025-02-06 - 07:48:23 GMT- IP address: 146.64.81.209
-  Eric Basson (ebasson@csir.co.za) authenticated with Adobe Acrobat Sign.
2025-02-06 - 08:25:20 GMT
-  Document e-signed by Eric Basson (ebasson@csir.co.za)
Signature Date: 2025-02-06 - 08:25:20 GMT - Time Source: server- IP address: 146.64.81.209
-  Document emailed to Darryl Rondganger (drondganger@csir.co.za) for signature
2025-02-06 - 08:25:21 GMT
-  Darryl Rondganger (drondganger@csir.co.za) authenticated with Adobe Acrobat Sign.
2025-02-06 - 12:08:24 GMT



Adobe Acrobat Sign



Document e-signed by Darryl Rondganger (drondganger@csir.co.za)

Signature Date: 2025-02-06 - 12:08:24 GMT - Time Source: server- IP address: 146.64.81.209



Document emailed to Kweku Arthur (kkarthur@csir.co.za) for approval

2025-02-06 - 12:08:25 GMT



Kweku Arthur (kkarthur@csir.co.za) authenticated with Adobe Acrobat Sign.

2025-02-07 - 10:47:59 GMT



Document approved by Kweku Arthur (kkarthur@csir.co.za)

Approval Date: 2025-02-07 - 10:47:59 GMT - Time Source: server- IP address: 146.64.81.209



Agreement completed.

2025-02-07 - 10:47:59 GMT

