RHODES UNIVERSITY
Grahamstown • 6140 • South Africa

Policy on ICT Governance

Policy Volume	Support Services
Policy Chapter	Information & Technology Services
Responsible Committee/Unit/Division/Faculty	Information and Communications Technology Committee
Responsible Chairperson/Director/Manager	Director: Information & Technology Services
Dates of First and Subsequent Council Approvals	
Policy Approval Pathways (e.g. committee, Senex, Senate, Council)	Director: Information & Technology Services → ICTC → Senate → ARC → Council
Revision History: Approved Reviews	2024
Review Cycle (e.g. every 2/5/7 years etc)	Every 3 Years
Next Review Date	2027

1. POLICY PARTICULARS

1.1. Policy Title	Policy on Governance of ICT
1.2. Policy Statement	This Policy seeks to give approval for governance of ICT. Delegating the authority to the I&TS Division in order to ensure security risks and technology are properly governed to reduce exposure and ensure that the technology contributes soundly to the teaching and learning goals, within a financially sustainable framework.
1.3. Reason for Policy	This Policy gives approval for the protocols within a technology service to be updated and changed when necessary. Technology changes required to address risk must be agile and adapt quickly. King IV recognises information separately from technology as a corporate asset and requires disclosure on the structures and processes for information and technology, key focus areas, mechanisms for monitoring and information management.
1.4. Policy Objective/s	This Policy aims to collate an agreed list of protocols that guide the ICT framework at Rhodes University. Procurement, Access, Cybersecurity and Risk, Acceptable Use and emerging strategies will exist under the umbrella of the Policy on Governance of ICT.
1.5. People affected by this Policy	All units of the University
1.5. Who should read this Policy	Members of ICTC, F&GP, Audit and Risk Committee and Council All users of Rhodes University ICT
1.6. Implementers of this Policy	Information & Technology Services Division
1.7 Website address/link for this Policy	TBC

2. RELATED DOCUMENTS, FORMS, TOOLS AND GUIDELINES

Relevant Legislation
King IV Protection of Personal Information Act (POPIA)
Related Policies
Acceptable Use Policy (AUP) Access to Information Policy POPIA Policy
Related Protocols
Protocol on password security standards Protocol to obtain access to processes on core University admin system Protocol to obtain access to the finance system Protocol to obtain access to the payroll system and ESS Protocol to obtain access to current systems governed under I&TS control Protocol on Identity Management Framework Protocol to obtain access to central authentication services Protocol on procurement and write-off of ICT asset equipment Protocol on procurement of ICT software and systems including cloud-based services Protocol on maintenance of systems and network Protocol on Data Information Security including Document Management and Protection Protocol on Cybersecurity and Mitigation of Risk Protocol on Management of Cloud-based storage Protocol on release of changes to Core Admin System

Forms and Tools

Access to ICT Information Application Form
Guest Application Form
Stolen laptop Form

Guidelines

Passwords
Email
Network Connection
AUP Examples

3. POLICY DEFINITIONS

No	TERM	DEFINITION
3.1	AUP	Acceptable Use Policy
3.2	ICT	Information and Communications Technology
3.3	POPIA	Protection of Personal Information Act
3.4	SSO	Single Sign On

4. PRINCIPLES GOVERNING THIS POLICY

OVERVIEW

Rhodes University strives to carry out the following, as far as is reasonably practicable:

4.1. Ensure that ICT is updated regularly to ensure that technologies used are not out of date

4.2. Ensure that cybersecurity risk is minimised within the context of a small research-intensive University

4.3. Ensure that disruption to research, teaching and learning is minimal with regular short maintenance windows

4.4. Ensure that longer maintenance windows are properly planned and executed

4.5. Ensure that role-based access is appropriate and authorised

4.6. Ensure that governance controls are appropriate and necessary

4.7. Ensure that vulnerability assessments and findings are responded to timeously

4.8. Ensure that risk is reduced by mitigation activities if the risk cannot be entirely removed

4.9. Ensure that ICT Business Continuity is recognised and forms part of the University Business Continuity Plan

4.10. Ensure that the ICT Disaster protocols or recovery are recognised and form part of the University Disaster Recovery Plan, delegating the operational maintenance of backups and restore to the I&TS Division

5. DIRECTIVES FOR IMPLEMENTING THIS POLICY

5.1. I&TS will maintain the protocols keeping them up to date and relevant. ICTC will approve these annually

5.2. I&TS will publish the protocols on the I&TS page on the intranet

5.3. I&TS will comply with the Procurement Policy and Delegation of Authority Framework

5.4.	External audit will review the protocols aligned to this Policy, recognising the authority of the Policy has been delegated to the I&TS Division
5.5.	Recognising that areas of ICT risk should not be publicly available, I&TS will keep an ICT risk register securely held within the I&TS Division and review all risk regularly with intention to mitigate and remove where possible
5.6.	I&TS will report regularly on cybersecurity and risk at the Audit and Risk Committee.
5.7.	As per the ICTC Terms of reference, ICTC will discuss strategy to inform the ICT governance framework, procurement processes, systems architecture and medium term to long term ICT solutions

6. ROLES AND RESPONSIBILITIES

ROLE	**RESPONSIBILITY**
University Line Managers	Follow processes aligned to protocols that govern access to roles, information, procurement
I&TS Division	Ensure that the protocols are up to date and published on the intranet Maintain ICT services
Director I&TS	Report regularly to Audit and Risk on developments and trends within cybersecurity Ensure that the annual external audit reviews governance and protocols and effects change where necessary
ICTC	Oversight of ICT Strategy and policies Inform Audit and Risk Committee when necessary
Audit and Risk Committee	Advise Council on the maturity of ICT governance in the University. Working with F&GP, ensure that relevant and sustainable financial support is provisioned for enhancement of ICT equipment, services and security

7. CONTACTS

Area of Concern	**Division/Faculty/Department**	**Telephone**	**Email**
Security vulnerabilities and general concerns	Director I&TS	7456	N.Ripley@ru.ac.za
Failure from I&TS to respond to concerns raised	DVC: RISP	8055	dvc.research@ru.ac.za

8. POLICY REVIEW PROCEDURE

The Policy will be reviewed every 3 years. The associated protocols will be updated regularly and tabled for noting at ICTC who have the authority to oversee ICT strategy within the University
Communication of Policy changes will be via Toplist.