ICT USER POLICY

UTHUKELA ECONOMIC DEVELOPMENT AGENCY

2026/2027 FINANCIAL YEAR

POLICY TITLE	**ICT USER POLICY**
DATE APPROVED	**29 MAY 2026**
IMPLEMENTATION DATE	**01 JULY 2026**
REVIEW DATE	

Contents

1. PURPOSE

The purpose of this ICT User Policy is to:

- Ensure the secure, responsible, and lawful use of ICT resources.
- Protect UEDA information assets.
- Define acceptable use standards for employees, contractors, and stakeholders.
- Provide clear guidance on password security, data protection, and remote working.
- Ensure compliance with applicable legislation including the Protection of Personal Information Act (POPIA).

2. SCOPE

This policy applies to:

- All employees (permanent, temporary, interns)
- Contractors and consultants
- Board members
- Any person granted access to UEDA ICT resources

It applies to all ICT resources, including:

- Laptops and portable devices
- Wi-Fi and internet connectivity
- Email systems
- Cloud services and outsourced IT platforms
- Printers and shared drives
- Remote access systems.

3. ICT ENVIRONMENT OVERVIEW

UEDA operates with:

- Company-issued laptops
- Office Wi-Fi network
- Cloud-based and outsourced IT services managed by an external IT service provider
- Business email accounts
- Remote working capability

The outsourced IT provider is responsible for infrastructure maintenance, cybersecurity monitoring, backups, and technical support, under service level agreements (SLAs).

4. ACCEPTABLE USE POLICY

4.1. General Use

ICT resources are provided strictly for official UEDA business purposes.

Limited personal use is permitted provided it:

- Does not interfere with work duties
- Does not consume excessive network resources
- Does not violate any laws or this policy
- Does not expose UEDA to cybersecurity risks.

4.2. Prohibited Activities

Users may NOT:

- Access, download, or distribute illegal, offensive, or inappropriate content
- Install unauthorized software
- Share login credentials
- Disable antivirus or security controls
- Connect unauthorized devices to UEDA Wi-Fi
- Use UEDA ICT resources for personal business activities
- Attempt to bypass security controls.

4.3. Email Usage

Users must:

- Use official email accounts for official communication
- Verify external email attachments before opening
- Report suspicious emails (phishing attempts) immediately
- Avoid sending sensitive information without encryption

Email accounts remain the property of UEDA.

5. PASSWORD REQUIREMENTS

5.1. Password Standards

All system passwords must:

- Be at least 12 characters long
- Include uppercase, lowercase, numbers, and special characters
- Not contain easily guessed information (names, birthdays)
- Be unique (not reused across systems)

5.2. Password Protection

Users must:

- Never share passwords
- Never write passwords on visible surfaces
- Use password managers if approved
- Change passwords immediately if compromise is suspected

Multi-Factor Authentication (MFA) must be enabled where available.

6. DATA PROTECTION & INFORMATION SECURITY

6.1. Data Classification

Information shall be classified as:

- Public
- Internal
- Confidential
- Highly Confidential (e.g., personal information, financial records)

6.2. Protection of Personal Information (POPIA Compliance)

Users must:

- Process personal information lawfully and for legitimate business purposes
- Only access information necessary for their role
- Not share personal data without authorization
- Report data breaches immediately

6.3. Storage & Backups

- All official documents must be saved on approved cloud/shared drives.
- Saving official documents on personal devices is prohibited.
- Backups are managed by the outsourced IT provider.
- USB storage devices are discouraged and must be encrypted if used.

6.4. Data Breach Reporting

Any suspected data breach must be reported immediately to:

- The ICT Service Provider
- The Information Officer / CEO

Failure to report incidents may result in disciplinary action.

7. REMOTE WORKING POLICY

7.1. Approved Remote Work

Remote work must be formally approved by management.

7.2. Secure Remote Access

When working remotely, users must:

- Use only company-issued laptops
- Connect via secure Wi-Fi (no public Wi-Fi without VPN)
- Use VPN if provided
- Lock screens when away from device
- Ensure family members do not access company devices.

7.3. Physical Security

Users must:

- Keep laptops secure at all times
- Not leave devices unattended in vehicles
- Report lost or stolen devices immediately.

8. WIFI USAGE POLICY

- UEDA Wi-Fi is for official use.
- Guest Wi-Fi (if available) must be separated from internal network.
- Users may not share Wi-Fi passwords externally.
- Personal hotspots should not be used in the office without approval.

9. OUTSOURCED IT SERVICE MANAGEMENT

The outsourced IT provider is responsible for:

- Cybersecurity monitoring
- Antivirus management

- System updates and patching
- Data backups
- Disaster recovery support
- User access management (on instruction from management)

UEDA management remains accountable for:

- Access approval
- Policy enforcement
- POPIA compliance
- Risk oversight

10. USER RESPONSIBILITIES

Each user is responsible for:

- Safeguarding company devices
- Protecting passwords
- Reporting incidents immediately
- Complying with this policy
- Completing basic cybersecurity awareness training.

11. MONITORING & PRIVACY

UEDA reserves the right to:

- Monitor email and internet usage
- Audit system access logs
- Investigate suspected policy violations

Monitoring will be conducted in accordance with applicable legislation.

12. NON-COMPLIANCE

Failure to comply with this policy may result in:

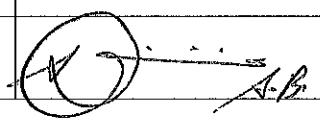
- Disciplinary action
- Revocation of system access
- Legal action where applicable
- Termination of employment or contract

13. POLICY REVIEW

This policy shall be reviewed:

- Annually
- After any major security incident
- Upon significant technology changes

14. APPROVAL BY:

NAME	SIGNATURE	DESIGNATION	DATE
MR SB SIBISI		ACTING CHIEF EXECUTIVE OFFICER	29/05/2026