INFORMATION COMMUNICATION TECHNOLOGY

POLICY ON ICT SECURITY
2014/2015
TABLE OF CONTENTS

1. Preamble .................................................................................................................. 1
2. Regulatory and Guidance Framework ..................................................................... 1
3. Scope of Application ............................................................................................... 2
4. Purpose .................................................................................................................... 2
5. Responsibilities ....................................................................................................... 3
   5.1 The Head of Department ...................................................................................... 3
   5.2 Government Information Technology Officer (GITO) ......................................... 3
   5.3 ICT Manager ....................................................................................................... 3
   5.4 Internal Audit ..................................................................................................... 4
   5.5 Security Services ............................................................................................... 4
6. ICT Security Risk Assessment ................................................................................ 5
7. Third Parties and Contractors .............................................................................. 5
8. Asset management .................................................................................................. 5
9. Server room ............................................................................................................ 6
11. Desktop Security .................................................................................................... 6
12. Mobile Devices ...................................................................................................... 7
13. Removable devices ................................................................................................ 7
14. Network Security .................................................................................................. 8
15. Logical Access ...................................................................................................... 8
16. Password .............................................................................................................. 8
15. Internet and Email ................................................................................................ 10
16. BAS, Persal, Walker, HSS, IMMIS ...................................................................... 10
17. Malicious Software .............................................................................................. 11
18. Firewall and Antivirus ......................................................................................... 11
19.1. Incident Management ....................................................................................... 12
19.2. HSS, Persal, BAS, User Account Management Procedures ............................. 12
20. Information system acquisition, development and maintenance ....................... 13
21 ICT Disaster Recovery Plan .................................................................................. 13
# Glossary of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICT</td>
<td>Information Communication Technology</td>
</tr>
<tr>
<td>dlghs</td>
<td>Department of Local Government Human Settlements</td>
</tr>
<tr>
<td>Department</td>
<td>Department of Local Government and Human Settlements</td>
</tr>
<tr>
<td>COBIT</td>
<td>Control Objectives of Information and related technology</td>
</tr>
<tr>
<td>ITIL</td>
<td>Information Technology Infrastructure Library</td>
</tr>
<tr>
<td>MISS</td>
<td>Minimum Information Security Standard</td>
</tr>
<tr>
<td>MPSS</td>
<td>Minimum Physical Security Standard</td>
</tr>
<tr>
<td>CGICTPF</td>
<td>Corporate Governance of ICT Policy Framework</td>
</tr>
<tr>
<td>HoD</td>
<td>Head of Department</td>
</tr>
<tr>
<td>GITO</td>
<td>Government Information Technology Officer</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreements</td>
</tr>
<tr>
<td>NWPG</td>
<td>North West Provincial Government</td>
</tr>
<tr>
<td>Sensitive Information</td>
<td>This includes any strategic information of the department, such</td>
</tr>
<tr>
<td>SITA</td>
<td>State Information Technology Agency</td>
</tr>
<tr>
<td>SSA</td>
<td>State Security Agency</td>
</tr>
<tr>
<td>Stakeholders</td>
<td>Auditor General, Provincial Internal Audit, GITO Council, SITA, SSA)</td>
</tr>
<tr>
<td>Critical Information</td>
<td>Information is designated as critical information if its unavailability would have a catastrophic adverse impact on the following:</td>
</tr>
<tr>
<td></td>
<td>- Client or employee life, safety, or health.</td>
</tr>
<tr>
<td></td>
<td>- Payment to suppliers or employees.</td>
</tr>
<tr>
<td></td>
<td>- Revenue collection.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Communications</td>
<td></td>
</tr>
<tr>
<td>Legal or regulatory</td>
<td></td>
</tr>
<tr>
<td>Official devices</td>
<td>Items provided with permission to access the departmental resources.</td>
</tr>
<tr>
<td></td>
<td>E.g. Desktop, Laptops etc</td>
</tr>
<tr>
<td>Information Systems</td>
<td>A combination of hardware, software, infrastructure and trained personnel</td>
</tr>
<tr>
<td></td>
<td>organized to facilitate planning, control, coordination, and decision</td>
</tr>
<tr>
<td></td>
<td>making in an organization.</td>
</tr>
<tr>
<td>Information Technology(I.T.)</td>
<td>The study or use of systems (especially computers and telecommunications)</td>
</tr>
<tr>
<td></td>
<td>for storing, retrieving, and sending information.</td>
</tr>
<tr>
<td>User</td>
<td>Employee or any authorized person utilising departmental ICT equipment</td>
</tr>
<tr>
<td>Server</td>
<td>A software program, or the specialised computer on which that program runs,</td>
</tr>
<tr>
<td></td>
<td>that provides a specific kind of service to client software running on the</td>
</tr>
<tr>
<td></td>
<td>same computer or other computers on a network.</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standard for Organization</td>
</tr>
<tr>
<td>SACSA</td>
<td>Special Assistant for Counterinsurgency and Special Activities</td>
</tr>
<tr>
<td>Filr</td>
<td>Software by Novell used for backup and remote access of user information</td>
</tr>
<tr>
<td>PIA</td>
<td>Provincial Internal Audit</td>
</tr>
<tr>
<td>BAS</td>
<td>Basic Accounting System</td>
</tr>
<tr>
<td>PERSAL</td>
<td>Personnel Salaries</td>
</tr>
<tr>
<td>HSS</td>
<td>Housing Subsidy System</td>
</tr>
</tbody>
</table>
1. PREAMBLE

People, hardware, software, telecommunications, facilities and data form an Information and Communications Technology system that is highly effective and productive. All ICT systems entail the creation of a condition to protect computer hardware, software, and data against incidental and/or deliberate unauthorized changes, destruction, disposal, removal and disclosure. Securing the integrity, confidentiality and availability of the computers and technology systems of the department against threats such as sabotage, unauthorized intrusions, malicious misuse or inadvertent compromise is of paramount importance for the operational effectiveness of all activities of the department.

All users are expected to sign the ICT Policy declaration form (Annexure A), failing which equipments shall not be allocated to them.

2. REGULATORY AND GUIDANCE FRAMEWORK

i. Public Service Act (Proclamation No 103 of 1994)
ii. Protection of Information Act 84 of 1982
iii. Promotion of Access to Information Act 2 of 2000
iv. Protection of Personal Information Act of 2013
vi. Regulation of interception of communication and provision of communication-related information Act 70 of 2002
vii. Copyright Act 98 of 1978
viii. Archives and Records service of South Africa Act 43 of 1996
x. Public Finance Management Act 1 of 1999 (as amended by Act 29 of 1999)
xii. Minimum Information Security Standard
xiii. Minimum Physical security Standard
xv. COBIT 5 Information Security Standards
xvi. ITIL
xvii. ISO 17799
xviii. ISO 27000 series
xix. ISO 38500
xx. SACS/A/090/1(4) "Communication Security in the RSA".
xxii. Electronic Communications and Transactions Act (no. 25 of 2002)
xxiii. Communication –related information Act (Act no. 70 of 2002)
xxv. Provincial Asset management framework
xxvi. CGICTPF

3. SCOPE OF APPLICATION

The ICT Security policy is applicable to all employees within the department, third parties and stakeholders utilizing the department's ICT resources and facilities in pursuit of the Department’s Goals and Strategic Objectives.

4. PURPOSE

The purpose of the ICT Policy is to ensure the effective protection and proper usage of the computer systems and its peripherals within the Department. Each employee of the department is responsible for the security and protection of electronic information resources over which he or she has control. Resources to be protected include but are not limited to networks, computers, software, removable media and data. The physical
and logical integrity of these resources must be protected against threats such as sabotage, unauthorized intrusions, malicious misuse or inadvertent compromise.

5. RESPONSIBILITIES

5.1 The Head of Department
5.1.1 The HoD bears the responsibility of overseeing the development, approval, accountability and implementation of the ICT Security Policy.

5.2 Government Information Technology Officer (GITO)
5.2.1 Is responsible for the oversight of development of the ICT policies and strategies, regulations, standards, norms, guidelines, best practices and procedures.
5.2.2 Shall coordinate ICT Security with the ICT Manager.
5.2.3 Shall manage the relationship with all stakeholders that supply Information Technology products and services; this is done by ensuring that all Business Agreements and SLAs are adhered to.
5.2.4 Shall monitor and ensure compliance with relevant ICT regulatory framework and policies.
5.2.5 The GITO shall provide a holistic view of the department’s current ICT security posture.

5.3 ICT Manager
5.3.1 Shall ensure that the ICT directorate foresees the implementation of all ICT Security processes in the department by the Security Manager.
5.3.2 Shall ensure that the ICT Security Policy conforms with the Information Security Plan.
5.3.3 In consultation with the GITO shall recommend all ICT projects of the department to the HoD.
5.3.4 In consultation with MISS shall ensure that all ICT service providers undergo all security procedures before providing services to the department.

5.3.5 Shall identify ICT risks.

5.3.6 Shall provide recommendations on remedial actions to be taken to solve all ICT risks faced by the department.

5.3.7 Shall ensure that ICT Directorate complies with the Risk Management Policy.

5.4 Internal Audit

5.4.1 NWPG internal Audit shall audit all ICT Compliance within the department.

5.4.2 NWPG internal Audit shall assist ICT Directorate in ensuring that recommendations provided from the audit findings are implemented correctly.

5.5 Security Services

5.5.1 Shall ensure that all ICT physical security breaches are reported to the ICT Directorate.

5.5.2 Shall in conjunction with the ICT Directorate ensure that the Information Security Policy is implemented and complied with.

5.5.3 Shall ensure the screening of all ICT service providers.

5.5.4 Shall in conjunction with ICT Directorate be responsible for physical protection of all ICT assets of the department.

5.5.5 Shall ensure that all employees having access to business application systems are vetted.

5.5.6 Shall in conjunction with Asset Management ensure that employees of the department are provided with approved movement of ICT assets; {see annexure B for movement of ICT asset}.

5.5.7 It is the responsibility of Security Services to ensure that the department's environment is secured from any internal and external threats.
6. ICT SECURITY RISK ASSESSMENT

6.1.1 ICT Directorate and Security services, shall conduct ICT Security Risk Assessments bi annually.

6.1.2 ICT Security Risk Assessment shall assist in identifying the ICT security risks and estimating the magnitude of the risks identified.

6.1.3 ICT Security Risk Assessment shall be conducted in compliance with the Security Management Policy.

7. THIRD PARTIES AND CONTRACTORS

7.1.1 All ICT Directorate third parties and contractors shall be screened by Security Services before providing services to the Department.

7.1.2 Shall sign a non-disclosure of classified information which shall be provided and archived by the Security Services Directorate.

7.1.3 Shall not be provided with access to the sensitive information unless security clearance is provided to Security Services.

7.1.4 SLA’s shall be signed by and between the department and Third parties and contractors before providing any ICT services to the department.

7.1.5 Shall be accompanied by ICT Directorate members when providing any services.

7.1.6 Shall not be provided with logical access to any critical information systems of the department; logical access shall be provided only with an approved authorization from HoD and GITO; [see annexure C: Third party Logical access Authorization]

8. ASSET MANAGEMENT

8.1. All ICT equipments shall be recorded and /or tagged with an asset tag.

8.2. ICT asset register shall have the following description:

   (a) Value of the asset

   (b) Asset owner
(c) Location of asset
(d) Date of acquisition
(e) Asset Description

8.3. All employees provided with ICT equipment shall ensure that such assets are provided with protection from damage and theft; *(this to be included in the Policy Declaration Form: Annexure A)*

8.4. Employees not reporting any damage and theft of allocated ICT equipment shall bear the responsibility and the losses shall be recovered from them.

8.5. This shall be done in compliance with the Asset Management Policy.

9. SERVER ROOM

9.1.1. Servers shall be located in a secure server room that shall be accessed only by authorised ICT employees.

9.1.2. Third parties and contractors shall not access server rooms without any escort from the ICT directorate employees.

9.1.3. Servers shall be accessed only by authorised owners.

10. PATCH MANAGEMENT PROCEDURES

The provision of patches is the responsibility of Central IT. The Department shall comply with Patch Management Policy provided by Provincial IT. Provincial IT shall assist the Department to identify Patch management resources for the Department to update the server and workstations.

11. DESKTOP SECURITY

11.1.1 All desktops provided to employees shall be allocated in accordance with the employee's job description.

11.1.2 Employees shall be given least privileges in desktop operating systems.
11.1.3 Employees shall ensure that they only utilise the equipment for official purposes.
11.1.4 Employees shall only have logical access to their allocated desktop.
11.1.5 No employee, except ICT personnel is allowed to open desktops.
11.1.6 Desktops shall be marked with security cable tie in order to identify if there has been physical temper to the asset.
11.1.7 No desktops shall be removed from the department’s premises without authorisation of Asset Management.

12 MOBILE DEVICES

Mobile devices herein refer to official laptops and official tablets

12.1 Official mobile devices shall be issued to employees in accordance with the SCM and ICT policies.
12.2 All employees issued with official laptops shall ensure that they are also provided with security cables.
12.3 Securing of mobile devices is the sole responsibility of the employee issued with such a device.

13 REMOVABLE DEVICES

Removable devices herein refers to USB Flash Drives, Compact and DVD discs, external Hard-drive and any other removable media storage devices.

13.1 Official removable devices are defined as documents as stipulated in the MISS and the Protection of Information Act 85 of 1985.
13.2 Shall be issued to employees according to their job descriptions.
13.3 All removable devices shall be requested from the ICT Directorate.
13.4 Removable devices that shall be utilised to store classified information shall be installed with an encryption system and users shall be trained as how to use such encryption system.
13.5 Encryption systems to be utilised shall be an approved system by the GITO and ICT Manager.
13.6 Official removable devices shall be locked away in accordance with the Information Security Policy and MISS.
13.7 Any loss of Removeable devices shall be reported to the ICT directorate and to the Security Services within 48 hours.

14. NETWORK SECURITY

14.1.1 Only official desktops and mobile devices shall be connected to the NWPG network.
14.1.2 The department shall not implement any wireless network without consulting the NW ICT Directorate Chief Director.
14.1.4 The Department shall be provided with network security procedures and guidelines by NWPG ICT directorate.

15. LOGICAL ACCESS

A user account management procedure shall be developed in order to achieve protection of the departmental information systems.

16. PASSWORD

16.1.1 Passwords shall be utilised to protect the confidentiality and integrity of the departmental systems.
16.1.2 Passwords to all systems shall not be shared/divulged; users who access other employees resources without authorisation from ICT directorate shall be classified as an ICT security breach.
16.1.3 Users must avoid using guessable passwords such as 12345 or names of animals.
16.1.4 Password length should be a minimum of 6 digits and a maximum of 12.
16.1.5 Password should be alphanumeric.
16.1.6 All users must change default password of email and computers.
16.1.7 New passwords must not be a simple change of the old password. For example, adding a number at the end or alternating between passwords
16.1.8 Every reasonable precaution must be taken to ensure that passwords, accounts and data are adequately secured.
16.1.9 No attempt should be made to find out another user's password, or to gain access to another user's account.
16.1.10 Do not write usernames and passwords on keyboards, walls, monitors, post-it note, table or material. A memorized password is not prone to accidental disclosure.
16.1.11 Passwords may not be saved in an electronic document unless the documents are encrypted and the user ensures that the encryption key cannot be accessed.
16.1.12 Password must not be sent via emails.
16.1.13 Users may use screen saver passwords to prevent unauthorized access when the user moves away from the computer.
16.1.14 Users must change their passwords on a monthly basis
16.1.15 When a password is changed, neither of the previous two passwords may be used

17. REMOTE ACCESS

17.1 Remote Access to operational systems is prohibited; operational systems include amongst others: BAS, Persal and Walker Systems.
17.1.1 The following are approved network resources that shall be allowed to be accessed utilising the internet:
(a) Remedy Online
(b) GroupWise
(c) Filr

18. INTERNET AND EMAIL

18.1.1 Internet and Email shall be accessed by utilising user's credentials.
18.1.2 Internet and Email access granted to employees shall not be abused and shall be utilised only for work related purposes.
18.1.3 Uploading government information in free cloud services is prohibited.
18.1.4 Downloading of pirated software and files is prohibited and employees caught doing so shall be warned for abusing government resources.
18.1.5 Employees shall sign Acceptable Usage of Internet and Email.
18.1.6 The above shall be in accordance with the Internet and Email policy.

19. BAS, PERSAL,WALKER, HSS, IMMIS

19.1.1 Only approved employees shall be provided with logical access to these systems.
19.1.2 System administrators shall ensure that passwords of these systems are changed at least monthly where applicable.
19.1.3 System administrators shall review system/database users at least every 6 months and review all logs created in the systems.
19.1.4 All systems policies and procedures shall be reviewed annually by system administrators in conjunction with ICT directorate.
19.1.5 Managers shall review the activity logs of the database administrators and the logs on violation every 6 months.
20. MALICIOUS SOFTWARE

20.1. Malicious Software (Virus, Trojans, Worms and Spyware) shall be reported by the employee once identified in the system. This should be done by:
   (a) Contacting the IT helpdesk to report the incident;
   (b) IT technician shall assist the user to remove the Malicious Software;
   (c) Network Administrator shall ensure that Antivirus installed in systems is setup to scan desktops and mobile devices daily.

20.2 Knowledge base shall be utilised in order to keep record of types of Malwares the department has faced.

20.3. Employees are prohibited from installing unauthorised software.

21. FIREWALL AND ANTIVIRUS

21.1 It is the responsibility of Provincial IT and the department’s ICT manager to ensure the implementation of an effective firewall and antivirus security strategy for the department.

21.2 It is the responsibility of the IT section of the department to ensure that the latest version of antivirus software is installed on all computers and mobile devices.

21.3 Remote users and users of portable computers should ensure that computers are plugged into Departments network at least twice a week for antivirus updates.

21.4 Staff members are responsible for scanning all media (e.g. memory sticks, CDs, external hard drives) before use. Assistance can be requested from an IT technician where necessary.

21.5 On detection of a virus, the staff member should notify the ICT section for assistance immediately.
21.6. Staff should not attempt to disable or interfere with the virus scanning software.

21.1. Incident Management

21.1.1 All the departmental ICT incidents shall be reported to the central ICT Directorate Helpdesk. (Tel: 0183881111) Alternatively, users can contact the ICT office to report faults. (Tel: 0183882955, 0183882230)

21.1.2 Remedy System shall be the tool to be used for logging ICT incidents.

21.1.3 ICT incidents shall be prioritized according to the impact they have on the NWPG network and critical systems.

21.2. HSS, Persal, BAS, User Account Management Procedures

21.2.1 User forms shall be completed for all new users and existing users whose performance areas have changed or modified.

21.2.2 Forms will be recommended by the Supervisor and approved by the Director responsible for HSS. For BAS and Persal, Forms will be recommended by the Supervisor and approved by the System Controller for BAS and Persal Controller for Persal.

21.2.3 User Access on the HSS database shall be checked, reviewed and verified every 6 months and every 3 months for BAS and Persal.

21.2.4. Users who have left the department or whose performance areas do not require access to the HSS, Persal and BAS will be removed from the system.

(See Annexure E and F: User Access Form)
22. INFORMATION SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

22.1. All Information system acquisition shall be procured in line with the SITA procurement procedure.
22.2. Failure to procure information systems without following the SITA procurement procedure shall constitute non-compliance with DPSA regulations.
22.3. Should the department utilise a service provider to develop an information system for the department, an SLA shall be signed by and between the service provider and the department.
22.4. Security requirements of the information system must be stated by the department.
22.5. The SLA shall state that the department owns the right of the information system developed by the service provider, this in line with Copyright Act.
22.6. Skills transfer of the development of the information system shall also be part of the SLA.
22.7. All acquired information system shall be tested before being deployed into the live network.
22.8. Information systems acquired or developed should protect the confidentiality and integrity of the departmental systems.

23. ICT DISASTER RECOVERY PLAN

23.1 Information Backups

23.1.1 By default, Provincial IT has allocated 2.5Gb of disk space for backup on filr server done automatically on a daily basis.
23.1.2 It is the responsibility of the IT section to install filr on all departmental computers.
23.1.3 Only work related information shall be backed up by the filr server.
23.1.4 Users of laptops should ensure that laptops are connected to the network on regular basis in order for filr to be backed up.
23.1.5 Where the need arises, the IT section shall provide officials with removable devices for the storage of work related information.

23.2 **Backup of department’s servers**

23.2.1 Backups of the systems database shall be done daily on the Server via an automated process available in the operating system.

23.2.2 Any access to backups, apart from the ICT team and System Administrators must be done in writing, signed and approved by the head of the Department.

23.2.3 Log files to be maintained on server confirming backup.

23.2.4 Bi-weekly backups of the database and log files shall be done on backup server (Offsite at Provincial IT Server Room)

**24. ICT DISASTER RECOVERY/ CONTINUITY PLAN**

24.1 ICT Continuity Plan/Disaster Recovery Plan shall be reviewed annually.
24.2 Identifies critical business information systems that should be prioritised.
24.5 Ensures that an ICT disaster recovery team is established.
24.6 Provides estimated time to recover all systems to be back online.

**25. SECURITY AWARENESS**

25.1 ICT directorate in conjunction with Security Services shall conduct Security awareness campaigns.
25.2 A security awareness plan shall be developed by both ICT directorate and Security Services.
25.3 The awareness program shall make employees of the department aware of internal security policies.

25.4 Security awareness shall be presented in a form of face to face engagement, posters, newsletters and utilising the intranet.

25.5 All directorates shall attend security awareness presentations once invited; failure to attend such awareness shall result in non-compliance of this policy.

26. COMPLIANCE

Any disciplinary action arising from non-compliance with this policy, annexure procedures and guidelines shall be dealt with in accordance with Public service disciplinary code and procedure.

27. REVIEW

This policy shall be reviewed annually depending upon the new developments that have been introduced within the Department.

28. RECOMMENDATION/APPROVAL

Supported by:

[Signature]

Mr. JK MASHIGO
CHAIRPERSON: DCC

Approved by:

[Signature]

Mr. MI KGANTSII
ACTING HEAD OF DEPARTMENT

27/03/15

DATE

23/03/15

DATE
ANNEXURE A

ICT SECURITY POLICY DECLARATION FORM

I, (name and surname) ___________________________ of (Persal no)______________ have read the Departmental ICT Security policy and I fully understand the terms and conditions and agree to abide by it.

Item : ____________________________________
Asset No. : ________________________________
Serial No. : ________________________________

The sharing, disclosure of passwords is an offence in terms of Section 3 and 4 of the Protection of Information Act. As the user / applicant, I understand and will refrain from engaging in any practices that could jeopardise the security of any Government system. I am accountable and fully responsible for ensuring that my user password is changed on a monthly basis, this includes immediately on receipt of my NEW USER ID, to change my default password.

I understand that any violation of this policy may lead to me being liable for the cost of damage or theft of any ICT equipment in my possession. I therefore undertake to take proper care of any Departmental ICT equipment, software, data or peripheral(s) allocated to me.

______________________________  ________________________________
Signature of User                 Date

______________________________
IT Unit staff member as Witness

Department Stamp
ANNEXURE B

ICT ASSET MOVEMENT FORM

Purpose of Movement:

<table>
<thead>
<tr>
<th>No</th>
<th>Asset Bar Code #</th>
<th>Room Bar Code #</th>
<th>Asset serial Number</th>
<th>Asset Description</th>
<th>Condition of Asset</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Current Location / User information

<table>
<thead>
<tr>
<th>Current Location / User Information</th>
<th>New Location / User Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office Number</td>
<td>Office Number</td>
</tr>
<tr>
<td>Name of building</td>
<td>Name of building</td>
</tr>
<tr>
<td>Head/Regional/District Office</td>
<td>Head/Regional/District Office</td>
</tr>
<tr>
<td>Asset User</td>
<td>Asset User</td>
</tr>
<tr>
<td>Asset Controller</td>
<td>Asset Controller</td>
</tr>
</tbody>
</table>

Movement of ICT Assets Sign Off

<table>
<thead>
<tr>
<th>Designation</th>
<th>Name</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Holder</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Receiver</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICT Personnel</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICT Manager</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Manager</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Annexure C

Logical Access Form

**Applicant's Personal Details:**

<table>
<thead>
<tr>
<th>First Name:</th>
<th>Surname:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID. No.:</td>
<td>Email:</td>
</tr>
<tr>
<td>Phone No.</td>
<td>Fax No.:</td>
</tr>
<tr>
<td>Company:</td>
<td>Section:</td>
</tr>
<tr>
<td>Location:</td>
<td>User ID/Profile</td>
</tr>
</tbody>
</table>

Put a tick where applicable

<table>
<thead>
<tr>
<th>New User ID</th>
<th>Reset User ID</th>
<th>Reset Password</th>
<th>Request for reports</th>
<th>Install Cables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify Application below:</td>
<td>Specify Application below:</td>
<td>Specify Reports</td>
<td>Specify Location below:</td>
<td></td>
</tr>
</tbody>
</table>

If not listed above, kindly describe your request in detail:
E.g. for what system/application, what reports, location of NW cables and points, duration of access, date and time.

Applicant:

Signature: ______________________ Date: ____________________

Duly authorised by Head of the Department

Initials: ___________________ Surname: ___________________

Signature: ______________________ Date: ____________________
ANNEXURE D

ASSET MOVEMENT AUTHORIZATION FORM

I, (Name and Surname) ___________________________ Persal no.: ___________ from Department of __________________________ have been authorized to carry the ICT Asset (description) __________________________ outside the department’s premises, Serial Number __________________________ and I agree to take full responsibility of this ICT Asset. I fully understand the terms and conditions as stipulated in the ICT Security Policy and agree to abide by it.

Applicant:

Signature: __________________________ Date: ______________

Duly authorised by: ICT Manager

Initials: ___________ Surname: __________________________

Signature: __________________________ Date: ______________
<table>
<thead>
<tr>
<th>HSS Functions</th>
<th>All Users</th>
<th>Project Registration</th>
<th>Project Editing</th>
<th>Project Approvals</th>
<th>Capturing</th>
<th>Verification</th>
<th>Supervisory</th>
<th>Approvals</th>
<th>Claims</th>
<th>HSS Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>View Beneficiary Application</td>
<td>Reserve Sites on Phases</td>
<td>Edit Project Information</td>
<td>Edit Site Information on Phases</td>
<td>Label files</td>
<td>Edit Beneficiary Applications</td>
<td>Edit Site Detail After Approval</td>
<td>Commit Beneficiary Approvals</td>
<td>Register New Claims</td>
<td>Edit System Setup Information</td>
</tr>
<tr>
<td></td>
<td>x Print Reports</td>
<td>Register New Projects</td>
<td>Delete Projects</td>
<td>Delete Sites on Phases</td>
<td>Register New Beneficiaries</td>
<td>Verify Beneficiary Application</td>
<td>Edit Applicant After Verification</td>
<td>Print PHB Final Lists</td>
<td>Edit Existing Claims</td>
<td>Add/Edit Companies</td>
</tr>
<tr>
<td></td>
<td>x Print Reports</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Print PHB Preview Lists</td>
<td>Edit Existing Claims</td>
<td>Add/Edit Reconciliations</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Withdraw Beneficiaries</td>
<td>View Payment Drill Down</td>
<td>Add/Edit Townships</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requested By:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>User:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recommended By:</td>
<td></td>
<td>Supervisory:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approved By:</td>
<td></td>
<td>Director:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implemented By:</td>
<td></td>
<td>Administrator:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* The user name for new users registered after January 2015 will be the same as the e-mail address.*
Annexure F

**EEWizard Access REQUEST FORM**

For other computer related services, forms are obtainable from the internet.

**Applicant Personal Details:**
- Name
- Phone No.
- Email
- Address

Please tick applicable boxes

For other computer related services, respective forms are obtainable from the internet.

**Supervisor/Manager Signature:**

<table>
<thead>
<tr>
<th>Department</th>
<th>Access Request Reqd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health</td>
<td></td>
</tr>
<tr>
<td>Education</td>
<td></td>
</tr>
<tr>
<td>Finance</td>
<td></td>
</tr>
<tr>
<td>House</td>
<td></td>
</tr>
<tr>
<td>Social Services Arts &amp; Sports</td>
<td></td>
</tr>
<tr>
<td>Planning &amp; Environment Services</td>
<td></td>
</tr>
</tbody>
</table>

**Applicant:**
- Signature
- Date

**Department Stamp**

**Supervisor/Manager Reqd**

<table>
<thead>
<tr>
<th>Name</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Duly Authorized Person**

<table>
<thead>
<tr>
<th>Name</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Pers. Manager**

<table>
<thead>
<tr>
<th>Name</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Conditions of Use:**

The above document authorizes an official name (department) to access the specified service.

If any changes occur, the above document must be updated accordingly.

Access may be revoked at any time at the discretion of the service provider.

Access to the service is subject to the user agreeing to the terms and conditions as stated in the document.

Any misuse of the service will result in revocation of access.

The user agrees to abide by all policies and procedures related to the service.

Any breach of these conditions may result in revocation of access.