ICT and Digital Services Policy

Version 1

Effective Date: 10 June 2026

Table of Contents

Document Management

Functional Area:	ICT & Digital Support Services
Owner/Contact:	ICT Manager
Directorate	Corporate Services
Approved by:	BOT
Date of approval:	10 June 2026
Date of Next Review:	09 June 2029
Title in English:	ICT and Digital Services Policy
Title in French:	
Related Policies and Procedures	Conflict of Interest Policy, Staff Management Policy, AfricaRice ICT Business Continuity Plan -2021, CGIAR ICT Policies, AfricaRice - SOP - Information System Access Account, AfricaRice - Information Systems Security Charter, ICT Incident Management Guidelines AfricaRice Open Access and Data Management Policy Data Sharing Policy
History of versions	Version 1
Key points	New Standard format not used in this document ICT management is significantly broad. Based on best practice, this has been split into six (6) segments to ensure clarity and understanding. Each segment has been individually addressed in this document

1. Preamble

The Africa Rice Center (AfricaRice) is an autonomous intergovernmental research association of African member countries. It is also a leading pan-African research organization with a mission to contribute to poverty alleviation and food security in Africa through research, development and partnership activities. It is one of 12 Centers and Alliance under One CGIAR supported by the CGIAR Fund.
The role of Information and Communication Technology (ICT) in the One CGIAR is undergoing some dynamic transformation away from the traditional corporate services dimensions and embracing the core objective of the One CGIAR and the Centers. ICT is evolving to serve as a tool for science to accelerate innovation, support research and impact. ICT is powered by an improved security posture and increased operational resilience of digital infrastructure with improved digital user experience.
The development of this policy is to ensure AfricaRice meets these key requirements.

AfricaRice recognizes the development, importance and use of Artificial Intelligence (AI) in the workplace. AfricaRice promotes responsible utilization of AI in its digital services infrastructure and systems. Specific Artificial Intelligence (AI) policies will be incorporated in the Data Management Policy under review.

2. Definitions

2.1. Board of Trustees: AfricaRice governing board per the institutions governing documents.
2.2. Executive Management Committee (EMC): Executive management committee (EMC) member who has responsibility for the person making the request.
2.3. ICT Manager: The most senior manager in the ICT department.
2.4. ICT Functional Heads: Managers of departments within the ICT service – Customer Service; EndPoint; Infrastructure; Business Systems; Project Management Office
2.5. ICT Unit: The department within Corporate Services Directorate charged with the management of ICT resources and assets in AfricaRice.
2.6. User: A person with a valid contract to work for AfricaRice, (permanent, temporary, consultant, student/intern, associate, hosted staff etc.) is entitled to a User ID to interact with AfricaRice ICT services.
2.7. Endpoint: desktops, laptops, tablets, mobile/handheld devices, anything at the edge of the Centre's local or wide area network.
2.8. Application: software programs storing, processing, and presenting Centre data, information and knowledge.
2.9. Data/Information: the fundamental records stored electronically represent Centre intellectual property.
2.10. Network: The system established by a Centre whereby workstations, servers and other data processing nodes are interconnected for the purpose of electronic data communication, storage and processing within and outside the Center
2.11. Secured Network segment: A network segment is a specially configured subset of a larger network, bounded by devices capable of regulating the flow of packets into and out of the segment, including routers, switches, hubs, bridges, or multi-homed gateways (but not simple repeaters), and is secured by a firewall.

2.12. Unsecured Network segment: A network segment that is not secured by a firewall.

2.13. Identification: The process that enables recognition of a user by a system, generally by the use of unique, machine-readable User IDs.

2.14. User ID: A unique character string that is used by a system to identify a specific user. It may also be referred to as username, user account, profile, user profile, login name, or login account

2.15. Password: A secret word, sentence, or code used to validate a user's identity to access an information system or service. Passphrases differ from passwords only in length. Passwords are usually shorter (from 8 to 12 characters) while passphrases are usually longer (up to 100 characters and more)

2.16. Authentication: The process of identifying an individual is usually based on a username and password. Authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be but says nothing about the access rights of the individual. Three types of factors are used to provide authentication:

2.16.1. something you know [e.g. a password],
2.16.2. item you have [e.g. a certificate or card],
2.16.3. something you are [e.g. a fingerprint or retinal pattern].
2.16.4. Using any two in conjunction is known as multi-factor authorization.

2.17. ICT systems: include but are not limited to computer equipment, software, operating systems, database systems, storage media, network accounts, e-mail, internet access, copying and printing systems, the telephone system (including voicemail), network backups and electronic archives, including systems hosted or controlled by third-party vendors of the Centre. Since technology changes quickly, other systems may be added to this definition as appropriate.

2.18. ICT resources and assets: include but are not limited to computer equipment, software, operating systems, database systems, storage media, network accounts, e-mail, internet access, copying and printing systems, the telephone system (including voicemail), network backups and electronic archives, including systems hosted or controlled by third-party vendors of the Centre. Since technology changes quickly, other systems may be added to this definition as appropriate.

2.19. Disclaimer Statement: Text added to a document to explicitly state how the content of the message can or cannot be used.

2.20. Information Incident: An adverse event affecting an information asset or resource that has caused or has the potential to have an adverse effect on the Centre, its staff or its partners

2.21. ICT Service Providers: External entities how provide ICT related services to the Center. This may range from a company installing air-conditioning or network cabling to a cloud hosting provider or specialist consultant.

2.22. Change Advisory Committee (CAC): The group of individuals who are accountable for reviewing, assessing, and approving system and configuration changes in the Center ICT services.

2.23. Change Solution owners: The individuals with accountability for specific systems and services who have requested changes which need to be approved by the EMC.

2.24. Artificial intelligence (AI): refers to technologies that enable computers and machines to simulate human capabilities such as learning, comprehension, problem solving, decision making, creativity and autonomy.

3. Access to ICT Resources and Information Assets

3.1. Purpose

3.1.1. The purpose of this document is to communicate the AfricaRice' policy, access to ICT resources and information assets

3.2. Scope

3.2.1. This policy governs user identification, authentication, and authorization via the AfricaRice Identity and Access Management (Active Directory) system. It applies to:

3.2.1.1. Endpoints
3.2.1.2. Networks
3.2.1.3. Applications
3.2.1.4. Data/Information

3.2.2. It does not cover controls relating to visitor temporary access to unsecured segments of the network for the purpose of granting Internet or extranet access. Nor does it cover access to specific applications run on the system - these are subject to specific AfricaRice policies which may provide for:-

3.2.2.1. "single sign on", in which case the standards applied to network access will also apply to the application access or:-
3.2.2.2. additional access controls for specific applications.

3.2.3. Access enforces least privilege, Role-Based Access Control RBAC, and MFA Multi Factor Authentication. Exclusions: visitor Internet access, app-specific controls, cloud/SaaS, and physical security.

.

3.3. Policy Statement

3.3.1. Access to any AfricaRice ICT resource is controlled and authenticated using an accredited User ID. . User IDs identify and administer user accounts; they are assigned only to eligible individuals, who are responsible for all activities performed under their User ID.

3.3.2. Access to AfricaRice ICT resources is governed by the *Information System Access Account Procedures*

3.3.3. Before a User Account is created the user should be made aware of, and should accept as a condition of access as stipulated in the AfricaRice Information System Security Charter

3.3.4. Users are responsible and accountable for all actions including information retrieval or communication on the AfricaRice' network performed using their User ID and credentials.

3.3.5. Generic network accounts should be disabled or locked down where possible and any exceptions should be documented. Generic (shared) network accounts must be disabled or restricted wherever possible; any exceptions require documentation and approval.

3.3.6. Privileged access rights (e.g., administrator) must be assigned to separate accounts from those used for routine activities, following the principle of least privilege.

3.3.7. All User IDs will be set to expire at the end of the contract date. Accounts will be extended on confirmation that a valid contract exists. Where a clear business justification exists, the creation and use of a specifically named User ID (e.g., HR Recruitment) or shared User ID for a group of users (e.g., ICT Helpdesk) may be used.

3.3.8. Access requires multi-factor authentication (MFA)

3.3.9. Accounts are reviewed every 6 months

4. Acceptable Use of ICT Resources and Assets

4.1. Purpose

4.1.1. The purpose of this document is to communicate AfricaRice' policy on acceptable use of ICT resources at AfricaRice and to outline expectations of privacy. The policy is in place to protect the employees and the AfricaRice. Inappropriate use can expose the Centre to risks at both a technical level (with potential damage being caused to ICT infrastructure) and at operational level (with misuse of Internet resources leading to possible reputational damage to AfricaRice and a loss in productivity).

4.1.2. AfricaRice intentions for publishing an ICT Privacy and Acceptable Use Policy are not to impose restrictions that are contrary to AfricaRice established culture of openness, trust, and integrity. AfricaRice is committed to protecting AfricaRice' employees, partners, and the organization from illegal or damaging actions by individuals, either knowingly or unknowingly.

4.2. Scope

4.2.1. This document covers an individual's privacy expectations, and the acceptable use of AfricaRice' ICT resources by employees, contractors, consultants, and other staff of the Centre and hosted organizations including all personnel affiliated with partners and third parties. This policy applies to all ICT resources and assets that are owned or leased by AfricaRice.

4.3. Policy Statement

Privacy

4.3.1. While the Center desires to provide a reasonable level of privacy, it should be noted that, information assets of employees, agents, independent contractors, or visitors; created, distributed, accessed, or managed; including all documents, messages or other content created, sent, or received over ICT systems, or stored on ICT systems; are and shall remain the property of the Center. This unavoidably limits personal privacy, and the Centre cannot ensure, and individuals should not assume, the confidentiality of any documents, messages, or other content, sent or received through, or stored on, ICT resources and assets controlled by the Center or its agents.

4.3.2. AfricaRice does not routinely examine or disclose information on its ICT systems. Nonetheless, subject to the procedures detailed below, AfricaRice may deny users access to any ICT system and may examine or disclose information on these systems under the following conditions:

4.3.2.1. When required by and consistent with the law;

4.3.2.2. When AfricaRice has reason to believe that a violation of law or of AfricaRice policies is threatened or has taken place.

4.3.2.3. When there are compelling circumstances where failure to act may result in significant harm to AfricaRice or an individual associated with AfricaRice.

4.3.2.4. Under time-dependent, operational circumstances.

Acceptance of Use

4.3.3. Users of the AfricaRice ICT resources and assets are expected to use them responsibly and securely in a manner that minimizes the risk of detrimental impact to AfricaRice. That is, to

comply with all applicable country and local laws, with this and other AfricaRice policies, and with normal standards of professional and personal courtesy and conduct.

4.3.4. All information stored or transmitted through the AfricaRice' ICT resources and assets must conform to law and the AfricaRice policies regarding protection of intellectual property, including laws and policies regarding licensing, copyright, patents, and trademarks. One should assume that material created by others, in electronic or other forms, is protected by copyright unless such material includes an explicit statement that it is not protected or unless such material is clearly in the public domain.

4.3.5. AfricaRice' ICT resources and assets should be used primarily for research and official business purposes.

4.3.6. AfricaRice ICT resources and assets must not be used for:

- 4.3.6.1. Unlawful, fraudulent or libelous activities;
- 4.3.6.2. Commercial purposes not under the auspices of AfricaRice
- 4.3.6.3. Personal financial gain
- 4.3.6.4. Political activities
- 4.3.6.5. Activities that put the reputation of AfricaRice or its employees at risk
- 4.3.6.6. Activities that violate other AfricaRice policies or guidelines.
- 4.3.6.7. Accessing, downloading, viewing storing or transmitting sexually explicit or pornographic material.

4.3.7. AfricaRice will not take any responsibility for the security of any personal information transmitted by staff (such as for personal e-commerce transactions or banking transactions) using AfricaRice provided Internet connections or email system, including any consequential losses sustained because of the transmission of this information.

4.3.8. AfricaRice retains the right to deny access to any ICT system and may examine or disclose online information that AfricaRice ICT resources, and assets have been used to access in line with the Privacy statements section

Prohibited Activities (Extended)

4.3.9. ICT resources must not be used for

- 4.3.9.1. Distribution of malware, phishing, or ransomware
- 4.3.9.2. Access to high-risk sites (e.g., known malware hosts, dark web)
- 4.3.9.3. Unauthorized circumvention tools (personal VPNs, proxies)
- 4.3.9.4. Bandwidth-intensive personal activities (streaming, P2P file sharing)

Enforcement

4.3.10. Violations result in

- Immediate suspension or revocation of ICT access
- Disciplinary action as provided in the AfricaRice Staff Management Policy
- Legal action or referral to law enforcement where applicable.

Training Requirements

4.3.11. All users must complete cybersecurity awareness training covering

- Phishing recognition and data protection
- Incident reporting procedures.

5. Security of ICT Resources and Assets

5.1. Purpose

5.1.1. The purpose of this document is to communicate AfricaRice' policy on ICT resource and asset security that has be put in place to minimize loss, damage or compromise of ICT assets and interruption to AfricaRice activities

5.2. Scope

5.2.1. The purpose of this document is to communicate the Centre' policy on ICT resource and asset security that has be put in place to minimize loss, damage or compromise of ICT assets and interruption to Centre activities

5.2.2. Implementing this policy is an important component of ensuring that potential threats to the overall ICT security position of AfricaRice are managed effectively.

5.3. Policy Statement

5.3.1. Implement human, organizational, and technological security controls to preserve the confidentiality, availability and integrity of AfricaRice' information systems and the information held therein.

5.3.2. Develop and maintain appropriate policies, procedures, and guidelines to affect a high standard of information technology security, reflecting industry's best practice.

5.3.3. Monitor, record and log certain activities on AfricaRice network and use of its information technology resources.

5.3.4. Comprehensively assess and manage risks to AfricaRice information systems and the information held therein.

5.3.5. Continuously review and improve AfricaRice information technology security controls and rapidly determine the cause of any breach of security and minimize damage to information systems should any such incident occur.

5.3.6. Comply with all laws and regulations governing information technology security.

5.3.7. Establish information technology security education and awareness initiatives within AfricaRice

6. Change Management of ICT Resources and Assets

6.1. Purpose

6.1.1. This document outlines policies for ICT Change Management for AfricaRice.

6.1.2. Change management is a critical success factor for any ICT project. The successful completion of a change process requires that the resulting product complies with the organization's policies, is aligned with the organization's objectives, meets the business requirements and is delivered on time and within budget.

6.2. Scope

6.2.1. This is a Center-wide Policy and is applicable to all parties operating within the organization's network environment or utilizing Information Resources.

6.2.2. It covers the data, networks, LAN servers and personal computers (stand-alone or network-enabled), located at organization offices and organization production related locations, where these systems are under the jurisdiction and/or ownership of the organization or subsidiaries, and any personal computers, laptops, mobile device and or servers authorized to access the organization's data networks. No employee is exempt from this policy.

6.2.3. The policy applies to all changes to be made to ICT systems & processes. However, all changes will be evaluated for risk and impact to determine whether the way their execution will be managed.

6.3. Policy Statement

6.3.1. All changes to an ICT resource/service that exceed a certain cost, risk or complexity must be submitted to, reviewed, and approved by a change advisory committee.
6.3.2. The committee is chaired by the ICT Manager or the Change Manager and includes ICT unit representatives.
6.3.3. The purpose of the committee is to understand, authorize and schedule proposed changes to the Centre's production ICT environment.
6.3.4. ICT Stakeholders from outside of ICT (e.g., Finance, Research etc.) may be invited to attend the committee meetings as required.
6.3.5. The committee has the authority to re-schedule, deny or request further detail regarding any Change Request.
6.3.6. The committee must maintain, track, and communicate all Change Requests using appropriate methods.
6.3.7. The committee is responsible for management but not execution activities.
6.3.8. The ICT Manager or the Change Owner, not the committee, is responsible for the success of their respective changes.
6.3.9. A documented audit trail, maintained at a Business Unit Level, containing relevant information shall be always maintained. This should include changing request documentation, changing authorization and the outcome of the change. No single person should effect changes to production information systems without the approval of other authorized personnel.
6.3.10. A risk assessment shall be performed for all changes and dependent on the outcome, an impact assessment should be carried out.
6.3.11. All changes require tested rollback plans
6.3.12. Rollback mandatory for negative impact on critical services

7. Incident Management

7.1. Purpose

7.1.1. Information incidents giving rise to threats to the confidentiality, integrity, and availability of AfricaRice' information are increasingly a part of everyday business. AfricaRice, through its information governance and security policies, seeks to minimize the frequency of such incidents.
7.1.2. The aim of this policy is to ensure that ICT Team and AfricaRice staff react appropriately to any actual, or suspected, security incidents relating to any of its information, be it digital, paper-based or any other media

7.2. Scope

7.2.1. This policy applies to all staff, contractors, consultants, students/interns, and associates who use AfricaRice' information, ICT facilities and equipment, or have access to, or custody of, AfricaRice' data or information. It applies to all information stored or transmitted through AfricaRice' ICT resources and assets.
7.2.2. All users must understand and adopt use of this policy and are responsible for ensuring the safety and security of the Centre's information assets.
7.2.3. All users have a role to play and a contribution to make to identifying potential risks to the safe and secure use of information and any Information technology.

7.3. Policy Statement

7.3.1. All information incidents will be reported to a single contact point (Service Desk), but distinction is drawn from that point between ICT technical incidents (e.g., malware, software malfunction, hacking incidents) and those involving disclosure of manual records or end user behavior, which will necessarily follow different investigation and incident management routes as stipulated in the Incident Management Guidelines led by the ICT manager.

7.3.2. Establish an Information Risk Register to include all identified risks arising from information incidents.

8. ICT Resource Acquisition

8.1. Purpose

8.1.1. AfricaRice is a research organization with a diverse range of information system needs. ICT takes place in three main spaces – infrastructure/personal productivity, business systems, science and research related. These have different budget authorizations and management which do not include ICT.

8.1.2. This policy provides a "light touch" approach to ensure visibility of all resource acquisition and investment, including hardware, software, consulting or contracting expertise or cloud services or other ICT related services. In this way the ICT team can maintain an overview and record of the expenditure and investments being made and the technologies and systems being deployed across the institute.

8.1.3. The intention is for the ICT team to be an aggregator of information and knowledge, to be able to advise and guide on ICT strategy and investment. It will also be able to identify opportunities for efficiencies and synergies.

8.2. Scope

8.2.1. This policy applies to all staff, contractors, consultants, students/interns, associates, hosted organizations, and their staff who use AfricaRice' information, ICT facilities and equipment. The policy addresses all actions to deploy or invest in information systems, services, or other resources.

8.2.2. All users, departments and hosted organizations must understand and adopt the use of this policy and are responsible for engaging and communicating their plans in the appropriate manner.

8.3. Policy Statement

8.3.1. If an outstation, department, project, or individual are going to spend money on or deploy an information system, they should involve the ICT Manager at the conceptualizations stage, to provide enough time for proper review and consultation.

8.3.2. The ICT Manager will make recommendations to the departments proposing or the center leadership in the interests of ICT security, ICT strategy, AfricaRice business plan, or other factors.

9. Roles and Responsibilities

9.1. Board of Trustees

9.1.1. Approval of this policy, all changes and amendments to this policy.

9.2. Director General

9.2.1. Review, approve and implement the provisions of this Policy

9.2.2. Review and approve investment proposals for ICT resources acquisitions

9.3. Executive Management Committee (EMC)

9.3.1. Recommend updates and revisions to this policy
9.3.2. Review investment proposals for ICT resources acquisitions.
9.3.3. Review and approve any exceptions to the requirements of this policy
9.3.4. Advise and mediate when ICT Manager and program leader/budget holder are not in agreement in relation to ICT resource acquisitions

9.4. Director of Corporate Services

9.4.1. Approve all proposed changes to the ICT resources/services

9.5. ICT Manager

9.5.1. Develop, implement and maintain this policy.
9.5.2. Review and recommend any exceptions to the requirements of this policy.
9.5.3. Take proactive steps to reinforce compliance of all stakeholders with this policy.
9.5.4. Implement, maintain and update the change management procedures with input from all stakeholders.
9.5.5. Review documentation prepared on project related ICT resources acquisition and related expenditure.
9.5.6. Analyze proposed investments for alignment with AfricaRice ICT strategy, workplan and possible synergies or interfaces with existing or planned systems in AfricaRice.
9.5.7. Meet with program leader/budget holder to review findings and discuss any suggested changes for ICT resource acquisition.
9.5.8. Documenting and implementing AfricaRice' ICT information incident management procedures.
9.5.9. The ICT Manager is responsible for documenting and implementing AfricaRice' ICT information incident management procedures.
9.5.10. The ICT Manager is also responsible, with support from Information Owners/Custodians, for ensuring that all incidents are subject to investigation and subjected to information risk management processes.

9.6. ICT Unit

9.6.1. The identification, implementation, and management of appropriate security controls necessary to safeguard Africa network (LAN/WAN) and supporting infrastructure.
9.6.2. The implementation of system-level security controls as defined by the information owner or the Director General.
9.6.3. The provision of facilities for information backups on network servers and other centralized information stores and backups of the hard disks on individual computers.
9.6.4. The provision of services which enable authorized user's access to appropriate electronic information systems and data.
9.6.5. Liaising with and advising AfricaRice' management, individual users, and line managers on the appropriate actions to take in the event of an actual or suspected breach of data security.
9.6.6. Shall comply with all change management and control statements of this policy.
9.6.7. Report on all deviations from the change management plans
9.6.8. The Information Incident Single Point of Contact (Service Desk) procedures must ensure that all events that are reported, are promptly recorded and forwarded to the appropriate staff for action

9.7. Information Owners/Custodians

9.7.1. The implementation of this policy and all other relevant policies within AfricaRice directorate or service they manage.

9.7.2. The ownership, management, control and security of the information and information systems deployed by their directorate or service on behalf of AfricaRice.

9.7.3. Maintaining a list of AfricaRice information systems and applications which are managed and controlled by their directorate or service.

9.7.4. Ensuring that adequate procedures are implemented within their directorate or service, so as to ensure all AfricaRice employees, contractors, sub-contractors, agency staff and third parties that report to them are made aware of and are instructed to comply with this policy and all other relevant policies.

9.7.5. Ensuring that adequate procedures are implemented within their directorate or service to ensure compliance with this policy and all other relevant policies.

9.8. Staff and other Users

9.8.1. Complying with the terms of this policy and all other relevant AfricaRice policies, procedures, regulations, and applicable legislation.

9.8.2. Respecting and protecting the privacy and confidentiality of the information they process at all times.

9.8.3. Complying with instructions issued by the ICT Department on behalf of AfricaRice.

9.8.4. Complying with the instructions and requirements of information owners whose information or information systems they use.

9.8.5. Reporting all misuse and breaches of this policy to the ICT Manager or their line manager immediately.

9.9. ICT Services Providers

9.9.1. Any information security incident that involves AfricaRice' information must be reported without delay.

9.9.2. This should be a contractual requirement where a service contract exists and included in any information sharing agreement for the sharing of personal information.

9.9.3. AfricaRice managers and staff must be aware of similar obligations to other agencies if a security breach involves their information.

9.9.4. Shall comply with all change management and control statements of this policy.

10. Review

10.1. This policy will be reviewed every three years or earlier if required by the ICT Manager.

10.2. Any changes made to the Policy will be presented to the Executive Management Committee (EMC) for endorsement and thereafter submitted to the Board of Trustees for approval.

11. Related Documentation

11.1. Conflict of interest Policy

11.2. Staff Management Policy

11.3. AfricaRice ICT Business Continuity Plan -2021

11.4. CGIAR – ICT Policies

11.5. AfricaRice - SOP - Information System Access Account

11.6. AfricaRice - Information Systems Security Charter

11.7. ICT Incident Management Guidelines

11.8. AfricaRice Open Access and Data Management Policy
11.9. Data Sharing Policy
11.10. IT Change Management Procedures