

## DEPARTMENT OF AGRICULTURE

### PROCUREMENT, SAFEKEEPING AND MAINTENANCE OF INFORMATION AND COMMUNICATION TECHNOLOGY RESOURCES POLICY

#### 1. OBJECTIVE

The purpose of this policy is to ensure that procurement of equipment is compliant with prescribed procedures in terms of the Acts, to ensure that accountability for assets and to reduce the risks of human error, theft fraud or misuse of equipment and facilities at acceptable level.

#### 2. PROCEDURES TO BE FOLLOWED TO PROCURE HARDWARE AND SOFTWARE

##### 2.1 Requisition of assets

User's request for computer equipment or resource must be in writing and authorized by user's head of component, of at least the rank of the Director or equivalent. The appropriate Information Technology request form should be filled adequately. To ensure proper procedures for the submission of IT requests to the Departmental IT Committee for recommendation and approval, the following is requested:

2.1.1 A completed typed IT request form must be submitted (not to be filled by hand). The applicant should request electronic IT request form from IT section.

2.1.2 Section 6 (Motivation part) of the IT request should be dealt with adequately. Please do not assume that the committee knows your problem but motivate in

full to ensure that the committee will have a clear picture of your situation. Failure to do so will result in to your application been sent back.

- 2.1.3 The IT section should compile the specification of items required (hardware and software).
- 2.1.4 The IT request should reach this office in 10days prior the DITC meeting. No request will be processed further in that month if received late. If your request is late, it will be considered in the next month meeting. The dates of DITC will be circulated within the department.
- 2.1.5 After approval, the Information technology Section will contact applicants to collect their requests. The applicant should complete the LOG 1 from as prescribed and submit it to the Procurement section for further processes. The approved IT application must be attached to LOG 1. No amendments must be made on the approval, unless again approved by the HOD.
- 2.1.6 The replacement of the old equipment must be done via the appropriate steps. The old equipment must be return to the IT section in exchange of the new equipment. The IT section should redistribute the usable equipment via the recommendation of the DITC. The unserviceable equipment must be disposed off through Asset Management Section. Usable hard disk drives must be formatted before it is re-distributed to other members in the department. If it is redundant it must be exposed off properly as is prescribed in the (MISS) Minimum Information Security Standards.
- 2.1.7 Information Technology Section should schedule dates Departmental Information Technology Committee meeting.

2.1.8 Where additional computer hardware and software may have to be procured, the relevant DIT committee must be approached and the normal procurement procedures should be followed. Information Technology section will liaise with all relevant service providers and ensure that the relevant and necessary equipment would be delivered.

2.2 IT resources are classified into the following groups:

2.2.1 Hardware assets such as computer equipment (CPU, Monitor, Keyboard, Laptops, Modems, Hubs, Routers, Cable, Switch, Fly Lead, Projector, Digital Camera, Web-Cam, Printer, Mouse, CD-Writer).

2.2.2 Software assets such as application and network operating system software.

2.2.3 Information assets such as database, data files, system documentation, user manuals, floppy data tapes and any form of item used for backup system.

2.2.4 Any other equipment which can be linked to the network and computer.

### **3. TRANSIT-IN OF IT RESOURCES (AT IT SECTION)**

3.1 Software and (or) hardware resources must be received at Transit-In of IT section.

3.2 The responsible person should check and ensure that item description, specification and amount correspond with computer generated order form. Assistance can be obtained from Network Controller for expertise.

- 3.3 The assets must be given an inventory number for reference, be recorded on the asset register indicating the item description, serial number, make and model, etc.
- 3.4 The items should be given to the Network Controller by way of register and relevant forms must be signed by both parties. The person who is issuing items must ensure that the person receiving items signs the relevant forms.

#### **4. IT SECTION RESPONSIBILITY**

4.1 The responsible IT person should do the following:

- 4.1.1 Install legal software on the computer equipment.
- 4.1.2 Configure computer before is given to the user.
- 4.1.3 Check and ensure that anti-virus definitions are up to date. Ensure that the latest patches and updates are loaded.
- 4.1.4 Record user's details for instance, name, surname, e-mail address, room number, building, place, etc on the IT register of the department.
- 4.1.5 Specify the description of hardware and software for instance, IP address, MAC address, serial number, Product ID number, license number, item description, make, model, etc.
- 4.1.6 Provide relevant access codes and passwords directly to the user. User has the right to change choose the password and access codes.
- 4.1.7 Helpdesk official must record the details of hardware, software and user to the Computerized

4.1.8 Inventory Recording.

4.1.9 Provide user with basic training in terms of relevant program, system and hardware.

4.1.10 Ensure that the user has received and signed for relevant IT policies

4.1.11 Ensure that 'Confidentiality of Information' form is signed by the user.

4.1.12 Hardware and software must be handed over to the user by way of register

## **5. RESPONSIBILITY OF MANAGEMENT AND SUPERVISOR**

5.1 Head of Component/Managers must ensure that IT section is informed immediately of the following changed circumstances regarding a user so that access right may be revoked or the level of access changed appropriately and immediately:

5.1.1 When the user terminated the service.

5.1.2 When the user is transferred to different position within or outside a department.

5.1.3 When there is a change of duties and original and access level requested is no longer required.

5.1.4 When the hardware resource is removed from its original location or be re-allocated to another person(s) or function(s) must be done with written permission from IT section. Managers should first obtain such permission from

the relevant DITC committee. Handing over of item certificate should be completed in-full.

## **6. USER RESPONSIBILITY**

- 6.1 The hardware and software allocated to a particular employee becomes his/her responsibility.
- 6.2 Hardware and software allocated to section or Directorate becomes responsibility of Head of Component.
- 6.3 IT resources must be used for official purposes only.
- 6.4 Users must take all reasonable precaution to ensure that equipment is secured.
- 6.5 Hardware and software must not be left unattended during office hours unless the doors are locked.
- 6.6 User must request written permission from his/her Director of the Component to use equipment at home for permanent or temporary period such as weekend. A copy should be forwarded to IT section. The official utilizing official's computer hardware and software at home will be responsible for safeguarding it in all respect.

## **7. MAINTENANCE OF COMPUTER EQUIPMENT**

- 7.1 Users should report hardware and software faults and require assistance directly from Helpdesk of IT section.

- 7.2 The user should report fault(s) between 7H30 and 16H00 during five working days
- 7.3 Users are not allowed to report directly to the supplier or technician or Network Controller.
- 7.4 In the event of a fault being outstanding for more than 48 hours or no reasonable or satisfactory feedback being received, the user may initiate the following procedures:
- 7.3.1 Fault(s) unresolved for longer than 24 hours may be referred to Information Technology Manager,
- 7.3.2 Should a fault(s) be considered urgent or should any further information be required, the IT Manager may be contacted directly. IT section should initiate appropriate actions to have such faults or problems repaired or resolved as soon as possible. IT authorized person manning the Helpdesk will at all times endeavor to resolve faults immediately and telephonically, within five to ten minutes. If a fault cannot be resolved within five to ten minutes, the call will be terminated and fault will be referred to Technician for further actions.
- 7.5 Only authorized maintenance personnel of IT should carry out repairs and service equipment.
- 7.6 Item descriptions and serial number should be recorded in the relevant form. The user should request a handing-over of equipment certificate from the authorized person. The user should keep a copy and authorized person should keep original form in the register.

- 7.7 Authorised person should keep the records of equipment when is send out to the supplier. The authorized person should ensure that the supplier completes and sign a handing over certificate.
- 7.8 Hard disk drive must be removed and kept in a safe place within the department and the rest of the PC can be send to the supplier. If PC returns the hard disk drive can be re-installed and PC issued to the user.
- 7.9 Faulty hard disk drives must be replaced in the department and destroyed by proper means (according to MISS).
- 7.10 Authorized person must reflect the hardware and software description (for instance, item serial number, model, make, etc) in the register.

## **8. SAFEKEEPING OF IT RESOURCES**

- 8.1 Authorised user of equipment should prevent loss, damage or compromise of software and hardware.
- 8.2 IT resources should be physically protected from security threads, and environmental hazards.
- 8.3 Necessary protection mechanism should be adopted and implemented to minimize the risk of potential threads including threads, theft, direct sunlight, fire, explosive, smoke, water, dust, vibrations, chemical effects and electromagnetic radiation.
- 8.4 Users must not repair hardware and software in anyway.



- 8.5 Users must not scratch, hit, kick or stand on hardware. Installed programs or settings must not be tampered with or/and changed.
- 8.6 Treat computer equipment with care and keep it in lockable environment at all times. Clean printers when changing ribbons and cartridges. Clean computer equipment regularly with special computer cleaning materials.

## **9. LAW ENFORCEMENT**

- 9.1 Computer users of this department who violate the content of this policy or perform any other illegal action in relation to rules and regulations outlined in this policy will be subject to disciplinary actions in terms of the Disciplinary Code and Procedures of the Public Service.
- 9.2 Should the department suffer any loss or damage through the illegal actions for proven negligence of computer usage, such value of loss or damage will be recovered from the person responsible in accordance with Regulation 12 of the Treasury Regulation 2001.

## **10. WRITTEN AGREEMENT REQUIRED**

- 10.1 All computer users of the department must acknowledge acceptance of and compliance with the 'Procurement, Safekeeping and Maintenance' policy by signing the attached declaration.
- 10.2 The declaration is attached as Annexure 'A'. Each Manager must ensure that signed declarations of all computer users are received and placed on record. A copy of signed declaration must be forwarded to Departmental Information Technology Services Component.

10.3 The user should give employer consent to intercept his or her communication and/or privacy by signing the declaration form. This is in line with Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No.70 of2002).

## 11. PARTIES CONSULTED

- National Intelligent Agency
- Department of Premier - State Law Advisors

DEPARTMENT OF AGRICULTURE

DECLARATION BY

Name: \_\_\_\_\_

Persal: \_\_\_\_\_

IP Address: \_\_\_\_\_

Directorate: \_\_\_\_\_

Hereby declare that, I

\_\_\_\_\_  
(Print Name and Surname)

Have;

- 1. read and understood the contents of the Policy" Procurement, Safekeeping and Maintenance of IT resources"
- 2. agree to comply with the contents mentioned in the above-mentioned policy
- 3. will be subject to disciplinary action in terms of the Disciplinary Code and Procedures of the Public Service for violation of the above-mentioned policy
- 4. allow my employer to investigate and institute charges against me for any violation of this policy
- 5. give my employer permission to intercept my communication, privacy and government property (hardware and software) in terms of Regulations of Interception of Communications and Provision of Communication Related Information Act, 2002 (Act No.70 of 2002)

SIGNATURE OF USER

DATE: \_\_\_\_\_

WITNESS

DATE: \_\_\_\_\_

3  
4  
5  
6  
7  
8  
9  
10