LIMPOPO

PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
CO-OPERATIVE GOVERNANCE,
HUMAN SETTLEMENTS & TRADITIONAL AFFAIRS

REVIEWED ICT EQUIPMENT USAGE POLICY

Version: 3

Table of Contents

I. Acronyms and Abbreviations

3G	Third Generation
CoGHSTA	Cooperative Governance, Human Settlement and Traditional Affairs
GITO	Government Information Technology Office(r)
ICT	Information Communication Technology

II. Clarification of Terms

Accountability: ensuring that the actions of an entity/individual may be traced uniquely to that entity/individual, which may then be held responsible for that action.

Authentication: establishing the validity of a claimed entity/verification of the identity of an individual or application.

Availability: being accessible and useable upon demand by an authorized entity.

Confidentiality: the principle that information is not made available or disclosed to unauthorized individuals, entities or processes.

Identification and authentication: functions to establish and verify the validity of the claimed identity of a user.

Information and communication systems: applications and systems to support the business, utilizing information technology as an enabler or tool.

Information technology: any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of vocal, pictorial, textual and numerical data or information.

Integrity: the inherent quality of protection that maintains the accuracy of entities of an information and communication system and ensures that the entities are not altered or destroyed in an unauthorized manner.

Monitoring: performance measurement to ensure the confidentiality, availability and integrity of operational systems and information.

Password: confidential authentication information composed of a string of characters.

Remote access: the access of remote users to corporate IT services by means of telephone lines or 3G data card through a gateway/computing that is performed at a location that is distant from a central site, over a network connection.

Third Generation (3G) Networks: Mobile technology and standard used to access the Internet.

1. Preamble

One of the most crucial responsibilities of an organization is the protection of its equipment or assets. The same is true for Department of Co-operative Governance, Human Settlements and Traditional Affairs (COGHSTA). Recognizing that ICT equipment amounts to a reasonably large portion of the departmental budget, it is necessary for COGHSTA to put mechanisms and controls in place to ensure and encourage proper and efficient use of these assets.

Department of Co-operative Governance, Human Settlements and Traditional Affairs Limpopo avails computer equipment and network infrastructure for all staff members to enhance departmental operations and enable seamless exchange, storage and processing of information. While the use of computer equipment is crucial to boosting overall productivity and ultimately improving service delivery to the public, COGHSTA can/may incur unnecessary costs and be subject to legal liabilities, arising from misuse or monopolization of the equipment. This policy aims to ensure that COGHSTA leverages the investment in its ICT infrastructure

2. Purpose and objectives

The purpose of this policy is to provide the COGHSTA with an ICT Equipment Usage Policy in order to apply an effective and consistent standard for the ICT equipment and software in use by the Department.

The objectives of this policy are:

2.1. Clearly state rules governing usage of COGHSTA computers and networks.

2.2. Encourage responsible and proper use of COGHSTA information systems.

2.3. Help ensure a COGHSTA computer and network infrastructure that supports COGHSTA objectives and operational requirements.

3. Scope of Application

This policy applies to all COGHSTA employees, contractors, service providers and others who are granted access to COGHSTA information systems. This includes but not limited to computers, associated peripherals and software.

4. Legal Framework

4.1 The following publications govern the execution of the Internet Use Policy and were taken into consideration during the drafting of the Internet Use Guidelines and Policy:

4.1.1 State Information Technology Act (Act no 88 of 1998)

4.1.2 Protection of Information Act (Act no 84 of 1982)

4.1.3 Minimum Information Security Standards (MISS), Second Edition March 1998

4.1.4 Departmental Email Policy

4.1.5 Departmental Password Policy

4.1.6 Departmental ICT Security Policy.

5. Administration of the policy

GITO is responsible for enforcing this policy and continuously ensuring monitoring and compliance.

6. Policy Content

6.1 Software

6.1.1. Software Installation

6.1.1.1. For purposes of complying with copyright laws and minimizing computer threats, only COGHSTA authorized software must be installed on computers and this must be done by authorized GITO staff only.

6.1.1.2. Computer users must not intentionally develop, use or distribute computer programs or software to disrupt other computer systems, information systems or damage software and hardware or bypass system security mechanisms and controls. More precisely, users must not use any software that may threaten the Confidentiality, Integrity and Availability of information and information systems. The use of any unauthorised or destructive program may result in legal civil action for damages or other punitive action by third parties, including COGHSTA, as well as criminal action.

6.1.1.3. All divisions shall purchase computer hardware and software through GITO. These divisions should clearly motivate the need for any special software or hardware.

6.1.1.4. Software under testing or evaluation must under no circumstances be installed on production computers including computers, laptops and servers. Evaluation software must be installed on IT equipment designated as test equipment and whenever possible separated from the production network. GITO has the sole authority to allocate ICT equipment for testing purposes.

6.2. Software Change Control

6.2.1. All software shall be held in a lockable cabinet held at GITO.

6.2.2. Software taken from the cabinet by authorized staff shall be recorded in a software register and upon return be signed back into the register.

6.2.3. GITO shall license all appropriate software.

6.2.4. Should an official require specialized software than currently available, the official shall motivate this in writing coupled with authorisation from the official's supervisor. GITO will at its discretion evaluate the merits of each software request.

6.3. Reporting Incidents

Business Software Alliance randomly carries out audits to prevent illegal use of software and as a result hefty fines may be imposed for use of unlicensed software. Illegal use of any software must be reported to GITO immediately.

6.4. Computer Equipment

6.4.1. Protection of ICT Equipment Off-Premises

6.4.1.1. Users shall ensure that COGHSTA ICT equipment is protected while in use away from COGHSTA premises regardless of ownership. The security of the equipment should wherever possible be equivalent to on-site use of the equipment. The following applies to ICT equipment away from the office:

6.4.1.2. Users shall not leave ICT equipment unattended in public places;

6.4.1.3. By removing ICT equipment from COGHSTA premises, users acknowledge the increased risk of theft and/or loss, thus users must take all necessary precautions to protect and disguise this equipment. This can include using non-conventional laptop bags such as back packs and keeping equipment away from public eyes;

6.4.1.4. Only users who have been authorised to remove specific ICT equipment from the premises, shall be allowed to use the equipment off-site;

6.5. Equipment Change Control

6.5.1. All problems and changes to the computer equipment must be registered with the ICT Helpdesk at telephone extension 2490

6.5.2. No unauthorised staff may alter any software and hardware configuration.

6.6. Transfer if Equipment between Users

6.6.1. The transfer of ICT equipment shall be managed by Supply Chain Management and all requests for transfers has to be submitted to Supply Chain Management.

6.7. Standardization of Hardware and Software

6.7.1. GITO personnel shall from time to time, ensure that ICT equipment in COGHSTA is standardized as much as possible to minimize resources needed for maintenance, therefore users shall be required to comply with any recommendations as prescribed by GITO. Simply, this means that users will not bypass or attempt to bypass or disregard controls implemented by GITO.

6.7.2. Additionally GITO shall standardize computer software and hardware for users based on but not limited to job function, division and the least privilege principle. This will help avoid unnecessary software license costs.

6.7.3. Should a user require specialized hardware than the current standard, the user shall motivate this in writing authorized by the user's superior. GITO shall at its discretion evaluate the merits of each hardware request.

6.7.4. Computer hardware shall only be modified by authorized GITO staff.

6.7.5. All computers shall come standard with Antivirus software to protect against viruses and malicious computer programs.

6.8. Stolen computers

Stolen computers shall be reported to Supply Chain Management and handled in terms of Supply Chain management policies.

6.9. Unattended User Equipment

6.9.1. It is the sole responsibility of users to ensure the protection of ICT equipment which have been assigned to them by COGHSTA. All laptop users shall be assigned with a laptop lock to prevent theft. Users shall ensure that they know how to physically secure their laptops. Offices, computer rooms and storage facilities shall also be locked when unattended. Failure to apply necessary protection for equipment shall constitute neglect and the user may be held liable for the loss.

6.9.2. Users shall terminate active sessions or log out of their computers when moving away from the workstation unless they lock the computer in which case they would be required to re-enter the password. No computer may be left unlocked.

6.10. Disposal and Reuse of Equipment

6.10.1. It may be necessary for the department to dispose of older or obsolete ICT equipment to make way for faster and more efficient computers. In this case GITO shall take the sole responsibility of ensuring that all licensed software is removed and all stored information is securely overwritten. Any individual who disposes any ICT equipment without the secure removal of data will be exposing COGHSTA to compromise and unauthorised disclosure of information, thus will be in direct breach of this policy.

6.10.2. In cases where previously used ICT equipment including laptops, personal computers or memory sticks are reassigned to another COGHSTA employee, GITO shall ensure that all information is securely deleted to protect the confidentiality of information.

6.11. ICT Equipment by Category

6.11.1. Critical ICT Equipment

To ensure that critical business activities take place and prevent loss, damage or compromise of critical assets, critical ICT equipment shall be protected from various security threats and environmental hazards. The following special controls shall govern the security of this critical equipment:

6.11.1.1. All critical system such as servers, switches, routers, printers used to print pay slips shall be stored in a physically secured environment protected by access control.

6.11.1.2. Owners of critical ICT equipment shall implement the highest possible protection of these assets against failure, disaster, unauthorised access, tampering and periodically review security breaches and misuse.

6.11.1.3. Owners of critical ICT equipment shall keep updated copies of configurations, operational procedures and usage guidelines to ensure continuity of operations after failures and prevent a single point of failure wherever possible.

6.12. Laptops

6.12.1. Officials that have been allocated or provided with laptops shall be responsible for the safety and custodianship of the laptop in the office and outside the office.

6.12.2. When it is in use, a notebook PC shall be fitted with a Kensington lock cable which shall be hooked to an immovable object to make it difficult to steal. The lock will be supplied with the notebook PC.

6.12.3. On connection to a local area network (LAN), a notebook that has been out of office shall be automatically updated with the latest antivirus signature file by a server. This is done in the background, and a user may not observe or be aware of this action.

6.12.4. An employee who has been issued with a notebook PC shall ensure that his or her security access control identification card bears the departmental inventory number of the notebook PC. Security and Risk Management division must be contacted in this regard.

6.13. Printers

6.13.1. Users shall be required to share printers on the network based on physical proximity and division in order to avoid unnecessary costs.

6.13.2. Users of printers shall take into account that printer resources such as cartridges and paper are not infinite and refrain from misuse of printers and printing of personal documents.

6.13.3. GITO shall ensure that all management interfaces of printers are protected by a password to prevent unauthorised use or configuration.

6.13.4. Recognizing that documents can be processed and stored on computers, users shall take care to optimize printing resources by only printing when a paper copy is necessary.

6.13.5. Sensitive or classified printed documents shall immediately be removed from the printer after printing to prevent unwanted information disclosures.

6.13.6. Printers that are dedicated to printing confidential information such as pay slips, invoices and cheques shall be stored in areas where physical access is strictly controlled. These areas should be clearly marked to deter unauthorised access. It is the responsibility of each division to protect such sensitive printers.

6.13.7. Only authorized maintenance personnel shall carry out printer repairs.

6.14. Personal Use

While ICT equipment is allocated to ensure that users have the necessary tools to carry out their official duties, it is inevitable that equipment will be used for personal use. While this is not prohibited, the use of ICT equipment for personal use should be in a responsible manner that does not incur unnecessary costs to COGHSTA. The following guidelines govern personal use of ICT equipment:

6.14.1. Equipment should not be used to process, distribute or store any data or information protected by copyright laws /or intellectual property rights as this can lead to legal action;

6.14.2. Computers must not be used to play games or perform any activities that may contribute to decreased employee productivity.

6.15. House Keeping

Users shall use COGHSTA ICT equipment responsibly in line with the following housekeeping rules:

6.15.1. Offices with ICT equipment shall be locked when leaving the office to prevent theft amongst other things;

6.15.2. ICT Equipment shall not be placed next to heaters or air conditioners as humidity and heat can shorten the life of internal computer components.

6.15.3. Users shall not eat, drink or smoke next to ICT equipment as this cause damage to the equipment and could be a health and safety risk;

6.15.4. Only damp cloths with suitable cleaning fluids shall be used when cleaning computer keyboards, screens, printers and other ICT equipment;

6.15.5. Whenever possible, ICT equipment shall not be connected to the same electric power as other power consuming devices. Red plugs should only be used for ICT equipment;

6.15.6. For purposes of information backups, GITO has put in place mechanisms to synchronize information on the user's computer to a central file server. As a result all files in the "My Documents" folder shall be backed up daily. Users shall not store any multimedia files like videos and music in this folder. These files shall be moved from this folder to the "C drive". It is the joint responsibility of the user and GITO to ensure that these files are relocated.

6.16. Movement of ICT Equipment to and from COGHSTA premises

6.16.1. ICT equipment shall not be moved from COGHSTA premises without authorisation from Supply Chain Management. This authorisation shall be in the form of a laptop card or an "Authority to remove GG equipment from Premises Form" obtainable from Supply Chain Management.

6.16.2. All removed ICT equipment shall be logged back in upon return by signing in the equipment register at security, except in cases where associated laptop cards are produced. Spot checks will be made from time to time to ensure that removed assets are returned.

6.16.3. All other ICT equipment taken into COGHSTA premises shall be signed in at security services at reception areas.

6.16.4. In case of repairs, authorized GITO personnel shall provide Supply Chain Management with the copy of the removal form. Only GITO personnel shall be allowed to complete removal forms for repairs.

6.17. Computer user's responsibilities

6.17.1. Users shall ensure proper use of ICT equipment in accordance with all provisions of this policy.

6.17.2. Users are required to report any misuse of ICT equipment or alert GITO of potential threats to ICT equipment.

6.17.3. It is the user's responsibility to seek guidance from GITO or any related division in the department when in doubt of what constitute acceptable or prohibited use of ICT equipment.

6.17.4. While security of ICT equipment is the primary responsibility of Security Services, users must take note that they share this responsibility.

6.17.5. All users shall sign an "ICT Issued or Returned Equipment Form" as an agreement to comply to this Equipment Usage Policy and abide by all its provisions

7. Default

Non-compliance with this policy shall constitute violation of the policy and shall be treated in terms of the departmental disciplinary code and procedure policy

8. **Inception Date**

This policy comes into effect from the date of approval by Member of Executive Council

9. **Policy Review**

This policy shall be reviewed bi-annually

10. **Enquiries**

Enquiries about the policy should be directed to the Government Information Technology Office

Document Title	ICT Equipment Usage Policy
Compiled by :	Government Information Technology Office Senior Manager (ICT Infrastructure and Systems) 24/12/2014 Date
Acknowledge by :	General Manager (GITO) Acting 24/12/2014 Date
Qualified by:	Senior Manager (Research and Policy Coordination) 24/12/2014 Date
Recommended by:	Senior General Manager (Corporate Services) 05th/01/2015 Date
Adopted by :	Head of Department 07/01/2015 Date
Approved by :	Member of the Executive Council 07/01/2015 Date