ICT POLICY

The ICT Policy of Africa Renewal University outlines the all-encompassing structure that oversees the utilization, administration, and safety of information and communication technology assets in the institution. This policy makes sure that ICT resources are used efficiently, safely, and morally in order to further the institution's goal of providing high quality education and transformational leadership for the church and society. It provides precise rules for data security, infrastructure management, software control, network access, and ICT support services. By abiding by this policy, all AfRU community members support the upkeep of a strong, safe, and effective ICT environment that supports administrative and academic activities while preserving the university's core values and legal compliance.

Table of Contents

Definition of Terms

ICT (Information and Communication Technology): Refers to all technologies used for communication and the management of information. This includes hardware (computers, servers, network devices), software (applications, operating systems), and communication technologies (email, internet, social media).

ICT Directorate: The administrative unit within Africa Renewal University responsible for overseeing all aspects of ICT management, including strategic planning, policy implementation, and resource allocation.

Data Protection: Measures and practices designed to safeguard sensitive and personal data from unauthorized access, alteration, or destruction. This includes encryption, access controls, and secure data storage.

Network Security: The protocols and tools used to protect the university's network infrastructure from unauthorized access, cyber threats, and other security risks. This includes firewalls, intrusion detection systems, and regular security updates.

Software Licensing: The legal permission and agreements required to use software. Proper licensing ensures that software is used in compliance with legal requirements and prevents unauthorized use.

IT Service Support: Services provided to assist users with technical issues related to ICT resources. This includes help desk operations, incident management, and maintenance of IT systems.

Infrastructure Management: The process of overseeing and maintaining the physical and virtual components of the university's ICT infrastructure, including hardware, networks, and data centers.

Backup and Recovery: Procedures and practices for creating copies of critical data and restoring it in the event of data loss or corruption. Regular backups and tested recovery plans are essential for data protection.

ICT Procurement: The process of acquiring ICT equipment, software, and services. This involves evaluating needs, selecting vendors, and ensuring that acquisitions meet university standards and requirements.

ICT Disposal: The process of properly disposing of outdated or surplus ICT equipment, ensuring that data is securely erased and that disposal complies with environmental and university policies.

Social Media: Online platforms and tools used for sharing information, communication, and networking. University-managed social media accounts must adhere to specific guidelines to maintain the institution's image and values.

Accessibility: The design and implementation of ICT resources to ensure they are usable by individuals with disabilities. This includes providing assistive technologies and ensuring that digital content is accessible to all users.

Training Programs: Educational initiatives aimed at enhancing the ICT skills of students, faculty, and staff. This includes workshops, seminars, and online courses related to the use of technology, security practices, and emerging trends.

Incident Management: The process of identifying, managing, and resolving ICT-related incidents, including technical issues and security breaches. This ensures prompt response and effective resolution to minimize impact.

Help Desk: A centralized support service that assists users with technical problems and queries related to ICT resources. The help desk acts as the first point of contact for resolving issues.

Policy Compliance: Adherence to established ICT policies, procedures, and legal requirements. Compliance ensures that ICT resources are used in accordance with the university's standards and regulations.

Preamble

Africa Renewal University (AfRU) continues to provide its staff, students and stakeholders, a number of computing devices and services in light of the overall goal of streamlining effective and efficient work processes at the University.

Appropriate and planned use and adoption of ICTs is key in enabling the university to achieve it vision and ensuring managed use of the available ICT resources as well as planning for resources that might not readily be available.

This policy is a guide on how the university shall operationalize and ensure the responsible and optimum use of its ICT capacity to ensure operational excellence in consideration of consistent, fair and controlled use and adoption of ICT technologies.

The policy shall be implemented to serve the university staff, students and visitors through the existing university governance structure with AfRU's Computing Services as the key functional and technical unit of the university.

1. Introduction

Africa Renewal University (AfRU) recognizes the critical role of Information and Communication Technology (ICT) in enhancing educational delivery, administrative efficiency, and research capabilities. This policy is designed to ensure that ICT resources are used effectively, securely, and ethically to support the university's mission of providing transformative Christian education and fostering a supportive academic environment. As technology continues to evolve, it is imperative that ARU maintains robust policies to protect its data, ensure equitable access, and promote best practices in ICT management.

2. Problem Statement

The rapid advancement of technology presents both opportunities and challenges. AfRU faces issues related to the security of sensitive data, unauthorized use of resources, compliance with legal requirements, and the need for continuous improvement in ICT infrastructure. Without a comprehensive and detailed ICT policy, the university risks compromising its data integrity, failing to comply with legal standards, and not fully leveraging technological advancements to support its mission.

3. Policy Statement

AfRU is committed to the responsible and ethical use of ICT resources. This policy sets forth guidelines to ensure the effective management of ICT infrastructure, the protection of data, and the support of academic and administrative functions. All members of the AfRU community are expected to adhere to these guidelines to foster a secure and productive ICT environment.

4. Policy Goal

The goal of this ICT Policy is to establish a framework that ensures the effective, secure, and ethical use of ICT resources at Africa Renewal University, supporting the institution's mission and enhancing its educational and administrative functions.

5. Objectives

- Effective Use: Optimize the use of ICT resources to support teaching, research, and administration.
- Security: Protect the integrity, confidentiality, and availability of university data and information.
- Compliance: Ensure adherence to legal and regulatory requirements.
- Responsibility: Promote responsible and ethical use of ICT resources among all university members.
- Education: Provide ongoing training and capacity building in ICT skills.

6. Legal Framework

This policy is designed to comply with relevant national and international laws and regulations, including:

- Data Protection Act or equivalent local regulations
- The National ICT Policy (2014)
- The National Information Technology Act (2009)
- The National e-Government Policy Framework (2011)
- The National E-Waste Management Policy (2012)
- The Computer Misuse Act (2011)
- The Anti-Pornography Act (2014)
- The Electronic Signatures Act (2011)
- The Copyright and Neighbouring Rights Act (2006)
- The PPDA Act, 2003
- The National Development Plan; Uganda Vision 2040
- The Universities and Other Tertiary Institutions Act, 2001
- Africa Renewal University Human Resource Manual, 2013
- Intellectual Property Rights laws
- Cybersecurity laws and regulations
- Licensing agreements and software compliance requirements

7. ICT Governance

The ICT Team

1. **Director of ICT:** The Director of ICT heads the ICT Directorate and is responsible for strategic planning, policy development, and overall management of the university's ICT infrastructure. The Director ensures that ICT initiatives align with the university's goals and objectives, oversees major projects, and represents the ICT Directorate in senior management discussions.
2. **IT Manager:** The IT Manager reports to the Director of ICT and is responsible for the day-to-day management of IT operations, including overseeing the implementation of ICT policies, managing IT staff, and ensuring that systems are running efficiently. The IT Manager coordinates with various departments to address their ICT needs and issues.
3. **IT Operations Officer:** Reporting to the IT Manager, the IT Operations Officer handles the operational aspects of the ICT infrastructure, including system administration, network management, and maintenance of hardware and software. The IT Operations Officer ensures that all IT systems are functional, secure, and compliant with university policies.
4. **Support Team:** The Support Team, led by the IT Operations Officer, provides technical assistance to students, faculty, and staff. They are responsible for resolving technical issues, managing the help desk, and ensuring user satisfaction with ICT services. The Support Team also conducts routine checks and updates to maintain the quality and performance of IT services.

In brief, the University ICT Team shall have its representation as determined by the University management, and shall be mandated to;

- Oversee the development and implementation of ICT related policies for the university
- Have an oversight on security of all ICT assets, facilities and logistical requirements.
- Advocate for appropriate budgetary allocation of the University total budget to ICT related activities and initiatives.
- Approve, monitor and review ICT implementation developmental projects for the university
- Approve, monitor and review annual ICT budgets and work plans for the university

The University Computing Services

The AfRU Computing Services shall provide the ICT management function of the university, and shall be mandated to;

- Provide technical and professional leadership to ICT implementations and developments in the university
- Operationalize the ICT policy implementation
- Ensure optimized utilization of ICT resources in the university
- Ensure legally and environmentally acceptable acquisition, use and disposal of ICT resources

Academic and Administrative Units

Heads of Academic and Administrative units shall in consultation with AfRU Computing Services;

- Ensure integration of ICTs into their activities
- Comply to ICT policy framework

Staff and Students

The staff and students of the university shall comply to the ICT policy regulatory framework.

8. University ICT Network Access

Access Control: Access to the university's ICT network will be controlled through secure authentication mechanisms. Users must be granted access based on their roles and responsibilities.

Network Security: The university will implement firewalls, intrusion detection systems, and other security measures to protect the network from unauthorized access and cyber threats.

Usage Monitoring: Network usage will be monitored to ensure compliance with this policy and to detect and respond to potential security incidents.

9. Software Management and Use

Licensing: All software used on university devices must be properly licensed. Unauthorized software installation is prohibited.

Updates and Patches: Software must be regularly updated and patched to protect against vulnerabilities and ensure compatibility with other systems.

Software Acquisition: Requests for new software must be reviewed and approved by the ICT department to ensure compatibility and licensing compliance.

10. IT Service Support

Help Desk: A centralized help desk will be available to provide support for ICT-related issues and to assist users with technical problems.

Incident Management: All ICT incidents must be reported to the help desk for resolution. Incident response procedures will be in place to address issues promptly and effectively.

Service Levels: Service levels and response times will be defined and communicated to users to manage expectations and ensure timely support.

11. Infrastructure Management

Hardware Maintenance: University-owned hardware must be maintained in accordance with manufacturer guidelines and university policies. Regular maintenance schedules will be established.

Infrastructure Upgrades: Upgrades to ICT infrastructure must be planned and executed to minimize disruption and ensure compatibility with existing systems.

Asset Management: An inventory of all ICT assets will be maintained, and assets will be tracked throughout their lifecycle.

12. Data and Information Security

Data Protection: Sensitive and personal data must be encrypted and stored securely. Access to such data will be restricted to authorized personnel only.

Backup and Recovery: Regular backups of critical data will be performed, and recovery procedures will be tested to ensure data can be restored in case of loss or corruption.

Incident Response: Procedures for responding to data breaches or security incidents will be established and followed to mitigate risks and address any impacts.

13. ICT Procurement & Disposal

Procurement: All ICT procurement must be conducted through approved channels, with consideration given to cost, compatibility, and compliance with university standards.

Disposal: Outdated or surplus ICT equipment must be disposed of in accordance with environmental regulations and university policies, ensuring that data is securely erased before disposal.

14. Social Media

Usage: Social media accounts related to the university must be managed according to university guidelines. Personal use of social media should not interfere with university operations or violate privacy policies.

Content: Content posted on university social media channels must be accurate, respectful, and aligned with the university's values and mission.

15. Special Needs ICT Use

Accessibility: ICT resources must be accessible to individuals with disabilities. The university will provide assistive technologies and ensure that digital content meets accessibility standards.

Support: Specialized support and training will be provided to ensure that all users, including those with special needs, can effectively use university ICT resources.

16. ICT Skills Capacity Building

Training Programs: Regular training programs will be conducted to enhance ICT skills among students, faculty, and staff. Training will cover various aspects of ICT use, security, and emerging technologies.

Professional Development: Opportunities for professional development in ICT will be provided to keep staff updated with the latest technological advancements and best practices.

Awareness Campaigns: Awareness campaigns will be conducted to promote understanding of ICT policies and the importance of data security and responsible use.

17. Conclusion

This ICT Policy is integral to maintaining a secure, efficient, and ethical ICT environment at Africa Renewal University. By adhering to these guidelines, the university community can contribute to the effective use of technology, support the university's mission, and uphold the values of integrity and responsibility.