



CONSOLIDATED ICT POLICIES

1.	DOCUMENT CONTROL.....	3
1.1	DOCUMENT LOCATION.....	3
1.2	REVISION HISTORY	3
1.3	DOCUMENT OWNER.....	3
1.4	DOCUMENT ACCEPTANCE	3
1.5	REVIEW CYCLE.....	3
1.6	CERTIFIED/ACCREDITED	3
1.7	DISTRIBUTION LIST.....	4
1.8	REFERENCE STANDARDS & GUIDELINES.....	4
2.	FOREWORD	4

ICT POLICIES 5

3.	ICT POLICIES	6
3.1	ACCEPTABLE USE AND BEHAVIOUR POLICY.....	6
3.2	ACCESS AND ENVIRONMENTAL CONTROL POLICY.....	9
3.3	PASSWORD POLICY	13
3.4	E-MAIL POLICY.....	18
3.5	MOBILE DEVICE SECURITY POLICY.....	20
3.6	WORKSTATION CONFIGURATION POLICY.....	26
3.7	MEDIA HANDLING POLICY	27
3.8	BACKUP POLICY	30
3.9	FIREWALL POLICY	38
3.10	CONFIGURATION MANAGEMENT POLICY	42
3.11	GENERAL CM TASKS AND PRINCIPLES	46
3.12	CONFIGURATION POLICY ELEMENTS	47
3.13	PERSONNEL SECURITY POLICY	48
3.14	MALICIOUS CODE POLICY	51
3.15	NETWORK MANAGEMENT POLICY	54
3.16	OUTSOURCING POLICY.....	57
3.17	CHANGE MANAGEMENT POLICY	62
3.18	SYSTEMS DEVELOPMENT POLICY	65
3.19	DISASTER RECOVERY POLICY	67
3.20	PATCH MANAGEMENT POLICY.....	69
3.21	PRIVACY POLICY	70

RECORDS MANAGEMENT POLICY 78

3.	RELATIONSHIP WITH OTHER POLICIES	84
4.	SCOPE AND INTENDED AUDIENCE	85
5.	REGULATORY FRAMEWORK.....	85

RECORDS MANAGEMENT POLICY 87

6.2	NATIONAL OR PROVINCIAL ARCHIVIST	88
6.3	RECORDS MANAGER	89
6.4	CHIEF INFORMATION OFFICER BEING THE HEAD OF DEPARTMENT	92
6.5	IT MANAGER	92
6.6	SECURITY MANAGER.....	92
6.7	LEGAL SERVICES MANAGER.....	92
6.8	CHIEF REGISTRY CLERK	92
6.9	EMPLOYEES	93
7.	RECORDS CLASSIFICATION SYSTEMS AND RELATED STORAGE AREAS	93
7.2	RECORDS OTHER THAN CORRESPONDENCE SYSTEMS.....	94
8.	DISPOSAL OF RECORDS (REGULATION PART V (10)(5)	95
9.	STORAGE AND CUSTODY.....	95
10.	ACCESS AND SECURITY	95
11.	LEGAL ADMISSIBILITY AND EVIDENTIAL WEIGHT.....	95
12.	TRAINING	96
13.	MONITOR AND REVIEW	96
	ANNEXURE 1 : LIST OF TERMINATED CORRESPONDENCE FILES / RECORDS	97
	ANNEXURE 2 : LIST OF TRANSFER OF RECORDS	98

1. Document control

1.1 DOCUMENT LOCATION

This document is located in the Eastern Cape Department of Human Settlements (ECDHS) site on www.ecdhs.gov.za.

1.2 REVISION HISTORY

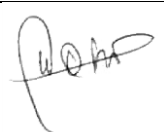
Version	Date	Description/Notes	Author(s)
1.0	2011	Creation of Policies	
1.1	24 February, 2015	Review & Update to Policies in alignment with current standards	KPMG
1.2	2 March 2020	Review & Update to Policies in alignment with current standards	ECDHS
1.3	October 2021	Review & Update to Policies in alignment with current standards and POPIA	ECDHS

1.3 DOCUMENT OWNER

Name	Role/On behalf of	Date	Signature
Vacant	Director: ICT		

1.4 DOCUMENT ACCEPTANCE

This document has been approved and accepted by:

Name	Role/On behalf of	Role Date	Signature
Mr. B. Skweyiya	Acting Director: ICT	10 January 2022	
Ms B. Gobe	Chief Director: Strategy and Systems	10 January 2022	
Mr. B. Lottering	Acting Chief Financial Officer	10 January 2022	
Ms T. Poswa	Head of Department	10 January 2022	

1.5 REVIEW CYCLE

This document should be reviewed annually or whenever the ECDHS Policies change, following the ECDHS change control procedure. The reviews will be initiated by the ECDHS ICT Manager.

1.6 CERTIFIED/ACCREDITED

Y/N	Date	Description/notes

1.7 DISTRIBUTION LIST

Name	Role	Date

1.8 REFERENCE STANDARDS & GUIDELINES

The Promotion of Access to Information Act, 2000 (Act no. 2 of 2000)			
The Protection of Information Act, 1982 (Act no. 84 of 1982)			
he State Information Technology Act, 1998 (Act no. 88 of 1998)			
ISO 27002			
CGICTPF			
Provincial ICT Governance Security Policy Framework			
Minimum Information Security Standards (MISS)			
Guidelines for the Handling of Classified Information (SP/2/8/1)			
Electronic Communications and Transaction Act, 2002 (Act no. 25 of 2002)			
The Promotion of Access to Information Act, 2000 (Act no. 2 of 2000)			
The Protection of Personal Information Act, 1982 (Act no. 84 of 1982)			

2. Foreword

The purpose of this document is to reduce the inherent risk of threats, whether internal or external, deliberate or accidental, to an acceptable level.

This document outlines ECDHS's standards for Information Security and is supported by customised policies, procedures and guidelines to facilitate compliance to the requirements.



ICT POLICIES

3. ICT policies

3.1 ACCEPTABLE USE AND BEHAVIOUR POLICY

3.1.1 Introduction

The intention to publish the Acceptable Use Policy is not to impose restrictions that are contrary to the ECDHS established culture, openness, trust and integrity. The department is committed to protecting employees, partners, and the government of South Africa as a whole from illegal or damaging actions by individuals, accidentally or intentionally.

Users shall be aware of the security limitations of the electronic communication channels, and shall not abuse their privileges. They shall promptly report all information security alerts, warnings, suspected vulnerabilities and suspected policy violations to the ICT. The ECDHS reserves the right to monitor all activity on ECDHS electronic communication channels. All policy violations shall be investigated by the ICT.

Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of any information user to know these guidelines and to conduct their activities accordingly.

3.1.2 Purpose

The purpose of this policy is to outline the acceptable use of any information and information system within the ECDHS.

The objectives of this policy are to:

- (a) mitigate against legal liability by setting boundaries for appropriate employee conduct when using electronic communications facilities;
- (b) safeguard our Electronic Communications facilities from abuse, damage or disruption;
- (c) ensure that employees understand that the electronic communications facilities provided to them are primarily for business use; and
- (d) comply with all relevant regulatory and legislative requirements such as the Regulation of Interception of Communications Act (2002) and the provisions of the Electronic Communications and Transactions Act (2001).

3.1.3 Scope

This is a standard departmental policy that applies to all users of the department's information and technology systems.

3.1.4 Roles and responsibilities

3.1.4.1 The GITO

The GITO shall implement, enforce and monitor the controls in accordance with the requirements outlined by management, and must advise users on the correct ways to access information and systems.

3.1.4.2 All employees

All employees are responsible for complying with this and other corporate policies at all times. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of acceptable behaviour) to comply with our information security policies.

3.1.4.3 Information security officer

Information Security Officer is responsible for maintaining this policy and advising generally on information security controls. Working in conjunction with other corporate functions, it is also

responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy.

3.1.4.4 Internal audit

Internal Audit is authorised by management to assess compliance with all corporate policies at any time.

3.1.5 Policy statements

- (a) The ECDHS shall utilize proxy or other internet gateway solutions. The proxy or gateway shall be capable of implementing as many of the following controls as possible:
 - i. monitoring and filtering content accessed via web browsing and any other internet services for appropriate use;
 - ii. detecting malicious content;
 - iii. detecting unauthorised disclosure of ECDHS information;
 - iv. allowing only authorised, authenticated users access to web resources;
 - v. logging access and Audit Usage;
 - vi. caching; and
 - vii. detecting and blocking unapproved applications and protocols tunnelling through open, permitted ports.
- (b) All internet browsing shall traverse the ECDHS-controlled content filtering and inspection solution, whether locally installed at the endpoint, or via the network internet gateway.
- (c) The ECDHS reserves the right to intercept and quarantine networking traffic and computing resources, such as internet mail and other internet services, which may pose a threat to the ECDHS.
- (d) All reports of alleged violations of this policy shall be investigated on a case-by-case basis by the ICT. During the course of the investigation, access privileges may be suspended. Violations of this policy may result in disciplinary action including, but not limited to the permanent loss of internet access privileges.
- (e) The ECDHS managers are responsible for ensuring that all employees, contractors, consultants, temporary staff and other users have read and will comply with the substance of this policy.
- (f) Users shall promptly report all information security alerts, warnings, suspected vulnerabilities and suspected policy violations to the ICT. Users are prohibited from utilizing ECDHS systems to forward such information to other users, whether the other users are internal or external to the ECDHS.
- (g) No media advertisement, internet home page, electronic bulletin board posting, electronic mail message, voice mail message, or any other public representation about the ECDHS may be issued unless it has first been approved by the Communications Directorate or relevant authority.
- (h) All non-text files (databases, software object code, spreadsheets, formatted word processing package files, etc.) downloaded from non-ECDHS sources via an electronic communication channel shall be screened with virus detection software prior to being used. Whenever an external provider of the software is not trusted, downloaded software should be tested on a stand-alone non-production machine that has been recently backed-up. Downloaded files shall be decrypted and decompressed before being screened for viruses.
- (i) If an electronic mail message contains information relevant to the completion of a business transaction, contains potentially important reference information, or has value as evidence of a management decision, it shall be retained for future reference. Users are responsible for archiving these messages on designate servers or other approved storage. Electronic mail systems are not intended for an archival storage solution.
- (j) Before employees release any internal ECDHS information, enter into any contracts, or order any products via public networks, the identity of the individuals and organisations contacted shall be confirmed. Identity confirmation is ideally performed via digital signatures or digital certificates.
- (k) All official ECDHS electronic mail messages, including those containing a formal management approval, authorization, delegation, or handing over of responsibility, or similar transaction, shall be filed in an acceptable manner within the appropriate department.
- (l) Misrepresenting, obscuring, suppressing, or replacing a user's identity on the internet or any ECDHS electronic communications system is forbidden. The user name, electronic mail address, organisational affiliation, and related information included with messages or postings shall reflect the actual originator of the messages or postings. Falsifying mail addresses, headers, or

- routing information so as to obscure the origins or route a message may have taken is in direct violation of the ECDHS's security policies.
- (m) Employees may not establish new internet web pages dealing with ECDHS business, or make modifications to existing web pages dealing with ECDHS business, unless they have first obtained the approval of the executive management. Modifications include the addition of hot-links to other sites, updating the information displayed, and altering the graphic layout of a page. Management shall ensure that all posted material is protected by adequate security measures approved by the ICT.
 - (n) In keeping with the confidentiality agreements signed by all employees, ECDHS software, documentation, and all other types of internal information shall not be disclosed to any non-ECDHS party for any purposes other than business purposes expressly authorised by management. Exchanges of software and/or data between the ECDHS and any third party may not proceed unless a written agreement has first been signed. Such an agreement shall specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected.
 - (o) Employees shall not post any information (software, internal memos, policies, etc.) on any publicly-accessible internet computer, unless the posting of these materials has first been approved by Executive Management. Likewise, the ECDHS's electronic mail system must not be used to send or receive copyrighted materials, trade secrets, proprietary financial information, client or employee information, or similar materials without prior authorisation.
 - (p) The ECDHS's electronic communication system shall not be used to create any offensive or disruptive messages. Disruptions include, but are not limited to: distribution of unsolicited advertising or information, chain letters, charitable solicitations or propagation of malicious software. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin, or disability. Users shall not use profanity, obscenities, or derogatory remarks in any form of electronic communication. To avoid libel, defamation of character, and other legal problems, whenever any affiliation with ECDHS is included with an internet message or posting, 'flaming' or similar written attacks are strictly prohibited. Likewise, employees shall not make threats against another user or organisation over the internet. All internet messages intended to harass, annoy, or alarm another person are similarly prohibited.
 - (q) The ECDHS's electronic mail system shall not be used to send or receive copyrighted materials, trade secrets, proprietary financial information, client or employee information, or similar materials without prior authorisation. Users are required to respect and comply with local and international legal protection provided by trade secrets, patents, copyrights, and trademarks to any information viewed or obtained via the internet. Copying of software in a manner that is not consistent with the vendor's license is strictly forbidden. Similarly, the reproduction, forwarding, or in any other way republishing or redistributing words, graphics, or other materials shall be done only with the permission of the author/owner. Employees should assume that all materials on the internet are copyrighted unless specific notice states otherwise. Under no condition may staff participate in pirate software bulletin boards and similar activities via ECDHS-owned infrastructure. All contracts shall be formed by paper documents prior to purchasing or selling via electronic systems. ECDHS, electronic mail, and similar binding business messages shall therefore be releases against blanket orders, such as a blanket purchase order.
 - (r) All electronic commerce systems shall be approved by the ICT and Legal representatives prior to usage. All contracts formed through electronic offer and acceptance messages (fax, EDI, electronic mail, etc.) shall be formalised and confirmed via paper documents, or other legally binding mechanism, within two weeks of acceptance. Employees shall not employ scanned versions of hand rendered signatures to give the impression that an electronic mail message or other electronic communications were signed by the sender. Taking into account all applicable local legislation, the ECDHS shall implement disclaimer text for all outbound e-mail communication.
 - (s) Sensitive information shall not be sent via unencrypted e-mail.
 - (t) Employees may not employ internet service provider (ISP) accounts and outside connections, for example dial-up lines, to access the internet with ECDHS computers. Instead, all internet activity shall pass through ECDHS firewalls so that access controls and related security mechanisms can be applied.
 - (u) The confidentiality of any e-mail message should not be assumed. Even when an e-mail message is erased, it may still be possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality. Where permitted by law, the ECDHS reserves and intends to exercise its right to review, audit, intercept, access and disclose all

messages created, received or sent over the electronic messaging system for any purpose. The content of electronic messages properly obtained for legitimate business purposes may be disclosed within the ECDHS and to law enforcement agencies without the permission of the employee. Notwithstanding the ECDHS's right to retrieve and read any electronic mail messages, such messages shall be treated as confidential by other employees and accessed only by the intended recipient. Other than authorised systems administrators, employees are not permitted to retrieve or read any email messages for which they are not the intended recipient. Any exception to this shall be received in writing prior to disclosure of the electronic mail's contents.

- (v) The decision to allow the personal use of Internet and e-mail is at the discretion of line management. Where allowed, any personal use of Internet, e-mail and other non- business activities must be performed on personal, not department time, and is subject to the stipulations in the information security policy document. Access to private e-mail boxes via ECDHS computing resources is forbidden.
- (w) Browsing or distribution of distasteful material such as erotica, discriminatory sites that advocate racial supremacy, material that is forbidden by the laws of the country and sites that are not in alignment with the ideals or image of the department are prohibited. Employees using ECDHS computers who discover that they have connected with a web site that contains sexually explicit, racist, violent, or other potentially offensive material shall immediately disconnect from that site. The ability to connect with a specific web site does not in itself imply that users of ECDHS systems are permitted to visit that site.
- (x) Employees shall not probe security mechanisms at either ECDHS or other internet sites unless they have first obtained permission from ICT. Likewise, the possession of tools for cracking information security systems is prohibited without the advance permission of ICT. Likewise, using ECDHS networking and computing resources to make or attempt unauthorized entry to any network or computer accessible via the internet, is strictly prohibited.
- (y) The ECDHS reserves the right to delete outdated electronic messages stored on exchange systems to reserve space and simplify records management.
- (z) Use of anonymous log-ins for electronic communication channels is not permitted.

3.1.6 Compliance

The GITO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.

Failure to comply with this policy may result in disciplinary action, which may include termination of employment.

Any conduct that interferes with the normal and proper operation of the departments IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved IT policies.

The ECDHS management reserves the right to revoke the privileges of any user at any time.

3.2 ACCESS AND ENVIRONMENTAL CONTROL POLICY

3.2.1 Introduction

An access and Environmental control policy authorises a group of users and tools to perform a set of actions on a set of resources. Unless authorised through one or more access control policies, users have no access to any functions of the system. To understand access control policies one should understand four main concepts: users, actions, resources, and relationships. Users are the people who use the system. Resources are objects in the system that needs to be protected. Actions are the activities that users can perform on the resources. Tools are systems or techniques or equipment used to protect the IT environment. Relationships are optional conditions that exist between users and resources.

The objective of access controls is to secure the access to business assets. The long-term purpose of these controls is to minimize the risks to the ECDHS's assets that might arise from unauthorised access, from local as well as from remote sources. Users can assist by keeping their access information like usernames and passwords secure, and by making sure that they access systems only for those purposes that they were authorised to. Management helps to achieve this objective by making sure

that access to information and business processes is controlled on the basis of security requirements that are in-line with business requirements. IT must implement, enforce and monitor the controls in accordance with the requirements outlined by management, and must advise users on the correct ways to access information and systems.

3.2.2 Purpose

The objective of access and Environmental controls is to ensure secure access to business assets as well as to ensure that ICT environment is protected. The long-term purpose of these controls is to minimize the risks to the ECDHS's assets that might arise from unauthorised access from local as well as from remote sources including environmental factors

3.2.3 Scope

The policy applies to all business units, employees, contractors, ICT environment and any other resources requiring access to the ECDHS computing environment.

Computing environment includes:

- physical and environmental; and
- hardware, software, system and applications

3.2.4 Roles and responsibilities

3.2.4.1 The HoD

The HoD working in conjunction with the CFO shall be responsible for ensuring the effective implementation and compliance of the ECDHS policies, standards and procedures.

3.2.4.2 Asset/information/application owner

- (a) The designated owner of the information asset shall take responsibility for all access granted.
- (b) The owner of the information resource shall ensure that all access to the resource granted is appropriate and justified.

3.2.4.3 Information security officer

The ISO is also responsible for maintaining this policy.

3.2.4.4 Internal audit

- (a) The Internal Audit department is authorised by management to assess compliance with all corporate policies at any time.
- (b) The Internal Audit department may assist with audits of outsourcing contracts including security compliance audits, and advise management on the risks and controls relating to access to ECDHS environment.

3.2.5 Policy statements

3.2.5.1 Privileged access rights

- (a) The number of people having elevated rights must be kept to a minimum.
- (b) A record must be kept of the people requiring elevated rights.
- (c) Access to operating system commands shall be restricted to IT staff members, who are authorised to perform systems administration functions.

3.2.5.2 Review and monitoring of access

- (a) Access to IT resources shall be logged and monitored on a continuous basis.
- (b) Logs of access to critical business systems, network and application shall be kept, these logs should be:

- i. reviewed regularly to help identify suspicious or unauthorised activity by the password administrator;
 - ii. retained for at least a three month period to be able to investigate past activities;
 - iii. protected against unauthorised change.
- (c) A formal record of all registered users in the department shall be maintained and updated yearly, clearly indicating appropriate access rights and/or privileges recorded in an access control register.

3.2.5.3 User registration

Granting of access to generic accounts (service accounts) must be strictly controlled. Formal and documented user registration and termination procedures for granting and terminating access to all multi-user information systems and services must exist. The user registration and termination procedures must include as many of the following components as possible:

- It must be clearly stated who has the responsibility for the correct registration of a user's access rights.
- Each user must be assigned a unique user ID. Generic (i.e. non-personal) accounts must be avoided wherever possible; all exceptions must be authorised by the ISO.
- A formal check that user has authorisation from the system owner for the use of the information system or service must be performed.
- A check that the level of access granted is appropriate to the business purpose and is consistent with the security policy and the security standards and does not violate segregation of duties.
- Users must receive a written statement of their access rights.
- Users must sign a document stating that they understand the conditions of access.
- Ensure that service providers do not provide access until authorisation procedures have been completed.
- Maintain a formal record of all persons registered to use the service.

3.2.5.4 Modification of users

In the event of an existing employee requiring changes to his/her access, the procedure to be followed is as set out below:

Notification of changes required

The manager of the employee requiring changes to his/her access should notify ICT by means of completing a modify user access form.

Implementation of changes

ICT will perform the requested changes once the changes have been approved by the ICT manager.

3.2.5.5 Termination of users

Promptly removing or re-evaluating access rights of users who have changed jobs or left the organisation.

Redundant user ID's are checked for and removed on a quarterly basis.

If an account is found to be inactive, an investigation will be performed within 7 working days as to the reason for the account being inactive. If the outcome of the investigation determines that the account is an offsite account, or if the account is a special account such as staff on maternity leave, the account will be flagged but will remain active. Otherwise the account will be disabled.

Ensuring that redundant user IDs are not issued to other users.

Accounts for consultants, contractors and temporary employees must be included in all new hire and termination processes that a department puts in place.

All ECDHS information systems privileges shall be promptly terminated at the time when an employee ceases to provide services to the department.

3.2.5.6 Access to applications

Access to the application and associated information should be restricted to authorised individuals in order to ensure that only authorised individuals are granted access to the application, and that individual accountability is assured.

Users of application, systems or data should be:

- i. authorised by the application owner;
- ii. identified by a unique user ID;
- iii. authenticated by a password;
- iv. provided with the minimum functionality required to perform their role; and
- v. revoked promptly when an individual user is no longer entitled to them such as when a user is transferred to another department, terminates his/her services, the department terminates his/her services or is suspended by the department.

Any user who has access to departmental classified information and/or data record(s) or database(s) in any format, shall be subject to appropriate security clearance and duly complete the oath of secrecy form (annex B) and the application for user creation form (annex C) to be kept safe by the business unit manager and another copy in his/her personnel file.

No employee or any user of the Department shall be given access to any other official(s), employee's files, information, data or records stored and/or processed on his/her desktop/laptop and/or server without his/her consent. Access shall be deemed to be authorised only when the appropriate user consent form (annex D) has been signed and approved by the head of IT services or the HoD.

No IT staff member or any employee may remotely take over a user's computer without his/her permission.

When issuing new or changed passwords it shall be ensured that:

- i. disclosure of passwords is minimised when they are communicated to the user (e.g. using encrypted e-mails or forcing the user to change passwords when they first use them);
- ii. it involves the target user directly (i.e. the person to whom the password uniquely applies);
- iii. the identity of the target user is verified (e.g. via a special code or through independent confirmation); and
- iv. passwords are changed regularly; and
- v. password must adhere to the ECDHS approved Password Policy.

3.2.5.7 User access management

The allocation of access rights to users should be strictly controlled through user registration and administration procedures, including special restrictions over the allocation of privileges and passwords, and regular access rights reviews.

3.2.5.8 User responsibilities

Users should be made aware of their responsibilities towards choosing strong passwords and keeping them confidential. Systems should be locked when left unattended (e.g. using password protected screensavers or key locks).

3.2.5.9 Network access control

Access to network services should be controlled, both within the organization and between organizations. Enforced paths and network segregation may be appropriate (e.g. using fixed/predefined network routes, firewalls and proxy servers). Remote users of the network and network nodes should be suitably authenticated. Remote diagnostic ports should be securely controlled. Security attributes of all network services should be clearly described.

3.2.5.10 Operating system access control

Operating system security facilities and utilities should be used appropriately (numerous controls are noted in this section).

3.2.5.11 Application access management

Application systems should incorporate security controls to restrict unauthorized access. Sensitive systems may require dedicated/isolated platforms and special handling. The access rights of users (e.g. read, write, delete, execute) should be controlled, along with the access rights of other applications.

3.2.5.12 Monitoring system access and use

Systems should be monitored for access policy violations and other security events such as use of privileges and alarms/exception conditions.

Logs and alarms should be reviewed at a frequency relating to the level of risk. System clocks should be synchronized.

3.2.5.13 Mobile computing and teleworking

There should be formal policies covering the secure use of portable PCs, PDAs, cellphones etc., and secure teleworking ("working from home" and other forms of mobile working).

3.2.5.14 ICT server-room environment

Departmental server room shall have the environmental control units in place to ensure that Departmental ICT infrastructure is protected:

- i. Brick-wall enclosure
- ii. Sufficient Air Conditioning System with optional fail-over support
- iii. Access Control security System shall be determined in consultation with Departmental Asset/Facilities Management for the appropriate access control method (biometrics system, metal key locks, magnetic card door locks etc.) and the appropriate access monitoring mechanism.
- iv. Fire detection, prevention, and control System
- v. Sufficient Un-Interrupted Power Supply (UPS) units
- vi. Raised access flooring (Raised Flooring) including Access ramp for environment with more than 100 staff count.
- vii. Network cabinet rooms: per each floor
- viii. Early warning systems in place for a quicker response to environmental risks.

3.2.6 Compliance

- (a) The ISO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.
- (b) Failure to comply with this policy may result in disciplinary action, which may include termination of employment.
- (c) Any conduct that interferes with the normal and proper operation of the department's IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved IT policies.
- (d) The ECDHS management reserves the right to revoke the privileges of any user at any time.

3.3 PASSWORD POLICY

3.3.1 Introduction

Policies are required to govern the passwords used when connecting to the ECDHS's network from any host and/or when accessing any operating system or application requesting a password. These policies are designed to minimize the potential exposure to the ECDHS from damages that may result from unauthorized use of resources. Damages include the loss of sensitive or department-confidential data, intellectual property, damage to public image and damage to critical the department's internal systems.

3.3.2 Purpose

The purpose of this policy is to ensure that only authorised users gain access to the ECDHS information, applications and computer installations.

The policy aims to restrict access to information or systems within government departments' computer environment to authorised users as well as to prevent unauthorised use or viewing of information and IT resources.

This policy focuses on password and user ID requirements, access to government computer systems and networks, and segregation of duties related to IT to ensure that IT users are aware of their responsibility towards usage of information systems in order to minimise possible information security risks. In addition, it covers remote, administrator and third party access.

3.3.3 Scope

The policy applies to all business units, employees, suppliers, vendor's contractors and any other resources requiring access to the ECDHS computing environment.

Computing environment includes:

- physical and environmental; and
- hardware, software, system and applications.

3.3.4 Roles and responsibilities

3.3.4.1 The GITO

The GITO must implement, enforce and monitor the controls in accordance with the requirements outlined by management, and must advise users on the correct ways to access information and systems.

3.3.4.2 The ECDHS executive management

Management helps achieving this objective by making sure that access to information and business processes is controlled on the basis of security requirements that are in-line with business requirements.

3.3.4.3 Information security officer

Information Security, in conjunction with functions such as Legal, Compliance and Risk Management, is responsible for assisting outsourced business process owners to analyse the associated risks and develop appropriate process, technical, physical and legal controls.

The ISO is also responsible for maintaining this policy.

3.3.4.4 Internal audit

The Internal Audit department is authorised by management to assess compliance with all corporate policies at any time.

3.3.4.5 Employees, contractors and service providers

Users must keep their access information like usernames and passwords secure, ensure that they access systems only for those purposes they were authorised to.

3.3.5 Policy statements

3.3.5.1 Issuing a new or changing a password

When issuing new or changed passwords it shall be ensured that:

- (a) the initial password is transferred to the individual in a secure way;

- (b) disclosure of passwords is minimised when they are communicated to the user (e.g. using encrypted e-mails or forcing the user to change passwords when they first use them);
- (c) the display and printing of passwords must be masked, suppressed, or otherwise obscured so that unauthorised parties are not able to observe or subsequently recover them. Where passwords are displayed to authorized third parties, for example to a security administrator, the following conditions must be met:
 - i. the users must be forced to change the password at first logon; and
 - ii. the functions and information that can be accessed through using the password have been classified as low sensitivity by the ECDHS.
- (d) it involves the target user directly (i.e. the person to whom the password uniquely applies);
- (e) the identity of the target user is verified (e.g. via a special code or through independent confirmation); and
- (f) when a password is initially assigned to a user the password must be a temporary one and the user must be forced to change it immediately;
- (g) a procedure of providing users who have forgotten their password with a new password must be in place; and
- (h) the procedure must include the following components:
 - i. a temporary password is to be supplied to the user after a positive identification;
 - ii. the temporary password must be given to the users in a secure way;
 - iii. the user must be forced to change the temporary password immediately; and iv. a procedure for users who believe that their password has been compromised must be in place.
- (i) passwords shall be changed every 30 days.
- (j) users that have system-level privileges granted through group membership shall have unique passwords held by the user of that account.

3.3.5.2 Minimum password length

The length of the password shall always be checked automatically at the time that users construct or select them. All passwords shall have at least eight alpha-numeric characters.

3.3.5.3 Difficult-to-guess passwords required

All user-chosen passwords for computers, web accounts, email accounts, servers and networks shall be difficult to guess. Words in a dictionary, derivatives of user-IDs, and common character sequences such as "123456", "qwerty", "aaabbbb", "zyxwvuts" shall not be employed. Likewise, personal details such as spouse's name, license plate, and birth date shall not be used unless accompanied by additional unrelated characters.

Backward spelling of any name or recognizable words shall not be used.

Avoid using days or months of the year

Passwords must contain uppercase, lower case, digits and any special characters.

3.3.5.4 Display and printing of passwords

The display and printing of passwords shall be masked, suppressed, or otherwise obscured so that unauthorised parties shall not be able to observe or subsequently recover them.

Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

3.3.5.5 Periodic forced password changes:

All users shall be automatically forced to change their passwords at least once every 30 days.

Users shall be informed of the password expiry 7 days before the expiry date.

3.3.5.6 Assignment of expired passwords:

The initial passwords issued by a security administrator shall be valid only for the involved user's first on-

line session. At that time, the user shall be forced to choose another password before any other work can be done.

3.3.5.7 Account lockout:

A user's account shall be locked after three unsuccessful logon attempts and only the system administrator can unlock user accounts. After 30 minutes after a lockout, the password attempts are reset and a further 3 attempts are allowed.

3.3.5.8 Disclosure

A password shall never be disclosed to any third party. A password shall not be written down.

The last six passwords should not be reusable, and a period of 15 days between password changes should be set to ensure that users do not change their passwords several times in a row to return to their known old password.

In order to prevent unauthorised access to other user's computers, information and/or data, requests to reset passwords shall be strictly and constantly monitored. System administrators shall not reset a password unless the user has logged the call with IT Helpdesk and has duly completed the password reset request form (annex B).

3.3.5.9 Password storage

Passwords may only be stored in encrypted form using a strong one-way encryption algorithm.

Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, or in other locations where unauthorized persons might discover or use them, except with the formal permission of the ISO.

3.3.5.10 Legacy system/applications

Some legacy systems constrain the length of passwords, or the characters that may be used, to the extent that the passwords cannot conform to the definition of secure passwords. These systems may continue to operate with the less secure passwords with the approval of the ISD, if one of the following conditions hold true:

- (a) the system is in the process of being decommissioned, or steps are being taken to correct the situation;
- (b) the functions and information exposed to the users have been classified as low sensitivity by the ISO;
- (c) steps have been taken to mitigate the risk, for example by isolating the system on the network and protecting access through an additional authentication layer; and
- (d) the risk has been formally documented, and accepted or transferred by the business/system/information owner.
- (e) should support authentication of individual users not groups.
- (f) passwords shall not be transported or communicated in clear text or in any easily reversible form.

3.3.5.11 Password management system

Any systems that generate and/or store passwords must do so securely. Where feasible, applications should rely on operating system controls for authentication and authorization. Systems must mask or obscure passwords while being entered. IDs and passwords must never be conveyed to users in the same communication.

Where enabled by operating systems and applications, the ECDHS must implement a password management system that has the following characteristics: It only accepts individual user IDs and passwords, as opposed to shared accounts. The users must be allowed to select and change their own passwords and the procedure must include a confirmation procedure to allow for input errors:

- the user must be instructed to change passwords whenever there is any indication of possible system or password compromise;
- enforce the selection of secure passwords; and

- have controls in place to protect against frequent password changes over a short period of time.

All sensitive information, including passwords, must be encrypted prior to transmission over a network.

All workstations used for ECDHS business activity, no matter where they are located, must use an access control system approved by the IT department. This system must lock access to the workstation after a period of inactivity.

Computer workstations and Laptops must be locked when workspace is unoccupied.

Computer workstations and laptops must be shut completely down at the end of the work day.

Every log-in process for multi-user computers must include a special ECDHS Information Security notice.

Following installation of hardware or software, all default vendor passwords must be altered (Guess Password)

If sent by regular mail or similar physical distribution systems, passwords must be sent separately from user-IDs. These mailings must have no markings indicating the nature of the enclosure. Passwords must also be concealed inside an opaque envelope that will readily reveal tampering.

All passwords must be promptly changed if they are suspected of being disclosed, or known to have been disclosed to unauthorised parties.

Whenever a system has been compromised, or suspected to have been compromised, a trusted version of the operating system and all security-related software must also be reloaded. In addition, all recent changes to user and system privileges must be reviewed for unauthorised modifications. All users must be instructed to change their passwords on the compromised machine, as well as on any other machines where they used the same passwords.

Security administrators must only disclose passwords if a new user-ID is being assigned, if the involved user has forgotten or misplaced a password, or if the involved user is otherwise locked out of his or her user-ID.

Security administrators must not reveal a password unless the involved user has first provided definitive evidence substantiating his or her identity.

- All users must keep their passwords confidential.
- A user must never keep a written copy of any ECDHS passwords.
- Users must not share passwords.

Access control to files, databases, computers, and other system resources via shared passwords is prohibited.

Procedures or security awareness training must be in place to ensure that users of electronic equipment, including desktops PCs, server consoles, mobile equipment and others, are instructed to:

- terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, for example a password protected screen saver;
- log-off mainframe computers and servers when the session is finished (i.e. not just switch off the PC or terminal);
- secure PCs, laptops or terminals from unauthorized use by using a key lock or an equivalent control, for example password access, when not in use. When a computer is distributed to a user, a password protected screensaver must be activated automatically after 15 minutes; and
- pay special attention to any type of small electronic devices that might easily be removed from the office and that could contain sensitive or classified data.

3.3.5.12 Remote access

- (a) Access to the ECDHS network via remote access shall be controlled using either one time password authentication or public/private key system with strong pass phrase.
- (b) Pass phrase shall not be the same as user's passwords.

3.3.6 Compliance

The GISO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.

Failure to comply with this policy may result in disciplinary action as described in the HR Policy employee conduct, which may include termination of employment.

Any conduct that interferes with the normal and proper operation of the ECDHS's IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved IT policies.

The ECDHS management reserves the right to revoke the privileges of any user at any time.

3.4 E-MAIL POLICY

3.4.1 Introduction

E-mail is perhaps the most important means of communication throughout the business world. Messages can be transferred quickly and conveniently across our internal network and globally via the public Internet. However, there are risks associated with conducting business via e-mail. E-mail is not inherently secure, particularly outside the department's own internal network. Messages can be intercepted, stored, read, modified and forwarded to anyone, and do sometimes go missing. Casual comments may be misinterpreted and lead to contractual or other legal issues.

3.4.2 Purpose

This policy defines and distinguishes acceptable/appropriate from unacceptable/inappropriate use of electronic mail (e-mail).

3.4.3 Scope

This is a standard corporate policy that applies throughout the organisation as part of the corporate governance framework. It applies to all users of the corporate e-mail systems.

3.4.4 Roles and responsibilities

3.4.4.1 The GITO

- (a) The GITO shall implement, enforce and monitor the controls in accordance with the requirements outlined by management, and must advise users on the correct ways to access information and systems.
- (b) Responsible for building, configuring, operating and maintaining the corporate e-mail facilities (including anti-spam, anti-malware and other e-mail security controls) in accordance with this policy.
- (c) Responsible for assisting users with secure use of e-mail facilities, and acts as a focal point for reporting e-mail security incidents.

3.4.4.2 All employees

All employees are responsible for complying with this and other corporate policies at all times. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of acceptable behaviour) to comply with our information security policies.

3.4.4.3 Information security officer

The information security officer is responsible for maintaining this policy and generally advising on information security controls. Working in conjunction with other corporate functions, it is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy.

3.4.4.4 Internal audit

The Internal Audit department is authorised by management to assess compliance with all corporate policies at any time.

3.4.5 Policy statements

Do not use e-mail:

- to send confidential/sensitive information, particularly over the Internet, unless it is first encrypted by an encryption system approved by Information Security;
- to create, send, forward or store e-mails with messages or attachments that might be illegal or considered offensive by an ordinary member of the public i.e. sexually explicit, racist, defamatory, abusive, obscene, derogatory, discriminatory, threatening, harassing or otherwise offensive;
- to commit the department to a third party for example through purchase or sales contracts, job offers or price quotations, unless you are explicitly authorised by management to do so (principally staff within Procurement and HR). Do not interfere with or remove the standard corporate e-mail disclaimer automatically appended to outbound e-mails;
- for private or charity work unconnected with the department's legitimate business;
- in ways that could be interpreted as representing or being official public statements on behalf of the department, unless you are a spokesperson explicitly authorised by management to make such statements;
- to send a message from anyone else's account or in their name (including the use of false 'From:' addresses); if authorised by the manager, a secretary may send e-mail on the manager's behalf but should sign the e-mail in his/her own name per pro ('for and on behalf of') the manager;
- to send any disruptive, offensive, unethical, illegal or otherwise inappropriate matter, including offensive comments about race, gender, colour, disability, age, sexual orientation, pornography, terrorism, religious beliefs and practice, political beliefs or national origin, hyperlinks or other references to indecent or patently offensive websites and similar materials, jokes, chain letters, virus warnings and hoaxes, charity requests, viruses or other malicious software; and
- for any other illegal, unethical or unauthorised purpose.

Department e-mail services are provided to serve operational and administrative purposes in connection with the business. All e-mails processed by the department's IT systems and networks are considered to be the organisation's property.

DoHS EC electronic communications systems generally shall be used only for business activities. Employees are reminded that the use of corporate resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

Misrepresenting, obscuring, suppressing or replacing the identity of a user on an electronic communications system is forbidden. The user name, electronic mail address, organisational affiliation and related information that are included with electronic messages or postings shall reflect the actual originator of the messages or postings.

Apply your professional discretion when using e-mail, for example abiding by the generally accepted rules of e-mail etiquette. Review e-mails carefully before sending, especially formal communications with external parties.

Do not unnecessarily disclose potentially sensitive information in "out of office" messages.

E-mails on the corporate IT systems are automatically scanned for malicious software, spam and unencrypted proprietary or personal information. Unfortunately, the scanning process is not 100% effective (e.g. compressed and encrypted attachments may not be fully scanned), therefore undesirable/unsavoury e-mails are sometimes delivered to users. Delete such e-mails or report them as security incidents to IT Help/Service Desk in the normal way.

Except when specifically authorised by management or where necessary for IT system administration purposes, employees must not intercept, divert, modify, delete, save or disclose e-mails.

Limited personal use of the corporate e-mail systems is permitted at the discretion of local management provided always that it is incidental and occasional, and does not interfere with business. You should have no expectations of privacy: all e-mails traversing the corporate systems and networks are subject to automated scanning and may be quarantined and/or reviewed by authorised employees.

Do not use Gmail, Hotmail, Yahoo or similar external/third-party e-mail services (commonly known as "Webmail") for business purposes. Do not forward or auto-forward corporate e-mail to external/third party e-mail systems. [You may access your own Webmail via corporate IT facilities at local management discretion provided that such personal use is strictly limited and is not considered private (*see previous statement*).]

Be reasonable about the number and size of e-mails you send and save. Periodically clear out your mailbox, deleting old emails that are no longer required and filing messages that need to be kept under appropriate e-mail folders. Send important e-mails for archival according to the *e-mail archival policy*.

Disciplinary actions will be taken against users found to be sending business critical information over external/third party e-mail services.

Special permission will need to be obtained for circumstances where external/third party e-mail services are required in order to send business critical information, e.g. where mailbox size limits need to be overcome to send a particularly large file.

3.4.6 Compliance

GISO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.

Failure to comply with this policy may result in disciplinary action, which may include termination of employment.

Any conduct that interferes with the normal and proper operation of the department's IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved IT policies.

The department management reserves the right to revoke the privileges of any user at any time.

3.5 MOBILE DEVICE SECURITY POLICY

3.5.1 Introduction

All departments' computer systems face information security risks. Laptop computers are an essential business tool but their very portability makes them particularly vulnerable to physical damage or theft. Furthermore, the fact that they are often used outside department's premises increases the threats from people who do not work for the department and may not have its interests at heart. Portable computers are especially vulnerable to physical damage or loss, and theft, either for resale (opportunistic thieves) or for the information they contain (industrial spies).

Bring Your Own (BYOD) therefore refers to the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged Departmental information and applications.

Permitting a range of devices to process personal data held by an organization gives rise to a number of questions a data controller must answer in order to continue to comply with its data protection obligations. It is important to remember that the data controller must remain in control of the personal data for which he is responsible, regardless of the ownership of the device used to carry out the processing.

Bring your own device raises a number of data protection concerns or risks due to the fact that the device is owned by the user rather than the data controller.

3.5.2 Purpose

The purpose of this policy is to ensure proper use and protection of mobile devices (laptop, Smartphone, and Tablets) and information stored within them. This policy describes the controls necessary to minimise information security risks affecting these personal device connected to the ECDHS ICT environment.

3.5.3 Scope

The policy applies to all users within the ECDHS who wishes to have access to or use ECDHS ICT environment using mobile devices as defined above.

3.5.4 Roles and responsibilities

3.5.4.1 The HoD

The HoD working in conjunction with the CFO shall be responsible for ensuring the effective implementation and compliance of the ECDHS policies, standards and procedures.

3.5.4.2 ICT systems administrator

The underlying feature of BYOD is that the user owns, maintains and supports the device. This means that the Systems Administrator will have significantly less control over the device than it would have over a traditional corporately owned and provided device. The security of the data is therefore a primary concern given that the Systems Administrator may have a large number and a wide range of devices to consider. The Systems Administrator will need to assess:

- what type of data is held;
- where data may be stored;
- how it is transferred;
- potential for data leakage;
- blurring of personal and business use;
- the device's security capacities;
- what to do if the person who owns the device leaves their employment; and
- how to deal with the loss, theft, failure and support of a device.

3.5.4.3 Internal audit

The Internal Audit department is authorised by management to assess compliance with all corporate policies at any time.

The Internal Audit department may assist with audits of outsourcing contracts including security compliance audits, and advise management on the risks and controls relating to outsourcing.

3.5.5 Policy statements

ECDHS grants its employees the privilege of purchasing and using smartphones, Laptops, Desktops and tablets of their choosing at work for their convenience. ECDHS reserves the right to revoke this privilege without notification if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of ECDHS' data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

The use of personal or private devices in connection with ECDHS business is a privilege granted to employees through approval of their management.

Please note that there may be limited exceptions to these policies owing to device limitations between vendors.

ECDHS employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the ECDHS network.

3.5.5.1 Physical security controls for laptops

The physical security of your laptop is your personal responsibility, therefore take all reasonable precautions. Be sensible and stay alert to the risks.

Keep your laptop in your possession and within sight whenever possible, just as if it were your wallet, handbag or mobile phone. Be extra careful in public places such as airports, railway stations and restaurants. It takes thieves just a fraction of a second to steal an unattended laptop.

If you have to leave the PC temporarily unattended in the office, meeting room or hotel room, even for a short while, use a laptop security cable or similar device to attach it firmly to a desk or similar heavy furniture.

Laptops must be either locked with a locking cable or locked away in a drawer.

Lock the laptop away out of sight when you are not using it, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office or in a hotel. Never leave a laptop visibly unattended in a vehicle. If absolutely necessary, lock it out of sight in the trunk or glove compartment but it is generally much safer to take it with you.

Carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage. Do not drop it or knock it about. Bubble-wrap packaging may be useful. An ordinary-looking briefcase is also less likely to attract thieves than an obvious laptop bag.

Keep a note of the make, model, serial number and the department asset label of your laptop but do not keep this information with the laptop. If it is lost or stolen, notify the Police immediately and inform the IT Help/Service Desk as soon as practicable (within hours not days).

3.5.5.2 Virus protection of devices

Viruses are a major threat to the department and mobile devices are particularly vulnerable if their anti-virus software is not kept up-to-date. The anti-virus software must be updated at least monthly. The easiest way of doing this is simply to log on to the department's network for the automatic update process to run. If you cannot log on for some reason, contact the IT Help/Service Desk for advice on obtaining and installing anti-virus updates.

E-mail attachments are the number one source of computer viruses. Avoid opening any e-mail attachment unless you were expecting to receive it from that person.

Always virus-scan any files downloaded to your computer from any source (CD/DVD, USB hard disks and memory sticks, network files, e-mail attachments or files from the Internet). Virus scans normally happen automatically but the IT Help/Service Desk can tell you how to initiate manual scans if you wish to be certain.

Report any security incidents (such as virus infections) promptly to the IT Help/Service Desk in order to minimise the damage.

Respond immediately to any virus warning message on your computer, or if you suspect a virus (e.g. by unusual file activity) by contacting the IT Help/Service Desk. Do not forward any files or upload data onto the network if you suspect your device might be infected.

Be especially careful to virus-scan your system before you send any files outside the Department. This includes e-mail attachments and CD-ROMs that you create.

3.5.5.3 Controls against unauthorised access to mobile device data

You must use approved encryption software on all mobile devices. A long, strong encryption password/phrase must be chosen and kept secure. Contact the IT Help/Service Desk for further information on device encryption. If your device is lost or stolen, encryption provides extremely strong protection against unauthorised access to the data.

You are personally accountable for all network and systems access under your user ID, so keep your password absolutely secret. Never share it with anyone, not even members of your family, friends or IT

staff.

Corporate laptops are provided to employees for official use. Do not loan your laptop or allow it to be used by others such as family and friends.

Avoid leaving your laptop unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before walking away from the machine.

3.5.5.4 Unlicensed software

Be careful about software licenses. Most software, unless it is specifically identified as “freeware” or “public domain software”, may only be installed and/or used if the appropriate license fee has been paid. Shareware or trial packages must be deleted or licensed by the end of the permitted free trial period. Some software is limited to free use by private individuals whereas commercial use requires a license payment. Individuals and companies are being prosecuted for infringing software copyright: do not risk bringing yourself and the department into disrepute by breaking the law.

3.5.5.5 Backups

You must take your own backups of data on your laptop. The simplest way to do this is to logon and upload a data from the laptop to the network on a regular basis – ideally daily, but weekly at least. If you are unable to access the network, it is your responsibility to take regular off-line backups to CD/DVD, USB memory sticks etc. Make sure that off-line backups are encrypted and physically secured. Remember, if the laptop is stolen, lost or damaged, or if it simply malfunctions, it may be impossible to retrieve any of the data from the laptop.

3.5.5.6 Acceptable Use

ECDHS defines acceptable business use as activities that directly or indirectly support the business of the Department.

Employees are blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the Department.

Devices' camera and/or video capabilities are not disabled while on-site.

Devices may not be used at any time to:

- Store or transmit illicit materials
- Store or transmit proprietary information belonging to another organization
- Harass others
- Engage in outside business activities

Employees may use their mobile device to access the following ECDHS-owned resources: email, calendars, contacts, documents, internet and specific systems as per the formal request.

ECDHS has a zero-tolerance for texting or emailing while driving and only hands-free talking while driving is permitted.

3.5.5.7 Devices and support

Smartphones including iPhone, Android and Windows phones are allowed

Tablets including iPad and Android are allowed

Connectivity issues are supported by ECDHS IT however employees should contact the device manufacturer or their carrier for operating system or hardware-related issues.

Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

3.5.5.8 Security

Users of personal devices are not permitted to connect to ECDHS infrastructure without documented consent from ECDHS IT.

In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the Departmental network.

Refer to Password Policy for rules regarding password strength.

The device must lock itself with a password or PIN if it's idle for five minutes.

After three failed login attempts, the device will lock. Contact IT to regain access. Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.

Employees are automatically prevented from downloading, installing and using any app that does not appear on the company's list of approved apps when connected to the Departmental networks.

Smartphones and tablets that are not on the company's list of supported devices are not allowed to connect to the network.

Smartphones and tablets belonging to employees that are for personal use are allowed to connect to the network.

Employees' access to Departmental data is limited based on user profiles and/or systems policies defined by IT and are automatically enforced.

The employee's device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

3.5.5.9 Risks/liabilities/disclaimers

While IT will take every precaution to prevent the employee's personal data stored in a Departmental file server from being lost, it is the employee's responsibility to take additional precautions, such as backing up email, contacts.

Lost or stolen devices must be reported to ECDHS IT as soon as possible

The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.

The employee is personally liable for all costs associated with his or her device.

The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

ECDHS reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

3.5.5.10 Physical security controls for laptops

The physical security of 'your' laptop is your personal responsibility, therefore take all reasonable precautions. Be sensible and stay alert to the risks.

Keep your laptop in your possession and within sight whenever possible, just as if it were your wallet, handbag or mobile phone. Be extra careful in public places such as airports, railway stations and restaurants. It takes thieves just a fraction of a second to steal an unattended laptop.

If you have to leave the PC temporarily unattended in the office, meeting room or hotel room, even for a short while, use a laptop security cable or similar device to attach it firmly to a desk or similar

heavy furniture. These locks are not very secure but they do deter casual thieves.

Lock the laptop away out of sight when you are not using it, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office or in a hotel. Never leave a laptop visibly unattended in a vehicle. If absolutely necessary, lock it out of sight in the trunk or glove compartment but it is generally much safer to take it with you.

Carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage. Do not drop it or knock it about. Bubble-wrap packaging may be useful. An ordinary-looking briefcase is also less likely to attract thieves than an obvious laptop bag.

Keep a note of the make, model, serial number and the department asset label of your laptop but do not keep this information with the laptop. If it is lost or stolen, notify the Police immediately and inform the IT Help/Service Desk as soon as practicable (within hours not days).

3.5.5.11 Controls against unauthorised access to laptop data

You must use approved encryption software on all corporate laptops, choose a long, strong encryption password/phrase and keep it secure. Contact the IT Help/Service Desk for further information on laptop encryption. If your laptop is lost or stolen, encryption provides extremely strong protection against unauthorised access to the data.

You are personally accountable for all network and systems access under your user ID, so keep your password absolutely secret. Never share it with anyone, not even members of your family, friends or IT staff.

Corporate laptops are provided to employees for official use. Do not loan your laptop or allow it to be used by others such as family and friends.

Avoid leaving your laptop unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before walking away from the machine.

3.5.5.12 Unauthorised software

Do not download, install or use unauthorised software programs. Unauthorised software could introduce serious security vulnerabilities into the department networks as well as affecting the functioning of your laptop. Software packages that permit the computer to be 'remote controlled' (e.g. PCanywhere) and 'hacking tools' (e.g. network sniffers and password crackers) are explicitly forbidden on the department's equipment unless they have been explicitly preauthorised by management for legitimate business purposes.

3.5.5.13 Unlicensed software

Be careful about software licences. Most software, unless it is specifically identified as "freeware" or "public domain software", may only be installed and/or used if the appropriate licence fee has been paid. Shareware or trial packages must be deleted or licensed by the end of the permitted free trial period. Some software is limited to free use by private individuals whereas commercial use requires a licence payment. Individuals and companies are being prosecuted for infringing software copyright: do not risk bringing yourself and the department into disrepute by breaking the law.

3.5.5.14 Backups

You must take your own backups of data on your laptop. The simplest way to do this is to logon and upload a data from the laptop to the network on a regular basis – ideally daily, but weekly at least. If you are unable to access the network, it is your responsibility to take regular off-line backups to CD/DVD, USB memory sticks etc. Make sure that off-line backups are encrypted and physically secured. Remember, if the laptop is stolen, lost or damaged, or if it simply malfunctions, it may be impossible to retrieve any of the data from the laptop. Off-line backups will save you a lot of headache and extra work.

3.5.5.15 Laws, regulations and policies

You must comply with relevant laws, regulations and policies applying to the use of computers and information. Software licensing has already been mentioned and privacy laws are another example. Various corporate security policies apply to laptops, the data they contain, and network access (including use of the Internet). Visit Information Security's intranet website for further information.

3.5.6 Compliance

- (a) ISO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.
- (b) Failure to comply with this policy may result in disciplinary action, which may include termination of employment.

3.6 WORKSTATION CONFIGURATION POLICY

3.6.1 Introduction

Personal computers, just as any other end-user devices, can be attacked and compromised. In addition to the possible loss of confidentiality, integrity and availability of the information on the device itself, such compromised devices can be used to launch an attack against the rest of the network. Some controls used to protect these devices against a breach include:

- protection against malicious software;
- patch management;
- disk encryption;
- strict control over access rights; and
- personal device firewalls.

3.6.2 Purpose

This policy defines and distinguished acceptable/appropriate from unacceptable/inappropriate process of configuring the department's personal computer.

3.6.3 Scope

This is a standard corporate policy that applies throughout the organisation as part of the corporate governance framework.

3.6.4 Roles and responsibilities

3.6.4.1 The GITO

The GITO must implement, enforce and monitor the controls in accordance with the requirements outlined by management, and must advise users on the correct ways to access information and systems.

3.6.4.2 All employees

All employees are responsible for complying with this and other corporate policies at all times. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of acceptable behaviour) to comply with our information security policies.

3.6.4.3 Information security officer

The Information Security Officer is responsible for maintaining this policy and advising generally on information security controls. Working in conjunction with other corporate functions, it is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy.

3.6.4.4 Internal audit

The Internal Audit department is authorised by management to assess compliance with all corporate policies at any time.

3.6.5 Policy statements

All desktop, laptop and server systems shall be configured with working anti-virus software. This software shall be configured such that:

- the virus protection software is active at all times;
- only the ICT shall have the permission to configure the software. Users with standard privileges shall not be able to change the settings, disable, de-activate, uninstall or otherwise subvert the normal operation of the software;
- all platforms shall be enrolled in a automatic update process to ensure that the latest virus definition file, tested and published by ICT, is installed as long as they are connected to
- the ECDHS network;
- all platforms have the functionality to be manually updated or to request the latest definition file be downloaded and installed;
- desktop and laptop systems are configured to scan all file types; permission to relax this requirement due to excessive utilization or latency may only be obtained from the ICT; and
- all platforms have predefined scanning schedules enabled to completely scan the device at least once every two weeks.

Clean desk policy as well as clear screen policy as per ISO

All servers, desktops, laptops and tablet devices shall be configured to automatically download and patch themselves with critical operating system and security patches in a controlled manner after pilot testing of the patch has been made. Additionally, automated external patching can be implemented as long as all desktop and laptop platforms are capable of being patched within a 24 hour period.

Laptop devices must be configured with approved disk encryption software which automatically encrypts all information on the device's hard drives, configured in such a way that all data that the user saves on the hard drives is encrypted with no special intervention on the part of the user.

All devices, when being re-deployed, shall be re-imaged such that all previous information is erased and only the latest patched version of the operating system and applications are deployed to the new user.

Devices delivered to general users shall be configured such that the user does not have administrative rights to the device and is not capable of making changes to the device that might affect the level of security on the device or network. Exceptions to this should be approved by the ICT.

Laptop and desktop devices must be configured with personal firewall software, and a host- based intrusion protection system.

3.6.6 Compliance

- (a) The GITO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.
- (b) Failure to comply with this policy may result in disciplinary action, which may include termination of employment.
- (c) Any conduct that interferes with the normal and proper operation of the departments IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved IT policies.

The ECDHS management reserves the right to revoke the privileges of any user at any time.

3.7 MEDIA HANDLING POLICY

3.7.1 Introduction

Media in the context of this document is a broad definition, including types such as hard copy, soft

copy (electronic), voice, and multimedia. All media shall be protected against unauthorised disclosure or misuse, in accordance with its security classification. This protection shall control the handling, distribution and storage of media.

3.7.2 Purpose

This policy defines and distinguishes control required to ensure media is handled in an appropriate, acceptable and approved way within the ECDHS.

3.7.3 Scope

This is a standard departmental policy that applies to all users of the department's information and technology systems including those that handle any departmental information in any form or type.

3.7.4 Roles and responsibilities

3.7.4.1 The GITO

The GITO must implement, enforce and monitor the controls in accordance with the requirements outlined by management, and must advise users on the correct ways to access information and systems.

3.7.4.2 All employees

All employees are responsible for complying with this and other corporate policies at all times. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of acceptable behaviour) to comply with our information security policies.

3.7.4.3 Information security officer

Information Security Officer is responsible for maintaining this policy and advising generally on information security controls. Working in conjunction with other corporate functions, this role is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy.

3.7.4.4 Internal audit

Internal Audit is authorised by management to assess compliance with all corporate policies at any time.

3.7.5 Policy statements

Procedures for the handling and storage of information shall be established to protect against unauthorised disclosure or misuse. These procedures shall be cognisant of the classification of the information. The following items shall be addressed by these procedures:

- handling and labelling all media;
- the storage of media, taking into account the manufacturers' specifications;
- review of distribution lists and lists of authorised recipients at regular intervals
- restriction of access;
- labelling of information to indicate the intended recipients;
- distribution;
- maintenance of a formal record of recipients;
- the integrity of input data and processing;
- the validation of output;
- the protection of spooled data; and
- management of removable media
- Examples of information items for which these procedures shall be drawn up include, but is not limited to:
 - i. documents,
 - ii. information in computing systems,
 - iii. information traversing networks,

- iv. information specific to mobile computing and mobile communications, v. information sent via mail,
- vi. voice mail, and voice communications in general,
- vii. multimedia,
- viii. faxes,
- ix. blank checks, and
- x. invoices.

The ECDHS shall have implemented procedures for inspecting hard-copy input documents to ensure that no unauthorised changes had been made.

The ECDHS shall have reliable procedures to ensure that systems documentation, for example Network Diagrams, are kept up to date and stored securely. The updating of systems documentation is a required step in all change processes.

Systems documentation shall only be released on a need-to-know basis.

All media shall be stored in a safe, secure environment, in accordance with manufacturers' specifications.

The previous contents of reusable media shall be erased or destroyed, if no longer required, using a method compliant with best practice. Media shall be disposed of securely and safely when no longer required.

Procedures should be in place to identify the items that might require secure disposal. Removable media drives should only be enabled if there is a business reason for doing so. Formal procedures for the secure destruction or disposal of media shall be established to minimize the risk of sensitive information leaking to outside persons.

Reliable transport or couriers should be used for the transport of physical media

Procedures to verify the identification of couriers should be developed.

Packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications.

Logs should be kept, identifying the content of the media, the protection applied as well as recording the times of transfer to the transit custodians and receipt at the destination.

Encryption process – 2 layer of encryption

3.7.6 Compliance

The GITO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.

Failure to comply with this policy may result in disciplinary action, which may include termination of employment.

Any conduct that interferes with the normal and proper operation of the departments IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved IT policies.

The department management reserves the right to revoke the privileges of any user at any time.

3.8 BACKUP POLICY

3.8.1 Introduction

This document is intended to define and provide a framework for managing data storage and focusing on efficient and dependable archival, preservation and retrieval of information leveraged by applications and employees of the Department of Human Settlements (Eastern Cape) within the guiding principles of the generally recognised practices and to promote good information management practice.

The most fundamental aspect of storage management is therefore the access, backup and recovery process. Managing huge quantities of diverse data, widely distributed across the enterprise is a daunting task. Technology, when integrated into a comprehensive data and business recovery strategy, can reduce the risk of data loss and reduce the cost of data recovery and downtime.

3.8.2 Purpose

This policy applies to all equipment and data owned and operated by the Department.

3.8.3 Scope

The Backup Policy and Procedures apply to all business units, employees, contractors and any other resources requiring access to the ECDHS ICT environment. These functions include:

- (a) physical and environmental; and
- (b) hardware, software, system and applications.

3.8.4 Roles and Responsibilities

3.8.4.1 The GITO

- (a) The GITO shall implement, enforce and monitor the controls in accordance with the requirements outlined by management, and must advise users on the correct ways to backup and restore information and systems.
- (b) Responsible for ensuring that the backups are running and documented all the time.
- (c) Responsible for assisting users with secure use of data files facilities, and acts as a focal point for reporting disaster incidents.

3.8.4.2 All employees

All employees are responsible for complying with this and other corporate policies at all times and ensuring that the data is stored on their respective user Home_folder. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of acceptable behaviour) to comply with our information security policies.

3.8.4.3 Backup administrator

The Backup administrator is responsible for maintaining this policy and generally advising on Data / information security controls. Working in conjunction with other corporate functions, it is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy. The backup administrator is also responsible for running day-to-day data backups and restores; testing of backups and modifies backup scripts.

3.8.5 Policy objectives and statement

- (a) Provide proper controls and management systems that will ensure effective, efficient and economical use of the ECDHS's information.
- (b) Establish controls that must ensure proper management of risks associated with ownership and safeguarding of information
 - i. implement and enforce storage of department approved information on enterprise computers and servers (H:\Home_Folder\UserName). This ensures that data such as

- ii. music files, and picture files, do not take space on enterprise storage facilities;
- ii. enforce centralised storage of documents on LAN servers [preferably with offline folder synchronisation for mobile laptops] to facilitate centralised data backup; and
- iii. implement a well-documented tape rotation system to safeguard against accidental overwriting of tapes.

Perform advanced scheduling, automated unattended operation, centralised reporting, and enterprise-wide media management.

Improve availability through high-performance backup and restore features that reduce the backup window.

Ensure that backup procedures adhere to international standards and procedures. Ensure that in the event of a disaster, backup files can be recovered:

- implement scheduled unattended but auditable backup systems that allow operation when network traffic on the enterprise network is at a minimum; and
- implement a backup solution that minimises the recovery time for information by allowing selective restoration.

Ensure data integrity at all times by regularly testing the backed up information.

Ensure offsite storage is maintained at all times to enable recovery of information should a disaster occur (onsite) due to fire, floods or other causes.

Ensure that backup tapes/cassettes are labelled according to the prescribed procedures:

- implement a regularly scheduled data restoration exercise to ensure backup media is recoverable within the appropriate recovery timeframe ; and
- keep backups on storage tape offsite to avoid being destroyed should a disaster occur onsite.

Ensure all changes to strategy, policy and procedures are properly authorised and documented:

- maintain a change control register to record all changes to the policy and procedures; and ensure the correct authorisation is obtained prior to effecting any changes.

3.8.6 Procedures for backup

3.8.6.1 Backup schedule and tape rotation

The ECDHS's Head Office backup solution uses a four-daily, four-weekly and one-monthly GFS data retention cycle. A Grandfather-Father-Son rotation scheme must be operated; incremental daily backups (*Son*) must run overnight from Monday to Thursday and must be rotated on a three or four week basis. A full weekly backup (the *Fathers*) must run on Fridays of each week and one full backup per month (the *Grandfather*) must run and be kept for 12 months.

The following data retention cycle must be used when performing backups:

- (a) Daily GFS data retention cycle:
 - i. F-DOHCENT-MON-DATE
 - ii. F-DOHCENT-TUE-DATE
 - iii. F-DOHCENT-WED-DATE
 - iv. F-DOHCENT-THU-DATE
- (b) Weekly GFS data retention cycle:
 - i. Week1 – F-DOHCENT-FRI-DATE
 - ii. Week2 – F-DOHCENT-FRI-DATE
 - iii. Week3 – F-DOHCENT-FRI-DATE
 - iv. Week4 – F-DOHCENT-FRI-DATE
 - v. Week4 – F-DOHCENT-FRI-DATE
 - vi. Week5 – F-DOHCENT-FRI-DATE
- (c) 12-monthly GFS data retention cycle:
 - i. January09 - F-DOHCENT-JAN-DATE
 - ii. February09 - F-DOHCENT-FEB-DATE
 - iii. March 09 till - F-DOHCENT-MAR-DATE
 - iv. December09 - F-DOHCENT-DEC-DATE

During week one, the Week1 set is used and during week two, Week2 set is used and so on. The following schedule is used for daily and weekly tape rotation:

Monday (or first business day of the week):

Deliver the previous Monthly's tape to the offsite storage facility and collect the oldest set of weekly tapes, e.g. (if you were using Week1 last week you need to send the tapes to the offsite storage and bring the current month tapes to the offices).

Make sure that you run a device inventory once the tape has been inserted into the tape library.

Place the old weekly set in the fire-proof safe and insert new weekly's tape in the tape library. Your tape is now ready for the backup in the evening of that day.

Also note that all monthly tapes and two spare tapes must be kept in the tape library and these can be changed over a longer period of time. Monthly tapes must be changed every Monday of the week and monthly tapes must be changed every first Monday of the month at 10:00 am.

It is therefore preferable to do this in the morning so that it becomes a routine. Backups only run at 19:00 so that all data for the day is captured on the tapes.

The following schedule is used for monthly tape rotation: The tapes in this must be labelled:

- January
- February
- March
- April
- May
- June
- July
- August
- September
- October
- November
- December

On the last business day of the month, the daily or weekly backup tape must not be used. Instead use the monthly tape corresponding with the month that you are in. This tape must be taken to the offsite storage as soon as possible. Note: These tapes should never be kept onsite; they can only be used for emergency recovery.

3.8.6.2 Checking backup job and completion of backup log

As part of the monthly backup job the tape will be ejected from the Tape drive into the Tape library after the backup has completed. If the tape has not ejected by 08:00 in the morning there could be an issue with the backups; notify the backup administrators.

Backup job status will be e-mailed to the backup administrators immediately after the job completion. Currently, a group, BackupAdmins which include the Manager of Networks and Infrastructure, the Systems Administrator and the Support Technician, is set up to receive the job status report. This e-mail is to be used to complete the backup log as it will have information on whether the backup job completed successfully or failed. A detailed log file will also be attached to the e-mail.

The technicians are not allowed to modify any jobs; it is the responsibility of the backup administrators to modify backup scripts. The log file can be forwarded to the backup administrator who will be able to identify the cause of the failed/incomplete backup.

Backup administrators must make sure that each backup tape is labelled stating the specific backup name and serial number. Both the tape and case must be labelled and it is the responsibility of the backup administrator to replace broken or faulty tapes. He/she must also make sure that all backup logs are analysed and resolved if there are any backup issues that are reported.

There are four types of backups logs that the ECDHS will be utilising:

Backup log: This log must be created and maintained by the backup software and stored on the backup tape and on the hard drive. The Backup Log is used to monitor the swapping of tapes and the status of the backups. This needs to be completed every morning when the tapes are swapped. The log file must also be printed and kept in a file in the fire-proof safe. A page will exist for every month and the backups are logged against the sheet.

Error log: This log must be created and maintained by the backup software and stored on the backup tape and on the hard drive.

Backup Restore Log: This log will be created and maintained by the backup software and stored on the backup tape and on the hard drive.

Backup Storage Log: A logbook will be kept at the on-site and off-site storage location. The following backup schedule must be adhered to.

Monday	Tuesday	Wednesday	Thursday	Friday
Daily backups	Daily backups	Daily backups	Daily backups	Full weekly backup
Daily backups	Daily backups	Daily backups	Daily backups	Full weekly backup
Daily backups	Daily backups	Daily backups	Daily backups	Full weekly backup
Daily backups	Daily backups	Daily backups	Daily backups	Full weekly backup

The following is an example of the backup log.

ECDHS Backup Log - Month/Year: December / 2021

DATE	TAPE NAME	Tape Serial#	JOB STATUS	ON FAILED/INCOMPLETE STATUS; WHAT ACTION WAS TAKEN	BACKUP ADMIN USER	SIGNATURE
3 Aug 09	Monday	BCS001	Finished		Buntu	
4 Aug 09	Tuesday	BCS002	Failed	Failed to backup SQL server on DOTR-KING- EX1. Informed server administrator	Buntu	
5 Aug 09	Wednesday	BCS003	Finished		Buntu	
6 Aug 09	Thursday	BCS004	Finished		Zitho	
7 Aug 09	Friday	BCS005	Finished		Zitho	

This log must be completed and signed by the relevant Backup Admin as a log to the completion of the backups. The updates to this log are just as critical as the tapes being swapped and are used when recovery of data is required.

3.8.7 Backup admin responsibilities and delegation

The backup administrators' responsibilities are to:

- swap the tapes;
- transfer tapes to offsite storage as per the tape rotation policy;
- check backup job status;
- complete the Backup Log daily;
- ensure that backup and storage logs are maintained;
- escalate backup issues;
- ensure that all tapes are write-enabled before inserting into the tape drive;
- ensure that all tapes are marked properly, i.e. with the name of the type of backup, as well as the date when the tape is used for backup and the save set name is written into the backup logbook next to the appropriate tape;
- on completion of a backup, the operator must enter the backup date and tape numbers onto

- the Backup Logbook as well as the backup on the label supplied in tape's case; and
- store backup tapes in a safe before they are collected to be stored off site.

Failure to execute the above responsibilities must be viewed as negligence and can result in severe data loss.

3.8.8 Administration and operations back-up and recovery strategy

Administration and operations activities are segregated into essential and non-essential within the context of a short-term emergency. For emergencies of longer durations, it is likely that more of these activities will be regarded as essential, and this requirement should also be reflected in the chart below.

Table 11: Essential activities

Name of process	Time-band*	Potential disruption	Potential impact
Systems update	1 day	Non-updating of systems: OS Patches, AV update, application updates	IT security breach: Confidentiality and Integrity
Back-up and recovery strategy: Network controller allocated laptop with mobile connectivity and VPN access			
Servers Backup	1 day	Inability to backup essential servers and services database	Non-availability of key data
BACKUP AND RECOVERY STRATEGY: Network controller allocated laptop with mobile connectivity and VPN access. Backup will continue using the back-up server at The office of the Premier District offices			

NOTE Time-band in which process becomes critical following start of emergency

Table 12: Less-essential activities

Name of process	Time-band*	Potential disruption	Potential impact
ECDHS Website update	4 hours	ECDHS website content is not up-to- date	Unable to do HSS reporting. Incorrect information on website
Back-up and recovery strategy: Network controller and ICT manager allocated laptops with mobile connectivity and VPN access Configure the ISA server to point to SITA for Internet connectivity			
User Account and e- mail Management	5 days	New employee/contractors are not allocated user account to access ECDHS network and use e-mail facility.	Loss of employee productivity.
BACK-UP AND RECOVERY STRATEGY: Network controller and ICT manager allocated laptop with mobile connectivity and VPN access. VPN access to ECDHS network via SITA			

TIME-BAND IN WHICH PROCESS BECOMES CRITICAL FOLLOWING START OF EMERGENCY

COMPLETED BY	NAME:	DATE:
REVIEWED BY	NAME:	DATE:

3.8.9 Information and documentation back-up and recovery strategy

It is necessary to clearly identify the dependencies that the organisation has on digitized information, and to develop workable strategies for continuing an adequate level of business operations during a serious disruption, even though, in certain circumstances, access to such information may become difficult or even impossible.

The main information, data and documentation required by the organisation to carry out its normal business processes are listed below, together with an assessment of the impact of a disruption, and an

agreed method of backup and recovery strategy, as considered appropriate.

Table 13: Data and information required to continue normal business

Name of document, data or information	System or location where normally held	Potential disruption	Potential impact	Method of back-up and recovery
ICT Policy	Electronic Copy on the Server			A copy will be kept at the off-site storage site
Communication Strategy	ICT Manager's Office			A copy will be kept at the off-site storage site
Exchange Infrastructure configuration document		Exchange not working as expected	Unable to reconfigure the Exchange server roles	A copy will be kept at the off-site storage site
SLA – Advisory and Project Management	ICT Manager's Office			Will be recovered from the server at the SITA switching centre. A copy will be kept at the off- site storage site
SLA Website Maintenance with SITA	ICT Manager's Office			Will be recovered from the server at the SITA switching centre. A copy will be kept at the off- site storage site
SLA – Wireless Maintenance with IT master	ICT Manager's Office			Will be recovered from the server at the SITA switching centre. A copy will be kept at the off- site storage site

COMPLETED BY	NAME:	DATE:
REVIEWED BY	NAME:	DATE:

3.8.9.1 Information and documentation back-up and recovery strategy

It is necessary to clearly identify the dependencies that the organisation has on digitized information, and to develop workable strategies for continuing an adequate level of business operations during a serious disruption, even though, in certain circumstances, access to such information may become difficult or even impossible.

The main information, data and documentation required by the organisation to carry out its normal business processes are listed below, together with an assessment of the impact of a disruption, and an agreed method of backup and recovery strategy, as considered appropriate.

Table 13: Data and information required to continue normal business

Name of document, data or information	System or location where normally held	Potential disruption	Potential impact	Method of back-up and recovery
ICT Policy	Electronic Copy on the Server			A copy will be kept at the off-site storage site
Communication Strategy	ICT Manager's Office			A copy will be kept at the off-site storage site
Exchange Infrastructure configuration document		Exchange not working as expected	Unable to reconfigure the Exchange server roles	A copy will be kept at the off-site storage site
SLA – Advisory and Project Management	ICT Manager's Office			Will be recovered from the server at the SITA switching centre. A copy will be kept at the off-site storage site
SLA Website Maintenance with SITA	ICT Manager's Office			Will be recovered from the server at the SITA switching centre. A copy will be kept at the off-site storage site
SLA – Wireless Maintenance with IT master	ICT Manager's Office			Will be recovered from the server at the SITA switching centre. A copy will be kept at the off-site storage site

COMPLETED BY	NAME:	DATE:
REVIEWED BY	NAME:	DATE:

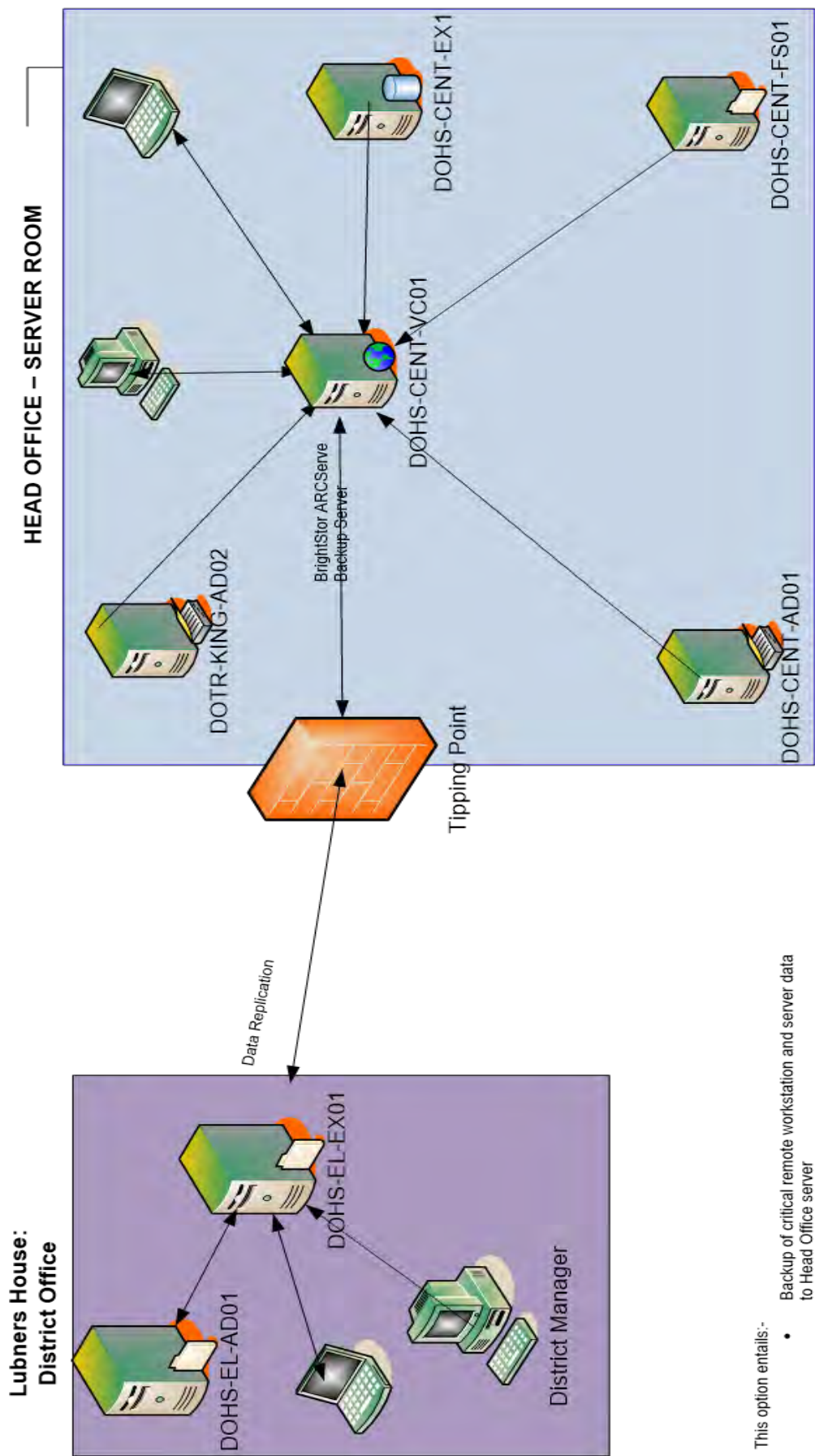
3.8.10 VMWARE backup strategy and architecture

3.8.10.1 Strategy

The following servers and subdirectories must be backed up using CA BrightStor Arcserve Software.

Server Name	Description	Server IP Address	Backup Folder
ECDHS-CENT-EX16	Exchange Server (eMail)	10.220.19.233	Systems state C:\inetpub C:\windows\NTDS C:\windows\Sysvol Exchange databases Ms Exc Storage group
ECDHS-CENT-FS01	File server	10.220.19.232	System State E:\All Data E:\Johan Cash Book E:\Server Application E:\Public Share G:\Apps G:\Home Folder
ECDHS-CENT-AD16	Active directory Primary	10.220.19.230	System State C:\windows\NTDS C:\windows\Sysvol
ECDHS-CENT-AD02	Active Directory Secondary Server	10.220.19.231	Systems state C:\windows\NTDS C:\windows\Sysvol
ECDHS-CENT-VC01	Virtual Configuration server (Runs the Backup Software)	10.220.19.245	Systems State CA Arcserve Backup Database
ECDHS-EL-AD01	Active directory Primary	10.220.51.230	System State C:\windows\NTDS C:\windows\Sysvol
ECDHS-EL-EX01	Exchange Server (eMail)	10.220.51.233	Systems state C:\inetpub C:\windows\NTDS C:\windows\Sysvol Exchange databases Ms Exc Storage group

3.8.10.2 Architecture-- decentralised backup



This option entails:-

- Backup of critical remote workstation and server data to Head Office server

Special consideration:

Care must b taken to limit the amount of data to be backed up over the WAN due to bandwidth

3.8.11 Constraints and special considerations

- (a) Only critical data must be backed up over the WAN, through replication of Active Directory and Exchange Server.
- (b) Tape devices will be required at remote servers to cater for remote servers for local remote server backup.
- (c) Offline folder synchronisation for desktops and laptops is required to facilitate local remote data centralisation for remote sites.
- (d) Firewall: care must be taken to ensure the backup traffic is allowed through.

Term	Definition
Archive	the process of moving inactive files from online disk storage to tape, i.e. deleting the files from disk after copying them, in order to release online storage for re-use
VMWARE	backup solution
Backup	the process of copying active files from online disk storage to tape so that files may be restored to disk in the event of damage to or loss of data
Backup administrator	a person designated to perform the administration functions and maintenance of the backup solution
Restore	The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.
Backup tape	the tape storage media where the information is to be stored for offline and/or offsite storage
Department	the Department of Human Settlements
End user	the person utilising the information
Grandfather- Father- Son (GFS)	a tape rotation strategy. GFS simplifies tape handling by organizing rotation into daily, weekly, and monthly backup tapes. You can also create Custom backup jobs that use the GFS strategy

3.9 FIREWALL POLICY

3.9.1 Introduction

One of the ECDHS ICT services' priorities is the maintenance of a safe and secure computing environment. There are a number of risks associated with the connection of any organisation to the Internet. The assets at risk from targeted attacks against the network include data/information, software and hardware. Services, including access to the Internet and access to central servers are also at risk. Often, the data that is stored on such servers are the true targets of attackers.

The department's firewalls must allow access to protected resources from authorized users located outside the firewall. An increasing number of users work at home or while travelling. While this method does protect against many intrusions, it is not bullet proof. When a violation is suspected, the firewall architecture has logging capabilities to provide forensic information.

The ECDHS ICT Services designed a firewall policy to effectively enable the security control mechanisms found within the perimeter firewalls.

3.9.2 Purpose

The ECDHS herewith known as "department" operates firewalls or gateways between the Internet and the ECDHS network to establish a security environment for the department's computer and network resources. The firewalls are key components of the Department's Network Security Architecture. The department's Firewall Policy governs how the firewalls will filter Internet traffic to mitigate the risks and losses associated with security threats to the department's network and information systems.

The purpose of this document is to define a firewall policy for the ECDHS. The policy will guide the commissioning, implementation and the maintenance of the firewall. The policy establishes a baseline on which the firewall shall be managed and operated.

3.9.3 Scope

This policy refers specifically to the ECDHS ICT environment. The policy provides governance for ECDHS ICT Services firewall. All employees, third parties and customers of ICT Services are subject to this policy and are required to comply with this policy.

This document describes the default set of rules for handling incoming and outgoing traffic for all departmental machines connected to the main collection of subnets, i.e., machines with “true” IP addresses being directly visible from the world. It also outlines the procedure for modifying the default policy for individual machines. Unless a different policy is explicitly requested for a given machine, the machine will be automatically covered by the default set of rules.

3.9.4 Firewall roles and responsibilities

The following roles and responsibilities are defined for the implementation, operation management and maintenance of the firewall:

ECDHS management

ECDHS ICT management is responsible for the overall firewall function which includes:

- ensuring that the firewall is implemented maintained and operated in a secure environment;
- putting in place processes and structures for secure firewall operations;
- assigning and overseeing the role and responsibilities of a firewall administrator;
- keeping an updated copy of documented firewall rules;
- ensuring that access requirements through the firewall are clearly articulated;
- ensuring that necessary firewall infrastructure is provided to the entire department; and
- effectively managing client's expectations.

Firewall administrator

The firewall administrator is responsible for the configuration of the firewall software; he/she shall ensure that the firewall is configured to only allow authorised and secure access to the hosted services and systems at the hosting site.

Adhere to all procedures and processes for secure operation and configuration of the firewall.

Provide technical lead for firewall policy and procedure implementation, with the primary responsibility for ensuring operational continuity of the firewall.

Implement firewall rule set changes, additions and deletions in line with the firewall access rules.

Maintain the firewall. Monitor firewall logs.

Initiate the response to any possible security incident on the firewall. Act as the liaison for incident reporting to the relevant stakeholders.

3.9.4.1 ECDHS infrastructure services management

The ECDHS business units are the client to ECDHS Infrastructure Services with regard to the firewall services. The following are their responsibilities.

3.9.4.2 Clients

Clients shall follow the prescribed processes and procedures for requesting access to hosted services and systems.

3.9.4.3 Firewall user account management and access control

The management of user accounts on the firewall is the responsibility of ECDHS ICT Management. Only authorised user accounts should be created on the firewall, changes to the firewall user accounts should be authorised and approved by ECDHS ICT Management before they are implemented.

Only the firewall administrator and backup administrator shall be given user accounts on the firewall. The responsible manager in ECDHS ICT shall also have supervisory access on the firewall.

3.9.5 Policy statements

The firewall system must be securely implemented and used only for the purpose it was intended to. All operations on the firewall shall be governed by this policy. ICT Management within Corporate Services must ensure that the firewall is implemented; maintained and managed appropriately in a secure manner.

3.9.5.1 Firewall configuration management

Firewall rules management

All firewall configurations should be documented and recorded in a configuration management system. Changes to configurations should be done in line with the department's change management procedure.

It is important that the operational procedures for a firewall and its configurable parameters be well documented, updated, and kept in a safe and secure place.

3.9.5.2 Change management

Any changes to the firewall should be implemented in line with the department's change management procedure. The ECDHS ICT management shall ensure that all changes are informed by a valid business requirement, authorised and tested before they are implemented on the firewall. Only authorised personnel must implement changes on the firewall.

3.9.5.3 Backup and recovery

A backup and recovery strategy for the firewall should be developed and implemented. The backup and recovery strategy should be based on the availability requirements for the firewall. ICT within Corporate Services shall develop and implement the backup and recovery strategy, and shall ensure that the firewall services can be restored as required in the event of a disaster.

3.9.5.4 Auditing and logging

In order to enable investigation and monitoring of the firewall activities, all firewall activities should be logged.

- (a) The firewall logs should be kept securely.
- (b) Only read access privileges should be assigned to the designated firewall administrator(s).
- (c) The firewall must be configured to log all reports on daily, weekly, and monthly bases.
- (d) Firewall logs should be examined on a regular basis to determine whether attacks have been detected.

The following are security-relevant events that should be recorded on the firewall's logs.

- (a) Break-in attempt
- (b) Changes to firewall rules
- (c) Security violation attempts
- (d) Hardware and disk media errors
- (e) Login/logout activity
- (f) Connect time
- (g) Use of system administrator privileges
- (h) Inbound and outbound traffic
- (i) TCP network connect attempts

In order to provide assurance and reliability on the firewall services; ICT management shall ensure that:

- an independent audit of the firewall security is conducted; and
- access to the firewall rules is monitored; unauthorised access is identified and appropriate action is taken.

3.9.5.5 Physical security

The firewall servers and all relevant firewall devices should be stored in a secured environment. All environmental threats to the firewall should be identified and eliminated. Departments ICT unit together with Anti-corruption unit shall ensure implementation of appropriate physical security such that, no unauthorised person will have physical access to the servers and devices.

3.9.5.6 Incident handling

An incident management process should be developed and implemented to deal with all security incidents on the firewall. The ICT department shall develop and implement the incident management process for the firewall. The firewall administrator(s) must be notified at any time of any security alarm by e-mail, pager, or other means so that she/he may immediately respond to such alarm.

3.9.5.7 Firewall rule set

Firewall rule set should be built to be as specific as possible with regard to the network traffic they control. Rule sets should be kept as simple as possible, so as not to accidentally introduce holes in the firewall that might allow unauthorized or unwanted traffic to traverse a firewall.

The default policy for the firewall for handling inbound traffic should be to block all packets and connections unless the traffic type and connections have been specifically permitted.

The firewall rule set should always block the following types of traffic:

- (a) Inbound traffic from a non-authenticated source system with a destination address of the firewall system itself. This type of packet normally represents some type of probe or attack against the firewall.
- (b) Inbound traffic with a source address indicating that the packet originated on a network behind the firewall. This type of packet likely represents some type of spoofing attempt.
- (c) Inbound traffic containing ICMP traffic. Since ICMP can be used to map the networks behind certain types of firewalls, ICMP should not be passed in from the Internet, or from any untrusted external network.
- (d) Inbound or outbound traffic from a system using a source address that falls within the address ranges set aside in RFC 1918 as being reserved for private networks. For reference purposes, RFC 1918 Inbound traffic with these source addresses typically indicates the beginning of a denial-of-service attack involving the TCP SYN flag.
- (e) Inbound traffic from a non-authenticated source system containing SNMP traffic. These packets can be an indicator that an intruder is probing a network, but there are few reasons an organisation or agency might want to allow inbound SNMP traffic, and it should be blocked in the vast majority of circumstances.
- (f) Inbound traffic containing IP source routing information. Source routing is a mechanism that allows a system to specify the routes a piece of network traffic shall employ while travelling from the source system to the destination system. Source routing has the potential to permit an attacker to construct a network packet that bypasses firewall controls. In modern networks.

Inbound or Outbound network traffic containing a source or destination address of 127.0.0.1 (localhost). Such traffic is usually some type of attack against the firewall system itself.

Inbound or Outbound network traffic containing a source or destination address of 0.0.0.0. Some operating systems interpret this address as either localhost or as a broadcast address, and these packets can be used for attack purposes.

Inbound or Outbound traffic containing directed broadcast addresses. A directed broadcast is often used to initiate a broadcast propagation attack such as SMURF. Directed broadcasts allow one computer system to send out a broadcast message with a source address other than its own. In other words, a system sends out a broadcast message with a spoofed source address. Any system that responds to the directed broadcast will then send its response to the system specified by the source, rather than to the source system itself. These packets can be used to create huge storms of network traffic.

Operations

Any changes that may be required to the firewall's configuration in order to allow previously disallowed traffic. An official department change request procedure shall be followed and the infrastructure manager may approve such request. All requests shall be assessed to determine whether they fall within the parameters of acceptable risk.

Approval is not guaranteed as associated risks may be deemed too high. If this is the case, an explanation will be provided to the original requestor and alternative solutions will be explored.

Customers may request access from the Internet for services located on the Hosting Services network. This remote access should be secured:

- i. Remote sessions shall have an absolute timeout length. At the end of these timeout periods, users must re-authenticate to continue or re-establish their remote connection.
- ii. A remote access request form, with full justification, must be submitted to the infrastructure manager for approval. Approval is not guaranteed.
- iii. From time to time, outside vendors, contractors, or other entities may require secure, short-term, remote access to the Infrastructure services shared network. If such a need arises, a third-party access request form, with full justification, must be submitted to the infrastructure manager for approval. Approval is not guaranteed.

3.9.5.8 Periodic review

Quite often, custom policies will be requested for a limited time. To avoid situations where a custom policy that was requested a long time ago, has not been needed for a long time (e.g., the service is not being offered any more), but it still remains in effect and creates a potential security problem:

- the policy document shall be reviewed at least annually in the third quarter of the financial year. Where the policy is materially revised, this shall be published before the end of the third quarter of the financial year to ensure that budgetary issues which may arise can be addressed during the annual budgetary cycle;
- the revised document shall be agreed and approved by the business continuity management team; and
- review of the policy must relate to the operational circumstances within the department and the overall business strategy, addressing any relevant changes in the department, its operations or operating environment and any legislative requirements, which may have occurred since the previous revision.

3.9.6 Compliance

ISO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.

Failure to comply with this policy may result in disciplinary action, which may include termination of employment.

Wherever possible, technological tools shall be used to enforce this policy and mitigate security risks.

3.10 CONFIGURATION MANAGEMENT POLICY

3.10.1 Introduction

The ECDHS shall develop, implement and maintain a coordinated department-wide plan for monitoring IT performance, including, the formulation of policies to effect the objectives of the department.

3.10.2 Purpose

The purpose of this IT Configuration Management policy is to ensure the integrity of hardware and software configurations are well establishment and maintenance of an accurate and complete configuration repository. This policy facilitates the collection of initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the

configuration repository as needed. Effective configuration management facilitates greater system availability, minimises production issues and resolves issues faster.

The implementation of the Configuration Management policy shall ensure that controls set up as baseline configurations to hardware and software within the department are adhered to. In addition this, it shall ensure that standard configuration comprises organising, implementing and supervising the following tasks.

- Identify the configuration; to identify the systems concerned, and to define their descriptive documentation (configuration identification).
- Control the configuration; to establish configuration baselines, to set up and implement change control, control of interfaces (configuration control).
- Record and follow-up the configuration; to record the product's different configurations, and to permit its use by means of configuration statuses (configuration status accounting).
- Verify that the product design meeting the required attributes has been adequately documented, as well as the verification article's compliance with the design in order to establish the product configuration (configuration verification); and
- Audit the Configuration Management system; to verify that the Configuration Management system is effective and meets the requirements of the organisation.

3.10.3 Scope

The policy applies to all business units within the ECDHS that has any Information and Technology system, application or infrastructure.

The policy addresses the following controls found in the ISO/IEC 27002:2005, ISO/IEC 27001 BSi, ITIL standards.

3.10.3.1 ITIL

- Change management
- Availability management
- Release management

3.10.3.2 ISO

- (a) 3.3.2.2 Design and development planning
- (b) 3.3.2.3 Design and development inputs
- (c) 3.3.2.4 Design and development outputs
- (d) 3.3.2.6 Design and development verification

3.10.3.3 BSi

Security in development and support processes.

- (a) 10.2.1 Input data validation
- (b) 10.2.2 Control of internal processing
- (c) 10.5.4 Covert channels and Trojan code

The supporting policy statements with regard to software configuration management should at minimum include:

- (a) identification,
- (b) version control,
- (c) change control,
- (d) configuration quality assurance, and
- (e) reporting.

3.10.4 Roles and responsibilities

3.10.4.1 The HoD

The HoD working in conjunction with the CFO shall be responsible for ensuring the effective implementation and compliance of the ECDHS policies, standards and procedures.

3.10.4.2 Information security officer

ISO is also responsible for maintaining this policy.

3.10.4.3 Internal audit

The Internal Audit department is authorised by management to assess compliance with all corporate policies at any time.

The Internal Audit department may assist with audits of outsourcing contracts including security compliance audits, and advise management on the risks and controls relating to outsourcing.

3.10.4.4 GITO

- (a) The GITO within the ECDHS is responsible, among other duties, to advise the department on the application of IT to improve service delivery. The GITO should be responsible for developing an IT Security policy framework, IT procurement guidelines, e-Government policy and strategy. The GITO should also monitor departmental IT projects to avoid duplication.
- (b) The GITO working in conjunction with the CFO, shall be responsible for ensuring the effective implementation of the ECDHS IT technology policies, standards and procedures.

3.10.5 Policy statements

3.10.5.1 Configuration repository baseline

The ECDHS must ensure that there is a central repository to contain all relevant information on configuration items and it must be well established. The ICT Configuration Management function via an appropriate configuration management database should be continuously updated and maintained, and moves, deletions, and change must be recorded.

Relevant information to consider is naming, version numbers and licensing details. A baseline of configuration items should be kept for every system and service as a checkpoint to which to return after changes.

3.10.5.2 Configuration repository and baseline – statements

The department shall establish and maintain a central repository that contains all relevant information on configuration items.

The department shall automate and integrate the configuration management function with the service desk and a CRM system.

The department shall establish and maintain a CMDB (Software Configuration Policy and Procedure Elements Information is provided in annex C).

The department shall make the CMDB available in easy format for Service Desk agents, incident managers, and problem managers.

The department must continuously update and maintain the CMDB for moves, additions, and deletions.

The department must add relevant information to the CMDB, e.g. naming, version numbers and licensing details.

The department must establish an audited baseline of configuration items and keep for every system

and service.

3.10.5.3 Identification and maintenance of configuration items

The department must ensure that there is a clear identification of configuration items and that this information is constantly and consistently updated and maintained.

Identification and maintenance of configuration items – statements

The department shall implement and maintain procedures and processes that prescribe the identification of configuration items and these attributes must be business oriented.

The department shall implement and maintain procedures for recording new, modified and deleted configuration items and these must function correctly and not be in manual format.

The department shall ensure that there are procedures for the process to identify and maintain relationships among configuration items in the CMDB.

The department shall ensure that updating existing configuration items into the CMDB must take place at all times and must not be a manual function.

The department shall ensure that there is a policy and procedure for preventing the use of unauthorised software.

3.10.5.4 Configuration integrity review

There shall be reviews to verify the CMDB on a regular and consistent basis.

Configuration integrity review – statements

The department shall implement a formal accepted policy and supporting procedures to regulate the use of software usage and unlicensed software, or any instances in excess of current license agreements.

The department shall ensure that there are mechanisms or tools in place to automate the detection of deviations and errors.

3.10.5.5 Consistent actions to be undertaken

Management shall be aware of the need for controlling the IT configuration and understand the benefits of accurate and complete configuration information.

Configuration management tools must be employed and it is recommended that they must be uniform among different ICT platforms within the organisation.

Consistent actions to be taken – statements

The department shall ensure that there are standard working practices with regard to IT Configuration and these must be clearly defined.

The department shall ensure that configuration data content is not limited and must be used by interrelated processes, such as change management and problem management.

The department shall ensure that procedures and working practices with regard to configuration management are documented, standardised and communicated, and training and application of the standards for all individuals must be a responsibility of the ICT directorate. In addition, similar configuration management tools must be implemented across platforms.

The department shall ensure that deviations from procedures are detected and physical verifications performed consistently. Automation must be adopted to assist in tracking equipment and software changes.

3.11 GENERAL CM TASKS AND PRINCIPLES

3.11.1 General configuration management tasks

Identify the configuration; to identify the systems concerned, and to define their descriptive documentation (configuration identification).

Control the configuration; to establish configuration baselines, to set up and implement change control, control of interfaces (configuration control).

Record and follow-up the configuration; to record the product's different configurations, and to permit its use by means of configuration statuses (configuration status accounting).

Verify that the product design meeting the required attributes has been adequately documented, as well as the verification article's compliance with the design in order to establish the product configuration (configuration verification).

Auditing the Configuration Management system; to verify that the Configuration Management system is effective and meets the requirements.

3.11.2 General configuration management principles

3.11.2.1 B.2.1 Configuration items

Configuration items divide a complex product or system into manageable segments and components.

A configuration item is an aggregation of hardware, software, processed materials, services or any of its discrete portions, which is designated for configuration management and treated as a single entity in the configuration management process.

Configuration item (CI). A configuration item is an aggregation of hardware or software that satisfies an end use function and is designated by the government for separate configuration management.

Software (*configuration*) item: An aggregation of software, such as a computer program or database, that satisfies an end use function and is designated for purposes of specification, qualification testing, interfacing, configuration management, or other purposes. Software items are selected based on tradeoffs among software function, size, host or target computers, developer, support strategy, plans for reuse, criticality, interface considerations, need to be separately documented and controlled, and other factors. A software item is made up of one or more software units.

3.11.2.2 B.2.2 Configuration baselines

Configuration baselines divide the project phases for concept evaluation (feasibility), development (preliminary definition), design (detailed definition), production and utilization of a product into manageable segments by defining specific reference configurations during the life-cycle of a product and provide agreed departure points for further evolutions.

Configuration of a product, formally established at a specific point in time, which serves as reference for further activities.

A configuration baseline is characterized by a (set of) document(s), which describe(s) the characteristics, or certain characteristics of a product. This (set of) document(s) is formally designated as the configuration reference at a key stage in the product life-cycle, which thus corresponds to a major product definition event. Any change of a product attribute specified or disclosed in this (set of) document(s) shall be subject to a formal change procedure involving all the actors and disciplines concerned before it can be taken into account.

(*Configuration*) baseline: (1) An agreed-to description of the attributes of a product, at a point in time, which serves as a basis for defining change. (2) An approved and released document, or a set of documents, each of a specific revision; the purpose of which is to provide a defined basis for

managing change. (3) The currently approved and released configuration documentation. (4) A released set of files comprising a software version and associated configuration documentation.

Configuration Baseline. Configuration documentation formally designated by the government at a specific time during a CI's life cycle. Configuration baselines, plus approved changes from (*correct: to*) those baselines, constitute the current approved configuration documentation. There are three formally designated configuration baselines in the life-cycle of a configuration item, namely the functional, allocated, and product baselines.

3.12 CONFIGURATION POLICY ELEMENTS

3.12.1.1 Software configuration elements

The relevant reference text and best practices in choosing and defining software configuration elements should at minimum include the following:

3.12.1.2 ISO 9001 – 20000

Integrated Quality Management System.

3.12.1.3 C.1.2 ITIL

- (a) Change management
- (b) Availability management
- (c) Release management

3.12.1.4 C.1.3 ISO

- (a) 3.3.2.2 Design and development planning
- (b) 3.3.2.3 Design and development inputs
- (c) 3.3.2.4 Design and development outputs
- (d) 3.3.2.6 Design and development verification

3.12.1.5 C.1.4 BSI

Security in development and support processes

- 10.2.1 Input data validation
- 10.2.2 Control of internal processing
- 10.5.4 Covert channels and Trojan code

The supporting policy statements with regard to software configuration management should at minimum include:

- (a) identification,
- (b) version control,
- (c) change control,
- (d) configuration quality assurance, and
- (e) reporting.

3.12.1.6 Software configuration procedure elements

At minimum the defined software configuration procedure elements should include the following:

- Identification of software configuration items
- Version control
- Change control
- Configuration quality assurance
- Reporting
- Systems development life cycle considerations
- New application development

Alpha or development phase (initial setup, program Loaded or component is to be changed, the development is complete).

Beta or testing phase (initial setup, compilation is complete and executables are ready, testing is complete).

Final or production phase (initial setup, application goes live, configuration quality assurance).

Existing application development

- (f) Status reporting (status accounting)
 - i. Determine what happened
 - ii. Determine who did it
 - iii. Determine when did it happen
 - iv. Determine what else will be affected
- (g) Maintenance and control
 - Maintain administration
 - Control workflow
 - Software configuration server physically controlled
 - Adequate accessibility
 - Control under normal development
 - Control under emergency conditions

3.13 PERSONNEL SECURITY POLICY

3.13.1 Introduction

Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of any information user to know these guidelines and to conduct their activities accordingly.

3.13.2 Purpose

The purpose of this policy is to outline the acceptable use of any information and information system within the ECDHS.

The objectives of this policy are to:

- (a) mitigate against legal liability by setting boundaries for appropriate employee conduct when using ICT facilities;
- (b) safeguard our ICT facilities from abuse, damage or disruption;
- (c) ensure that employees understand that ICT facilities provided to them are primarily for business use; and
- (d) comply with all relevant regulatory and legislative requirements such as the Regulation of Interception of Communications Act (2002) and the provisions of the Electronic Communications and Transactions Act (2001).

3.13.3 Scope

This is a standard departmental policy that applies to all contractors, vendors and users with access to the department's information and technology systems.

3.13.4 Roles and responsibilities

3.13.4.1 The GITO

The GITO shall implement, enforce and monitor the controls in accordance with the requirements outlined by management, and must advise users on the correct ways to access information and systems.

3.13.4.2 All employees

All employees are responsible for complying with this and other corporate policies at all times. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of acceptable behaviour) to comply with our information security policies.

3.13.4.3 Information security officer

Information Security Officer is responsible for maintaining this policy and advising generally on information security controls. Working in conjunction with other corporate functions, it is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy.

3.13.4.4 Internal audit

Internal Audit is authorised by management to assess compliance with all corporate policies at any time.

3.13.4.5 Human resource department

The Human Resources department shall perform a pre-employment screening on all employees of the Department of Human Settlements. This may include background investigations, character references, education verification, credit check (if applicable) and independent identity checks (if the employee is hired via a third party or staffing agency; proper screening checks shall be verified by that agency).

The Human Resources department shall facilitate secure and confidential information handling policies when introducing new individuals to the Department of Human Settlements. All new employees shall receive a copy of the information security policies and/or security awareness materials appropriate for their positions and roles in the Department of Human Settlements and acknowledge, in writing, that they understand their responsibilities as stated in the policies.

The Human Resources department shall immediately notify ICT department on the resignation or termination of employees. On notification of transfer or termination, ICT department shall ensure that the user ID access is revoked or modified on notification of transfer or termination. Any items issued to the employee or vendor, such as laptop computers, keys, Access cards, software, data, documentation, manuals etc., shall be returned to their manager or the Human Resources department, as appropriate.

3.13.5 Policy statements

All users shall sign a non-disclosure or confidentiality agreement prior to accessing Department of Human Settlements' facilities or information. Employees shall sign this agreement as part of the initial terms and conditions of employment.

All users are responsible for reviewing and understanding the security policies and procedures of the ICT department. Employees shall agree, in writing, to accept and abide by the standards set forth in the policies. Any questions on specific details of the policies should be directed to their supervisor or Senior Manager ICT.

Security responsibility is part of the terms and conditions of employment. Violation or disregard for the responsibilities documented in the Department of Human Settlements' security policies will be grounds for disciplinary actions.

Before receiving their first computer accounts, all users shall sign a statement that they are aware that actions on Department of Human Settlements' networks may be monitored and that they give their consent to the monitoring.

Information stored on or passed through Department of Human Settlements' computer communications hardware is not considered private. Users of this equipment shall not have expectations of privacy of any data and information; electronic mail and voice mails are specifically

covered under this policy.

Security responsibilities are extended beyond the premise of Department of Human Settlements with regard to the Department of Human Settlements information. Therefore, employees shall maintain confidentiality of information outside work, in home-working or remote access situations.

Casual browsing of user e-mail and voice mail by administrators and alternates is a violation of Department of Human Settlements' policy. However, management has the right to examine any such information without prior consent of or notification to the employee if it is believed that the employee is misusing Department of Human Settlements equipment.

3.13.5.1 User security awareness training

The ICT department is responsible for posting security advisories for all users who may be affected by security issues.

- (a) It is the responsibility of the Senior Manager ICT department to promote constant security awareness to all information users. The security awareness programme shall consist of awareness training and periodic awareness briefings.
- (b) Third party employee orientation: on contract employment and joint ventures at the ICT department, all staff members shall be briefed by the Human Resources department on the application of the information security policy and procedures in the Department of Human Settlements. A written summary of the basic information security measures shall be provided to new staff.
- (c) New employee orientation: on permanent or contract employment at Department of Human Settlements, all staff members shall be briefed on the application of the information security policy and procedures in the Department of Human Settlements. A written summary of the basic information security measures shall be provided.

3.13.5.2 Responding to security incidents and malfunctions

General responsibilities

If an employee suspects a security weakness or notices an area of exposure to Department of Human Settlements' security, the employee shall notify the Senior Manager ICT department. The employee is forbidden to test the security weakness without the cooperation and information security officer.

If a virus is suspected on a system, the user shall disconnect the system from the network immediately, notify and work with the ICT department to remove the virus prior to any reconnection to network services. It is the responsibility of the user, with appropriate technical assistance, to ensure that the virus is successfully removed before reassuming communications on Department of Human Settlements' networks. The ICT department shall notify the Senior Manager ICT or ICT manager of the incident.

If a security incident is suspected or noticed by any employee, the employee shall immediately notify the Senior Manager or ICT Manager of the incident.

General standards

The employee shall document all reports of security incidents. Led by the Senior Manager ICT or ICT manager, the IT Manager shall also include a process to review all incidents, document "lessons learned" and coordinate training and learning sessions for applicable areas in Department of Human Settlements.

To report a software malfunction or error, users shall contact the ICT department. The user should note any symptoms, error messages or failures. The ICT department shall notify the Senior Manager ICT or ICT manager if the software malfunction is in any way suspect or indicative of security vulnerability.

For Department of Human Settlements' officials, contractors or joint venture partners, disciplinary action resulting in violation of the security policy will be consistent with the severity of the incident, as determined by an investigation. Disciplinary actions may include, but are not limited to, loss of access privilege to data processing resources, dismissal of consultants, cancellation of contracts, termination of employment or other actions as deemed appropriate. Disciplinary actions are coordinated through

the Human Resources department in accordance with the South African Labour Relations Act (Act no. 12 of 2002) in case of employees.

3.13.6 Compliance

The GITO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.

Failure to comply with this policy may result in disciplinary action, which may include termination of employment.

Any conduct that interferes with the normal and proper operation of the departments IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved IT policies.

The ECDHS management reserves the right to revoke the privileges of any user at any time.

Violations of this policy will be subject to disciplinary action as described in HR policy: employee conduct, and in accordance with the South African Labour Relations Act (Act no. 12 of 2002). It may result in dismissal.

3.14 MALICIOUS CODE POLICY

3.14.1 Introduction

In order to protect the integrity of ECDHS software and information an antivirus and malicious-code program shall be deployed and managed to ensure effective management of the risks relating to viruses and malicious code. Damage caused by malicious software must be prevented, using preventive and detective controls.

Malicious code is a new breed of Internet threat that cannot be efficiently controlled by conventional antivirus software alone. In contrast to viruses that require a user to execute a program in order to cause damage, malicious codes are auto-executable applications. Malicious-code program typically includes computer viruses, worms, Trojan horses, spyware, adware and malicious mobile code (executable code in the form of Java applets, MS ActiveX, JavaScript or VBScript, that has been written deliberately to perform unauthorised functions). All individuals who have access to information and systems of the Department should be aware of the risks from malware, and the actions required minimising those risks.

3.14.2 Purpose

This policy establishes malicious code prevention requirements for ECDHS information resources.

3.14.3 Scope

This is a standard department policy that applies throughout the department as part of the corporate governance framework. It applies to all users of the departments ICT systems and all devices capable of propagating malicious code and attached or requires access to the department network.

3.14.4 Roles and responsibilities

3.14.4.1 The GITO

The GITO must implement, enforce and monitor the controls in accordance with the requirements outlined by management, and must advise users on the correct ways to access information and systems.

Responsible for building, configuring, operating and maintaining the departments ICT facilities (including anti-spam, anti-malware and other email security controls) in accordance with this policy.

Responsible for assisting users with secure use of ICT facilities, and acts as a focal point for reporting

ICT security incidents.

Responsible for ensuring that all devices have approved malicious code version and release installed and mechanism is in place to ensure malicious code patterns are updated and current.

3.14.4.2 All employees

All employees are responsible for complying with this and other corporate policies at all times. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of acceptable behaviour) to comply with our information security policies.

3.14.4.3 Information security officer

Information Security Officer is responsible for maintaining this policy and advising generally on information security controls. Working in conjunction with other corporate functions, it is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy.

3.14.4.4 Internal audit

Internal Audit is authorized by management to assess compliance with all corporate policies at any time.

3.14.5 Policy statements

The ECDHS shall ensure that there are adequate resources and skills for:

- installing virus protection software;
- updating software;
- updating virus definition files;
- cleaning infected computers;
- distributing information to users;
- identifying unprotected computers and implementing remedial measures; and
- where the ECDHS does not have these resources in-house, it must make a contract with an external provider. The ECDHS shall have access to either internal or third party resources for the:
 - evaluation of virus protection software for PCs and workstations;
 - evaluation of virus protection software for servers, mail-servers and firewalls;
 - evaluation of the vendors of the software packages;
 - evaluation of the risk in a new virus;
 - deciding if distributed warning signals are true or false; and
 - continuous evaluation of the efficiency of software installed.
- The ECDHS shall have effective procedures in place:
- for logging, reporting and escalation of potential virus incidents; and
- for cleaning virus-infected computers; the cleaning should be performed at the ECDHS premises. If this is not possible and the infected computer has to be transported to an external party, the policies for removing equipment from the ECDHS premises apply.

Any user who suspects infection by a virus shall immediately shut down the specific computer, call the IT Administrator, and make no attempt to remove the virus, unless they are instructed by IT administration or server administrator.

Users shall forward any security warnings information received, for example via e-mail, to the ICT, who will then determine what action is appropriate. Users shall not personally redistribute system-vulnerability information, nor forward the warnings to any other party.

Users must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any ECDHS computer or network.

ECDHS approved anti-virus software shall be installed and enabled on all ECDHS servers (including but not limited to application servers, exchange servers, file servers, network servers), desktop, laptop computers and other end user computing devices.

These machines shall also have the latest virus screening pattern file. The installation and configuration/setup of the virus screening software shall be as per the standards prescribed by the ICT. Any deviation from these standards shall first be approved by ICT.

Exceptions will be made for operating systems and platforms where no known vulnerabilities exist, and for which no anti-virus software exists. All ECDHS computers except for end-user devices must run software that checks for unauthorized files or changes.

ICT shall implement network scanning tools to assess internal vulnerabilities and virus readiness across the network. ICT shall implement real time alerting utilities to centrally monitor the network for virus outbreaks and threats. Computer systems joining the network shall be scanned to ensure that the required software patches and anti-virus software is up to date, and that no viruses are present. This scan shall be carried out periodically while the computer system remains attached to the network. Computer systems failing this scan shall be disconnected or quarantined from the network until steps have been taken to ensure compliance.

Every ECDHS employee who examines, processes, or stores ECDHS information using a computer that he or she owns shall install and regularly run the most current version of a virus detection software package approved by ICT.

Externally-supplied removable computer readable media may not be used on any ECDHS personal computer or server unless they have been checked for viruses.

All outbound software and executable files containing software or executable statements shall be certified as virus free prior to being sent to any third party.

All externally-supplied computer-readable files shall be decrypted prior to being subjected to an approved virus checking process;

Only application software and systems software formally approved by ICT management are to be installed. No executable software, regardless of the source may knowingly be installed on a device connected to the department network. This is applicable to all platforms. The following rules must be observed when planning to download and/or install any software.

Where authorization has been obtained, software may only be downloaded from a known and trusted source. Software verification tools, such as digital signatures shall be employed where possible, for example code-signing certificates, MD5 checksums;

Downloaded software shall be scanned for malicious code prior to being installed.

Software or files received from an external entity, and intended to be installed on ECDHS production machine shall be tested for unauthorized software on a standalone non- production machine before being deployed.

Before any files are restored to a production ECDHS computer system from backup storage media, all backup files shall have been scanned with the latest version of virus screening software.

To ensure that viruses are neither received at nor sent from ECDHS, all communications transmitted shall be checked by virus protection and protocol filtering software installed on mail server and/or firewall.

Anti-Virus software shall be configured to update itself on a regular basis and be capable of receiving pushed updates as and when required.

Virus protection software shall trigger an alarm when a virus has been detected. If the computer is connected to a network, that alarm shall be sent to either a virus protection console that aggregates alarms for the facility or to the person responsible for the cleaning of virus infected computers at the facility.

The virus protection software must be able to quarantine or delete infected files, programs and documents.

Only devices approved by ICT manager may be connected to the department network.

3.14.6 Compliance

- (a) GITO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.
- (b) Failure to comply with this policy may result in disciplinary action, which may include termination of employment.
- (c) Any conduct that interferes with the normal and proper operation of the departments IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved IT policies.
- (d) The department management reserves the right to revoke the privileges of any user at any time.

3.15 NETWORK MANAGEMENT POLICY

3.15.1 Introduction

The ECDHS shall ensure the security of its network, both for internal trusted connections, as well as for untrusted external connections. Network equipment, such as wiring closets, switches and firewalls, shall be regarded as sensitive, and shall be protected with physical and logical access control. The activities on managed network equipment shall be logged in centralized syslog facilities. The network may be internally divided into different segments, depending on evaluated risks. This segmentation may be implemented by means of secure network nodes. The ICT shall be notified immediately of each security event, system implementation or additional network connectivity that may have a security implication for the rest of ECDHS.

3.15.2 Purpose

The purpose of this document is to define and distinguish policies and procedures of how Network should be controlled and managed properly within the ECDHS to ensure security and proper usage.

3.15.3 Scope

This is a standard departmental policy that applies to all users of the departments Information and technology systems.

3.15.4 Roles and responsibilities

3.15.4.1 The GITO

IT must implement, enforce and monitor the controls in accordance with the requirements outlined by management, and must advise users on the correct ways to access information and systems.

3.15.4.2 All employees

All employees are responsible for complying with this and other corporate policies at all times. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of acceptable behaviour) to comply with our information security policies.

3.15.4.3 Information security officer

Information Security Officer is responsible for maintaining this policy and advising generally on information security controls. Working in conjunction with other corporate functions, it is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy.

3.15.4.4 Internal audit department

The Internal Audit department is authorised by management to assess compliance with all corporate policies at any time.

3.15.5 Policy statements

Only authorised people shall have access to wiring closets, especially in buildings where other companies other than ECDHS reside.

For the IT service provider to the ECDHS, the communication between the service provider's network and the ECDHS network shall be controlled by secure, documented interfaces approved by the ECDHS.

In case an interruption in communications or similar event should take place, the ECDHS shall have procedures in place to make sure that all data affected by an interrupted transaction is restored.

Where supported by the device firmware or operating system, managed network devices such as print servers, routers, hubs and switches shall be protected with user name and password credentials, changed from their default values and capable of identifying unique individual users.

The log information of managed network equipment shall be included in centralized syslog facilities.

All data communication between systems and applications shall be controlled, to ensure that:

- all data is transmitted in its entirety; and
- transmission cannot be intercepted or manipulated.
- The following principles apply to untrusted connections:
- all untrusted connections shall be registered with, and authorized by the ICT;
- the ICT shall maintain a current inventory of all connections to external networks including telephone networks, extranets and the internet;
- all untrusted connections shall make use of a secure network node;
- all untrusted connections, shall be secured and will not allow unauthorised access to any sensitive data or systems of ECDHS; and
- all untrusted connections shall be authorised at IT executive level.

The security of an untrusted connection shall not depend on the secrecy of the point of access.

Systems or users who make use of untrusted connections shall not be provided with any unnecessary functionality which may impact the security (system or data) of ECDHS.

All untrusted connectivity (HTTP or SSL) shall be terminated on the secure part of the ECDHS Network.

Application-gateway firewalls (layer 7 firewalls) are required to protect the traffic at the message level.

ECDHS computer systems containing secret information shall not be connected to any untrusted network or computer.

All web servers accessible via the Internet shall be protected by a router and firewall approved by the ICT. All internet commerce servers including payment servers, database servers, and web servers shall be protected by firewalls in a demilitarized zone. Public Internet servers shall be placed on subnets separate from internal ECDHS networks.

Routers and firewalls shall be employed to restrict traffic from the public servers to internal networks. Any user and/or systems requiring access to the ECDHS Internal Network via an untrusted network shall be authenticated on the ECDHS Network. Strong authentication via an access control and/or authentication server is required to authenticate this type of users and/or systems via the network perimeter firewall.

The access control server will be used to authenticate users and/or systems and provide a role based profile which will restrict the user and/or system to the various systems and/or servers. All information security measures which are used in securing an untrusted connection, for example the installation of

a secure network node, shall be in compliance with the information security standards set by ICT. Where standards have not yet been set, ICT shall be approached to ratify proposals.

All inbound dial-up lines, or other in-bound real-time external connections to ECDHS internal networks and/or multi-user computer systems shall pass through an additional access control point including an approved firewall, and access server before users can reach a log-in banner.

All firewalls used to protect ECDHS's internal network shall run on separate dedicated computers. These computers may not serve other purposes such as act as web servers.

Firewall configuration rules and permissible service rules have been reached after an extended evaluation of costs and benefits. These rules shall not be changed unless the permission of the ICT has first been obtained, and appropriate change control procedures have been followed.

All connections between ECDHS internal networks and the internet (or any other publicly accessible computer network) shall include an approved firewall and related access controls.

The establishment of Internet or any other external network connections (including 3G), is prohibited unless this connection has first been approved by ICT, and after the ICT has determined that the combined system will be in compliance with ECDHS security requirements. These connections include the establishment of multi-computer file systems, internet home pages, internet FTP servers, and the like. All tunnels are to be secured via methods acceptable to ICT and will terminate on a dedicated tunnelling device such as a VPN concentrator. Users and vendors shall not make arrangements for, or actually complete the installation of data lines with any carrier, if they have not first obtained approval from the ICT. The management of nodes (routers etc.) which reside on untrusted networks may not reduce the level of security, which is required between trusted and untrusted networks.

Unless the executive management have all approved in advance, employees are prohibited from using new or existing internet connections to establish new business channels. These channels include EDI arrangements, electronic malls with on-line shopping and on-line database service.

Users shall not establish intranet servers, electronic bulletin boards, local area networks, modem connections to existing internal networks, or other multi-user systems for communicating information without the specific approval of ICT. This policy helps ensure that all ECDHS-networked systems have the controls needed to prevent unauthorised access.

Real-time connections between two or more in-house computer systems shall not be established unless ICT has first determined that such connections will not jeopardize information security of the department.

As a condition of gaining access to ECDHS's computer network, every third party shall secure its own connected systems in a manner consistent with ECDHS requirements.

ECDHS reserve the right to audit the security measures in effect on these connected systems without prior warning. ECDHS also reserve the right to immediately terminate network connections with all third party systems not meeting such requirements.

Where third party suppliers provide support for an environment and telnet or FTP applications are required, strong authentication i.e. two factor authentication will be imposed on the Firewall when connecting to the device.

Unless ICT approval has been obtained, all ECDHS computers that are internet connected or directly reachable through the internet are prohibited from using shared directory systems, sometimes called shared file systems. These systems allow a user to obtain access to more than one computer's file system with only a single log-in process.

Exceptions are made for internet commerce and other systems where multiple machine architecture involves automatically passing users with severely restricted privileges from one computer to another.

All large networks crossing national or organisational boundaries shall have separately defined logical domains, each protected with suitable security perimeters and access control mechanisms.

The internal system addresses, configurations, and related system design information for ECDHS networked computer systems shall be restricted such that both systems and users outside ECDHS's internal network cannot access this information;

All secure network nodes, will be classified as having a high security risk to the systems and data of ECDHS. The security measures which are implemented to address the security exposures shall be capable of enforcing the level of security, (as defined by its classification) which is required within that environment. The integrity of these nodes will be monitored on a daily basis. All changes made to secure network nodes should be verified by change control, that the correct change control procedures were followed;

Except as otherwise specifically provided, employees may not intercept or disclose, or assist in intercepting or disclosing, electronic communications.

Unless ICT approval has been obtained in advance, employees are prohibited from using new or existing internet connections to establish new business channels. These channels include EDI arrangements, electronic malls with on-line shopping, on-line database services, etc.

3.15.6 Compliance

GISO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.

Failure to comply with this policy may result in disciplinary action, which may include termination of employment.

Any conduct that interferes with the normal and proper operation of the departments IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved IT policies.

The department management reserves the right to revoke the privileges of any user at any time.

3.16 OUTSOURCING POLICY

3.16.1 Introduction

Outsourcing involves transferring responsibility for carrying out an activity (previously carried out internally) to an outsourcer for an agreed charge. The outsourcer provides services to the customer based on a mutually agreed service level, normally defined in a formal contract.

Many commercial benefits have been ascribed to outsourcing, the most common amongst these being:

- reducing the organization's costs;
- greater focus on core business by outsourcing non-core functions; and
- access to world-class skills and resources.

Despite the potential benefits, information security incidents such as inappropriate access to or disclosure of sensitive information, loss of intellectual property protection or the inability of the outsourcer to live up to agreed service levels, would reduce the benefits and could jeopardize the security position of the department.

3.16.2 Purpose

The purpose of this policy is to ensure that the need to manage services that are outsourced to external service provided is complied with. The department should be aware that, although the services can be outsourced to a third party service provider, it generally cannot outsource responsibility.

Whenever IT services are outsourced to an external department, the onus is on the ECDHS to ensure that the service provider adheres to the department's security policy and standards.

3.16.3 Scope

The policy applies to all business units within the ECDHS that has outsourced or is seeking to outsource any services to an external service provider.

Outsourcing providers (also known as outsourcers or service providers) include:

- hardware and software support and maintenance staff;
- external consultants and contractors;
- IT or business process outsourcing firms; and
- temporary staff.

The policy addresses the following controls found in the ISO/IEC 27002:2013 and ISO/IEC 27001:2013 standards.

- (a) 15.1.1 Information security policy for supplier relationships
- (b) 15.1.2 Addressing security within supplier agreements
- (c) 15.1.3 ICT Supply chain

3.16.4 Roles and responsibilities

To conduct operations as effectively and efficiently as possible, the ECDHS may find it advantageous to outsource (use outside contractors for) certain functions. To ensure compliance with security objectives, these requirements must be followed.

3.16.4.1 The HoD

- is responsible for ensuring that adequate risk mitigation practices are in place for the effective oversight and management of outsourcing arrangements.

The HoD working in conjunction with the CFO shall be responsible for ensuring the effective implementation and compliance of the ECDHS policies, standards and procedures.

3.16.4.2 The risk management committee

The risk management committee should:

- develop a risk management framework for outsourcing arrangements that reflects the HoD-approved policy;
- approve all outsourcing arrangements of material business activities;
- review and approve risk management policies for outsourcing, including ensuring that an appropriate exit strategy is in place;
- regularly review compliance with the outsourcing policy; and
- regularly review reports on outsourcing arrangements and be informed of the performance of the service provider.

In managing the outsourcing arrangement, senior management should:

- be involved in the due diligence process, evaluation and selection of potential service providers;
- establish and implement an oversight process that ensures that outsourcing arrangements, and outsourcing of material business activities in particular, are reported to the risk management committee and HoD for the service prior to implementation;
- ensure that, for each outsourcing arrangement, there is a formal evaluation of the service provider, that a contract with appropriate SLAs is in place, and that confidentiality provisions and security needs are adequately addressed; and
- ensure that appropriate reporting is in place to enable effective management and control of outsourcing arrangements and to identify potential problems at an early stage.

3.16.4.3 Outsourced business process owners

Designated owners of outsourced business processes are responsible for assessing and managing the commercial and security risks associated with outsourcing, working in conjunction with Information Security, Legal and other functions as necessary.

3.16.4.4 Information security officer

Information Security, in conjunction with functions such as legal, compliance and risk management, is responsible for assisting outsourced business process owners to analyse the associated risks and develop appropriate process, technical, physical and legal controls.

ISO is also responsible for maintaining this policy.

3.16.4.5 Internal audit

The Internal Audit department is authorised by management to assess compliance with all corporate policies at any time.

The Internal Audit department may assist with audits of outsourcing contracts including security compliance audits, and advise management on the risks and controls relating to outsourcing.

3.16.5 Final approval

Decisions to outsource material business activities should be approved or endorsed by the HoD or delegated committee.

3.16.6 Policy statements

3.16.6.1 Choosing an outsourcer

Criteria for selecting an outsourcer shall be defined and documented, taking into account the:

- (a) company's reputation and history;
- (b) quality of services provided to other customers;
- (c) number and competence of staff and managers;
- (d) financial stability of the company and commercial record;
- (e) retention rates of the company's employees; and
- (f) quality assurance and security management standards currently followed by the company (e.g. certified compliance with MISS, PFMA and ISO/IEC 27001).

3.16.6.2 Risk mitigation strategies

- (a) ECDHS management shall nominate a suitable owner for each business function/process outsourced.
- (b) The owner - with the help of the risk management committee - shall perform risk assessments based on the department's risk assessment methodology prior to entering into the agreement with any outsourcing service provider.
- (c) ECDHS management shall consider establishing an outsourcing team comprising individuals from both the business area proposing the outsourcing arrangement and other individuals with the necessary skills to assess the risks involved in outsourcing. This may include specialists in the relevant risk areas and may involve using external experts.
- (d) Ensure that the HoD-approved policy on outsourcing is being followed at all times, including the due diligence processes, evaluating the outsourcing options and making recommendations to the risk management committee and the HoD.
- (e) Ensure that all applicable laws and regulations are complied with.
- (f) The result of the risk assessment shall be presented to management for approval prior to signing the outsourcing contract.
- (g) Management shall decide whether the department will benefit overall by outsourcing the function to the service provider, taking into account both the commercial and information security aspects. If the risks involved are high and the commercial benefits are marginal (e.g. if the controls necessary to manage the risks are too costly), the function shall not be outsourced.

In relation to outsourcing, specifically, the risk assessment shall take due account of the:

- nature of logical and physical access to information assets and facilities required by the service provider to fulfil the contract;
- sensitivity, volume and value of any information assets involved;
- commercial risks such as the possibility of the service providers business failing completely, or of them failing to meet agreed service levels; and

- security and commercial controls known to be currently employed by and/or by the service provider.

3.16.6.3 Business case

- A detailed business case should be prepared, detailing the potential costs, benefits and risks associated with the proposed outsourcing arrangement.
- As part of this process, the Board should be making an "in principle" decision to continue the outsourcing process and to call for RFPs or other selection process documents. The RFPs should clearly outline the requirements of department for the proposed outsourcing arrangement.

3.16.6.4 Due diligence

The due diligence process should always be undertaken prior to any final decision being made as to whether to outsource a material business activity. This should address all material factors that would impact on the potential service provider's ability to perform the business activity.

The due diligence process should, as a minimum, assess the financial ability, technical ability and capacity of the service provider to deliver, including in stress situations, the required services.

The evaluation process should include an assessment of the service provider's control framework, covering performance standards, policies, procedures, compliance, reporting and monitoring processes.

The due diligence should also address other issues, such as business strategy, reputation, experience with the proposed outsourced function, reliance on and performance of external service providers, insurance coverage, business BCM, and potential conflict of interest where the service provider is related to Organization XYZ or has arrangements with competitors.

3.16.6.5 Contractual and confidentiality agreements

- A formal (written and legally binding) contract between the department and the service provider shall exist to protect both parties. The contract shall clearly define the types of information exchanged and the purpose for doing so.
- If the information being exchanged is sensitive, a binding confidentiality agreement shall be in place between the department and the service provider, whether as part of the outsource contract itself or a separate non-disclosure agreement (which may be required before the main contract is negotiated).
- The agreement should be for a specified period and contain both start and finish dates. There should also be a clause allowing for periodic review of the agreement within the term of the contract and renegotiation if appropriate.
- The contract should specify the content, frequency and format of the service being provided. It should state timelines for receipt and delivery of work, including specifying priorities. It should contain performance benchmarks, including default benchmarks which, if not met, would result in penalties being applied or, in the extreme, termination of the agreement. The agreed service levels should be specified in SLAs.
- The circumstances that would lead to a termination of the outsourcing arrangement should be clearly specified in the contract. It should set out possible reasons for terminating the arrangement and procedures to be followed in the event of termination, including notice periods, the rights and responsibilities of the respective parties and transition arrangements. The latter would address access to, and ownership of, documents, records, software and hardware. Termination clauses should also specify the time period over which the business activity continues to be undertaken by the service provider and its role in transitional arrangements should the activity be brought back in-house within the department or outsourced to another service provider.
- The department shall ensure that there are appropriate information risk management clauses in the outsourcing contract.
- The department shall define and implement information risk management measures to protect the information within the business functions that have been outsourced to a third party to operate on a day-by-day basis.
- Legal, regulatory and other third party obligations such as data protection/privacy laws, money laundering.

- (i) Information security obligations and controls such as:
- information security policies, procedures, standards and guidelines, normally within the context of an Information Security Management System such as that defined in ISO/IEC 27001 and MISS;
 - background checks on employees or third parties working on the contract;
 - access controls to restrict unauthorized disclosure, modification or destruction of information, including physical and logical access controls, procedures for granting, reviewing, updating and revoking access to systems, data and facilities;
 - information security incident management procedures including mandatory incident reporting;
 - return or destruction of all information assets by the outsourcer after the completion of the outsourced activity or whenever the asset is no longer required to support the outsourced activity;
 - copyright, patents and similar protection for any intellectual property shared with the outsourcer or developed in the course of the contract;
 - specification, design, development, testing, implementation, configuration, management, maintenance, support and use of security controls within or associated with IT systems, plus source code escrow;
 - anti-malware, anti-spam and similar controls; and
 - IT change and configuration management, including vulnerability management, patching and verification of system security controls prior to their connection to production networks.

3.16.6.6 Hiring and training of employees

- (a) Outsource employees, contractors and consultants working on behalf of Department shall be subjected to background checks equivalent to those performed on Department's employees. Such screening shall take into consideration the level of trust and responsibility associated with the position and (where permitted by local laws):
- proof of the person's identity (e.g. passport);
 - proof of their academic qualifications (e.g. certificates);
 - proof of their work experience (e.g. résumé/CV and references);
 - criminal record check; and
 - credit check.
- (b) Companies providing contractors/consultants directly to Department or to service providers used by the department shall perform at least the same standard of background checks as those indicated above.
- (c) Suitable information security awareness, training and education shall be provided to all employees and third parties working on the contract, clarifying their responsibilities relating to the department information security policies, standards, procedures and guidelines (e.g. privacy policy, acceptable use policy, procedure for reporting information security incidents etc.) and all relevant obligations defined in the contract.
- (d) Outsourced employees also need to comply with acceptable use and behaviour policy, as well as all relevant personnel security policies.

3.16.6.7 Access controls

In order to prevent unauthorised access to the department's information assets by the service provider, suitable security controls are required as outlined in this section. The details depend on the nature of the information assets and the associated risks, implying the need to assess the risks and design suitable controls architecture.

3.16.6.8 Technical access controls

Technical access controls shall include:

- user identification and authentication;
- authorisation of access, generally through the assignment of users to defined user roles having appropriate logical access rights and controls;
- data encryption in accordance with the department's encryption policies and standards
- defining algorithms, key lengths, key management and escrow etc.; and
- accounting/audit logging of access checks, plus alarms/alerts for attempted access violations where applicable.

3.16.6.9 Procedural components of access controls

Shall be documented within procedures, guidelines and related documents and incorporated into awareness, training and educational activities. This includes:

- choice of strong passwords;
- determining and configuring appropriate logical access rights; and
- reviewing and, if necessary, revising access controls to maintain compliance with requirements.

3.16.6.10 Physical access controls

Physical access controls shall include:

- (a) layered controls covering perimeter and internal barriers;
- (b) strongly-constructed facilities;
- (c) suitable locks with key management procedures;
- (d) access logging through the use of automated key cards, visitor registers etc.; and
- (e) intruder alarms/alerts and response procedures.

3.16.6.11 Hosting

If parts of department's IT infrastructure is to be hosted at a third party data centre, the data centre operator shall ensure that the department's assets are both physically and logically isolated from other systems.

The department shall ensure that all information assets handed over to the service provider during the course of the contract (plus any copies made thereafter, including backups and archives) are duly retrieved or destroyed at the appropriate point on or before termination of the contract. In the case of highly classified information assets, this normally requires the use of a schedule or register and a process whereby the outsourcer formally accepts accountability for the assets at the point of hand-over.

3.16.7 Compliance

- (a) ISO and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.
- (b) Failure to comply with this policy may result in disciplinary action, which may include termination of employment.

3.17 CHANGE MANAGEMENT POLICY

3.17.1 Introduction

Change Management is the process of planning, coordinating, implementing and monitoring changes affecting any production platform within Information Technology's control. The objectives of the Change Management process are to:

- ensure that changes are made with minimum disruption to the services IT has committed to its users,
- support the efficient and prompt handling of all changes,
- provide accurate and timely information about all changes,
- ensure all changes are consistent with business and technical plans and strategies,
- ensure that a consistent approach is used,
- provide additional functionality and performance enhancements to systems while maintaining an acceptable level of user services,
- reduce the ratio of changes that need to be backed out of the system due to inadequate preparation,
- ensure that the required level of technical and management accountability is maintained for every change,
- monitor the number, reason, type, and associated risk of the changes.

3.17.2 Purpose

The purpose of the Change Management Policy is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of Information Resources.

The goal of change management process is to ensure that standardized methods and procedures are used for efficient and effective handling of all changes, in order to minimise the impact of change related incidents upon service quality, and to improve the day-to-day operation of the organization

3.17.3 Scope

ECDHS Change Management Policy applies to all individuals that install, operate or maintain information Resources within the department.

It includes the management of any installation or alteration to hardware, network, system or application software, procedure or environmental facilities which adds to, deletes from or modifies the service delivery environment.

3.17.4 Roles and responsibilities

3.17.4.1 The GITO

The GITO shall implement, enforce and monitor the controls in accordance with the requirements outlined by management, and shall advise users on the correct ways to access information and systems.

3.17.4.2 All employees

All employees are responsible for complying with this and other policy at all times. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of acceptable behaviour) to comply with ECDHS's policies.

3.17.4.3 Information systems owners

Responsible for analysing and form part of the committee approving all changes that affect the system they are responsible for.

3.17.4.4 Information security manager

The information security officer is responsible for maintaining this policy and generally advising on information security controls. Working in conjunction with other department functions, is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy.

3.17.4.5 Internal audit

The Internal Audit department is authorised by management to assess compliance with all department policies at any time.

3.17.5 Policy statements

- (a) every change to ECDHS Information Resources such as: operating systems, computing hardware, networks, and applications is subject to the Change Management Policy and shall be performed according to the Change Management Procedures;
- (b) the change management procedure shall ensure that proposed changes are reviewed for relevancy and impact (business, technical and financial);
- (c) Prior to any change being implemented there shall be a risk assessment that:
 - identifies significant changes;

- records significant changes;
 - assesses the potential impact of such changes; and
 - procedures and responsibilities for aborting and recovering from unsuccessful changes.
- (d) the change management procedure will be formally defined, documented and adhered to;
- (e) all changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) need to be reported to or coordinated with the leader of the change management process;
- (f) an ICT Change Management Committee, appointed by CIO, shall meet regularly to review change requests and to ensure that change reviews and communications are being satisfactorily performed;
- (g) A formal change control procedure shall be documented and enforced to govern application, computer installation, network and system development changes.
- (h) a formal written change request shall be submitted for all changes, both scheduled and unscheduled;
- (i) All business application changes with a financial impact shall be approved by the relevant system owner and the Financial Management. All infrastructure/ architectural changes shall be approved by the GITO.
- (j) all scheduled change requests shall be submitted in accordance with change management procedures so that the ICT Change Management Committee has time to review the request, determine and review potential failures, and make the decision to allow or delay the request;
- (k) each scheduled change request shall receive formal Change Management Committee approval before proceeding with the change;
- (l) the appointed leader of the Change Management Board may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back out plans, the timing of the change will negatively impact a key business process such as year-end accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events;
- (m) changes are to be fully tested in an isolated, controlled and representative environment, and approved before being implemented;
- (n) any software change and/or update will be controlled with version control;
- (o) Data to be tested for system changes should not be live data. If live data is required to test system changes, data should first be backed up, with adequate controls in place, and then sanitised before being used for testing.
- (p) data is to be protected against unauthorised or accidental changes;
- (q) fallback procedures for aborting and recovering from unsuccessful changes will be documented and tested;
- (r) emergency changes will be authorized and recorded;
- (s) disaster recovery plans will be updated with relevant changes and managed through the change control process;
- (t) information resources documentation will be updated when each change is complete and old documentation will be archived or disposed of according to the documentation and data retention policies;
- (u) customer notification shall be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedures;
- (v) a Change Review shall be completed for each change, whether scheduled or unscheduled, and whether successful or not;
- (w) a Change Management Log must be maintained for all changes. The log must contain, but is not limited to:
- Date of submission and date of change;
 - Owner and custodian contact information;
 - Nature of the change;
 - Indication of success or failure.
- (x) all ECDHS information systems shall comply with an Information Resources change management process that meets the standards outlined above;
- (y) the integrity of general use software, utilities, operating systems, networks, and respective data files are the responsibility of the custodian department. Data for test and research purposes shall be de-personalized prior to release to testers unless each individual involved in the testing has authorized access to the data;
- (z) all changes or modifications to Information systems, networks, programs or data shall be approved by the owner business unit that is responsible for their integrity.

3.17.6 Compliance

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of ECDHS Information Resources access privileges, civil, and criminal prosecution.

3.17.7 Definitions

Term	Definition
Change Management	The process of controlling modifications to hardware, software, firmware, and documentation to ensure that Information Resources are protected against improper modification before, during, and after system implementation.
Information Resource	Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.
Information Owner Policy	The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.
Policy	a high level, overall statement of intent embracing general principles and the steps that the ECDHS expects to be followed to achieve them
Standard	a specific prescribed or proscribed technical approach, solution, methodology, product or protocol which should be used in the design, development, implementation or upgrade of information technology systems architecture (e.g. hardware/software/services)
Procedure	a formal set of steps to follow in order to achieve a specific outcome, which are specifically agreed for designated staff. Any deviation from the step is acceptable if this can be justified and the rationale for doing so documented appropriately
Guideline	a systematically developed statement which assists in making decisions about appropriate actions for specific conditions. Guidelines are not intended to prescribe the detailed management of information technology management

3.18 SYSTEMS DEVELOPMENT POLICY

3.18.1 Introduction

Systems are the blood line of how organisations function to automate work and save cost and time in doing so. However, there are risks associated with implementing systems in an organisation without proper resource planning. The new system can be useful to the section of the business required in, but provide no integration possibilities with other core systems already in the organisation. Thus leading to a system that exists in isolation and can never be used to harvest business intelligence. Other risks include IP rights (Intellectual Property), which refers to who owns the source code that makes up the system software to allow the organisation to extend the functionality of the application and update in a later stage. This also has legislative consequences if not properly defined in a policy document of this nature and is later entrenched in an agreement with the developer if the solution is outsourced.

3.18.2 Purpose

The purpose of the System Development Policy is to describe the requirements for developing and/or implementing new software systems for Human Settlements.

3.18.3 Scope

This is a standard corporate policy that applies throughout the organisation as part of the corporate governance framework. It applies equally to all individuals who wish to develop new systems in the department. To the extent this policy conflicts with existing organisational policy, the existing policy is superseded by this policy.

3.18.4 Roles and responsibilities

3.18.4.1 The GITO

- (a) The GITO shall implement, enforce and monitor the controls in accordance with the requirements outlined by management, and must advise users on the correct ways to access information and systems.
- (b) Responsible for developing and maintaining the corporate software systems in accordance with this policy.
- (c) Responsible for assisting users with secure use of this systems, and acts as a focal point for managing all software applications deployed to the organisation.

3.18.4.2 All employees

All employees are responsible for complying with this and other corporate policies at all times. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of acceptable behaviour) to comply with our information security policies.

3.18.4.3 Systems development manager

The systems development manager is responsible for maintaining this policy and generally advising on systems development initiatives. Working in conjunction with other corporate functions, the manager is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy.

3.18.4.4 Internal audit

The internal audit must evaluate risk exposures relating to the Organization's governance, operations, and information systems regarding the:

- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations.
- Safeguarding of assets; and
- Compliance with laws, regulations, and contracts.

3.18.5 Policy statements

Department of Human Settlements is responsible for developing, maintaining, and participating in a System Development Life Cycle (SDLC) system development projects. All software developed in-house which runs on production systems must be developed according to the SDLC. At a minimum, this plan should address the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; general design; detail design; development; quality assurance and acceptance testing; implementation; and post-implementation maintenance and review. This methodology ensures that the software will be adequately documented and tested before it is used for critical departmental information.

A rollback strategy should be in place before changes are implemented.

All production systems must have designated Owners and Custodians for the critical information they

process. The department must perform annual risk assessments of production systems to determine whether the controls employed are adequate.

All production systems must have an access control system to restrict who can access the system as well as restrict the privileges available to these Users. A designated access control administrator (who is not a regular User on the system in question) must be assigned for all production systems.

Where resources permit, there should be a separation between the production, development, and test environments. This will ensure that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions. Where these distinctions have been established, development and test staff must not be permitted to have access to production systems. Likewise, all production software testing must utilize sanitized information.

All application-program-based access paths other than the formal user access paths must be deleted or disabled before software is moved into production.

Violations of this policy must be reported to the Manager: Systems Development Unit.

3.18.6 Compliance

Manager: Systems Development and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.

Failure to comply with this policy may result in disciplinary action, which may include termination of employment.

Any conduct that interferes with the normal and proper operation of the department's IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved IT policies.

The department management reserves the right to revoke the privileges of any user at any time.

3.19 DISASTER RECOVERY POLICY

3.19.1 Introduction

This document provides an overall policy that governs the nature and detail to which Disaster Recovery (DR) is deployed and used within the Information and Communications Technology (ICT) unit of ECDHS.

In the event of a major disaster the Information Systems controlled by ECDHS may become unavailable for an undetermined period. This poses a serious risk to the reputation and even the existence of ECDHS. Provision must therefore be made for an alternative Information System capability that will replace the effected system for a limited period of time, allowing ECDHS to carry on with its operations.

Disaster recovery can be defined as the simultaneous or separate taking over of one or more system, which has been disabled due to a major disaster, by an alternative system on another suitable site. This is executed against a confirmed and joint decision that the effected system will not be able to be repaired and continue its operations within a particular time limit.

The ICT DR Policy falls into, and should be read in conjunction with the wider ECDHS Business Continuity Management Policy which ensures ECDHS as a business will continue to deliver its key services should a disruption arises either in or out of normal office hours.

3.19.2 Purpose

This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by Eastern Cape Department of Human Settlements that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

3.19.3 Scope

This policy is directed to the ICT Management Staff who is accountable to ensure the plan is developed, tested and kept up-to-date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans. ICT DR responsibility

3.19.4 Roles and Responsibilities

To conduct operations as effectively and efficiently as possible and ensure the department can recover from a disastrous event. Clear roles and responsibilities have to be defined and communicated to the stakeholders. The following roles and responsibilities are required to ensure the DRP requirements are fulfilled:

The HoD

- a) The HoD is and remains responsible for the overall DRP. This responsibility is delegated to GITO.
- b) Ensures that resources are made available to plan, test and maintain the DRP.
- c) Receives reports on the status of the DRP testing

Asset/information/ application owner

The owner of the information resource shall ensure that contingency plan is developed to recover their service after a disaster. 1

Information Security Officer

Ensure that security is being considered when developing, implementing and testing the DRP.

Internal Audit unit

- a) Internal Audit is authorized by management to assess compliance with all corporate policies at any time.
- b) Internal Audit may assist with audits of the DRP including testing and maintenance of the plan.

Policy ownership

The HoD is and remains responsible for the overall disaster recovery policy.

- b) It is the responsibility of the business units to ensure that they have enough information in their specific section of the Continuity Plan, to enable them to recover from an incident and continue to provide a service to clients within acceptable timeframes.

3.19.5 Contingency Plans

The following contingency plans must be created:

- Computer Emergency Response Plan: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?
- Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.
- Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.
- Criticality of Service List: List all the services provided and their order of importance.
- It also explains the order of recovery in both short-term and long-term timeframes.
- Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.
- Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.
- Mass Media Management: Who is in charge of giving information to the mass media?
- Also provide some guidelines on what data is appropriate to be provided.

3.19.6 Policy Statements

- The department must have an approved comprehensive DR Plan in place to ensure that it can recover all critical IT and Information Systems in the event of a disaster
- The DR Plan must be periodically tested at pre-determined dates (at least once a year) or on adhoc basis to ensure that it can be implemented in an emergency situation, and that management and staff understands what is required for execution
- The DR Plan must cover all essential and critical business activities which relate to its daily operations. In the event of a disaster, it must be possible for the Department to continue operating even at limited capacity
- The DRP must be kept up to date to take into account any relevant change within the department's IT and information systems environment
- Staff members must be made aware of the DR Plan and their specific roles (if applicable) defined within the plan. Business unit managers shall ensure that all employees comply fully with all the requirements of this disaster recovery policy
- After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Table top exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.
- The plan, at a minimum, should be reviewed and updated on an annual basis.

3.19.7 Compliance

The Information Security Officer and senior management are required to ensure that internal audit mechanisms exist to monitor and measure ICT compliance with this Policy.

Any conduct that interferes with the normal and proper operation of the departments ICT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved IT policies. Failure to comply with this policy may result in disciplinary action, which may include termination of employment. *Refer, User Awareness Policy.*

3.20 Patch Management Policy

3.20.1 Overview

Regular application of vendor-issued critical security updates and patches are necessary to protect ECDHS data and systems from malicious attacks and erroneous function. All electronic devices connected to the network including servers, workstations, firewalls, network switches and routers, tablets, mobile devices, and cellular devices routinely require patching for functional and secure operations.

3.20.2 Purpose

Software is critical to the delivery of services to ECDHS customers and ECDHS users. This policy provides the basis for an ongoing and consistent system and application update policy that stresses regular security updates and patches to operating systems, firmware, productivity applications, and utilities. Regular updates are critical to maintaining a secure operational environment.

3.20.3 Scope

This policy applies to all ECDHS staff create, deploy, or support application and system software.

3.20.4 GENERAL

All system components and software shall be protected from known vulnerabilities by installing applicable vendor supplied security patches. System components and devices attached to the ECDHS network shall be regularly maintained by applying critical security patches within thirty (30) days after release by the vendor. Other patches not designated as critical by the vendor shall be applied on a normal maintenance schedule as defined by normal systems maintenance and support operating procedures.

3.20.5 Systems, Utility and Application Patching

A regular schedule shall be developed for security patching of all ECDHS systems and devices. Patching shall include updates to all operating systems as well as office productivity software, data base software, third party applications (e.g. Flash, Shockwave, etc.), and mobile devices under the direct management of ECDHS [Insert Applicable Department].

Most vendors have automated patching procedures for their individual applications. There are a number of third party tools to assist in the patching process and the ECDHS should make use of appropriate management software to support this process across the many different platforms and devices the ECDHS [Insert Applicable Department] supports. The regular application of critical security patches is reviewed as part of normal change management and audit procedures.

3.20.6 Patching Exceptions

Patches on production systems (e.g. servers and enterprise applications) may require complex testing and installation procedures. In certain cases, risk mitigation rather than patching may be preferable. The risk mitigation alternative selected should be determined through an outage risk to exposure comparison. The reason for any departure from the above standard and alternative protection measures taken shall be documented in writing for devices storing non-public data. Deviations from normal patch schedules shall require ICT: Director's authorization.

3.20.7 Security Patching Procedures

Policies and procedures shall be established and implemented for vulnerability and patch management. The process shall ensure that application, system, and network device vulnerabilities are:

- Evaluated regularly and responded to in a timely fashion
- Documented and well understood by support staff
- Automated and regularly monitored wherever possible
- Executed in a manner applicable vendor-supplied tools on a regularly communicated schedule
- Applied in a timely and orderly manner based on criticality and applicability of patches and enhancements

3.20.8 Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the ECDHS internal systems change management and update procedures. Examples of adequate controls include:

- System updates and patch logs for all major system and utility categories
- Logs should include system ID, date patched, patch status, exception, and reason for exception
- Demonstrated infrastructure supporting enterprise patch management across systems, applications, and devices

3.20.9 Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

3.20.10 Distribution

This policy is to be distributed to all ECDHS staff responsible for support and management

3.21 PRIVACY POLICY

3.21.1 Introduction

The intention to publish the Privacy Policy is not to impose restrictions that are contrary to the ECDHS established culture, openness, trust and integrity. ECDHS is committed to protecting your privacy. This Privacy Policy explains how personal information of internal/external stakeholders/individuals is collected, used, and disclosed through electronic communication channels/systems/platforms.

By accessing or using our services, internal/external stakeholders/individuals signify that they have read, understood, and agree to our collection, storage, use, and disclosure of personal information as described in this Privacy Policy and our Terms of Service including relevant government legislations.

3.21.2 Purpose

The purpose of this policy is to outline the privacy provisions for safeguarding/protecting the privacy of any personal information and information system within the ECDHS.

The objectives of this policy are to:

- (a) mitigate against legal liability by setting boundaries for appropriate employee conduct when using electronic communications facilities;
- (c) ensure that internal/external stakeholders/individuals understand how their personal information provided to ECDHS would be used
- (d) comply with all relevant regulatory and legislative requirements such as the Protection of Personal Information Act (POPI Act), **EU's General Data Protection Regulation (GDPR)** and other relevant legislations both in South African and International on data privacy law.

3.21.3 Scope

This is a standard departmental policy that applies to all personal information provided/collected from internal/external stakeholders/individuals through the department's electronic communication channels or platforms or information and technology systems.

3.21.4 Roles and responsibilities

3.21.4.1 The GITO

The GITO shall implement, enforce and monitor the controls in accordance with the requirements outlined by management, and must advise users on the correct ways to access information and systems.

3.21.4.2 All employees

All employees are responsible for complying with this and other corporate policies at all times. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of privacy behaviour) to comply with our information security policies and this privacy policy.

3.21.4.3 Information security officer

Information Security Officer is responsible for maintaining this policy and advising generally on information security controls. Working in conjunction with other corporate functions, it is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy.

Information officer:

The POPI Act stipulates the following general responsibilities:

- to encourage compliance with POPI
- dealing with requests made to the organisation in relation to POPI (for instance, requests from Data Subjects to update or view their personal information)
- working with the Regulator in relation to investigations
- otherwise ensuring compliance with POPI

3.21.4.4 Internal audit

Internal Audit is authorised by management to assess compliance with all corporate policies at any time.

3.21.5 Policy statements

How does ECDHS use the personal information we collect or provided?

Any of the personal information we provided/collected from internal/external stakeholders/individuals may be used in one of the following ways:

- i) To personalize the user/individuals' experience (information helps us to better respond to the individual needs)
- ii) To improve our electronic communication channels/systems/platforms (we continually strive to improve our offerings based on the information and feedback we receive)
- iii) To improve customer service (the information helps us to more effectively respond to customer service requests and support needs)
- iv) To process transactions according to our various business processes in line with relevant legislations.
- v) To administer a contest, promotion, survey or other electronic communication channels/ systems/ platforms feature(s)
- vi) To send periodic emails or other relevant electronic communication or notifications.

When does Departmental electronic communication channels/systems/platforms use end user/customer personal information from third parties?

The Departmental electronic communication channels/systems/platforms collector allows for the submission of End User Data necessary to provide the ECDHS relevant services to our customers.

End-users (internal/external stakeholders/individuals) may voluntarily provide us with information they have made available on social media or other digital platforms. If such information is available, we may collect such publicly available personal information from the social media websites or other digital platforms individuals have indicated. You can control how much of your information social media websites make public by visiting these websites and changing your privacy settings.

We may receive some information from the third parties when end-users/customers contact us. For example, when submit their email address to us to show interest in Departmental programmes or services, we receive information from a third party (including Public Sector or Private sector entities) that provides automated fraud detection services or such external service for data validation/verification.

We may also occasionally collect personal information that is made publicly available on social media or other digital platforms should that be required as part of our services offerings or programmes. End-users can control how much of their personal information is available on social media or digital platforms by visiting these such platforms and changing their privacy settings.

(a) Do we share the information we collect with third parties?

We may share the information that we collect, both personal and non-personal, with third parties such as advertisers, contest sponsors, promotional and marketing partners, and others who provide our content or whose products or services we think may interest our end-users should that be part/complementing our service offerings or programmes. We may also share it with our current and future affiliated companies, business partners, and other Public Sector entities and if we are involved in a merger, asset sale or other Government Department reorganization, we may also share or transfer end-user's personal and non-personal information to our successors-in-interest.

We may engage trusted third-party service providers (in both public and private sector) to perform functions and provide services to us, such as hosting and maintaining our servers and the website, database storage and management, e-mail management, storage marketing, credit card processing, customer service and fulfilling orders for products and services end-users/customers may purchase through the digital platforms. We will likely share end-users/customers personal information, and possibly some non-personal information, with these third parties to enable them to perform these services on half of ECDHS.

We may share portions of our log file data, including IP addresses, for analytics purposes with third parties such as web analytics partners, application developers, and ad networks. If end-users/customers IP address is shared, it may be used to estimate general location and other technographics such as connection speed, whether end-users/customers have visited the ECDHS digital channels/platforms in a shared location, and type of the device used to visit the digital channel/platform. They may aggregate information about our advertising and what end-users/customers see on the digital channels/platforms and then provide auditing, research and

reporting for us and our advertisers/stakeholders.

We may also disclose personal and non-personal information about end-users/customers to government or law enforcement officials or private parties as we, in our sole discretion, believe necessary or appropriate in order to respond to claims, legal process (including subpoenas), to protect ECDHS rights and interests or those of a third party, the safety of the public or any person, to prevent or stop any illegal, unethical, or legally actionable activity, or to otherwise comply with applicable court orders, laws, rules and regulations.

(b) Where and when is information collected from customers and end users?

Departmental digital channels/platforms may collect personal information that you submit to us. We may also receive personal information about end-users/customers from third parties as described above.

(c) How do we use end-users/customers email addresses?

By submitting email address on ECDHS digital channels/platforms, internal/external stakeholders/individuals agree to receive emails or notifications from ECDHS. End-users/customers can cancel their participation in any of these email lists at any time by clicking on the opt-out link or other unsubscribe option that is included in the respective email. We only send emails to people who have authorized us to contact them, either directly, or through a third party. We do not send unsolicited commercial emails or spam emails.

By submitting any email address, end-users/customers also agree to allow us to use their email address for customer audience targeting on digital/social sites like Facebook/Twitter, where we display custom advertising to specific people who have opted-in to receive communications from ECDHS. Email addresses submitted only through the order processing page will be used for the sole purpose of sending end-users/customers information and updates pertaining to their order/service offerings/programmes. If, however, internal/external stakeholders/individuals have provided the same email to us through another method, we may use it for any of the purposes stated in this Policy. Note: If at any time end-users/customers would like to unsubscribe from receiving future emails/notifications, we include detailed unsubscribe instructions at the bottom of each email.

(d) How long do we keep end-users/customers personal information?

We keep end-users/customers personal information only so long as we need it to provide Departmental service offerings/programmes to end-users/customers and fulfil the purposes described in this policy. This is also the case for anyone (both in the public and private sectors) that we share end-users/customers information with and who carries out services on our behalf.

When we no longer need to use end-users/customers information and there is no need for us to keep it to comply with our legal or regulatory obligations, we'll either remove it from our systems/digital channels/platforms or depersonalize it so that we can't identify an end-user/customer.

(e) How do we protect end-users/customers information?

We implement a variety of security measures to maintain the safety of your personal information when you place an order or enter, submit, or access your personal information. We offer the use of a secure server. All supplied sensitive/credit information would be transmitted via Secure Socket Layer (SSL) technology and then encrypted into our Payment gateway providers database only to be accessible by those authorized with special access rights to such systems/digital channels/platforms, and are required to keep the information confidential.

After a transaction, private information (credit cards, social security numbers, financials, etc.) is never kept on file. We cannot, however, ensure or warrant the absolute security of any information transmit to Departmental digital channels/platforms or guarantee that information on the Service may not be accessed, disclosed, altered, or destroyed by a breach of any of our physical, technical, or managerial safeguards.

(f) Could end-users/customers information be transferred to other countries?

ECDHS digital channels/platforms is Provincial Govern Department in South Africa, Eastern Cape Province. Information collected via our digital channels/platforms, through direct interactions with end-users/customers, or from use of our help services may be transferred from time to time to our offices or personnel, or to third parties, located throughout the world, and may be viewed and hosted anywhere in the world, including countries that may not have laws of general applicability regulating the use and transfer of such data.

To the fullest extent allowed by applicable law, by using any of the above, end-users/customers voluntarily consent to the trans-border transfer and hosting of such information.

(g) Is the information collected through the ECDHS digital channels/platforms service secure?

We take precautions to protect the security of internal/external stakeholders'/individuals' information. We have physical, electronic, and managerial procedures to help safeguard, prevent unauthorized access, maintain data security, and correctly use end-users/customers information. However, neither people nor security systems are fool proof, including encryption systems. In addition, people can commit intentional crimes, make mistakes or fail to follow policies. Therefore, while we use reasonable efforts to protect end-users/customers personal information, we cannot guarantee its absolute security. If applicable law imposes any non-disclaimable duty to protect end-users/customers personal information, end-users/customers agree that intentional misconduct will be the standards used to measure our compliance with that duty.

(h) Can end-users/customers update or correct their information?

The rights end-users/customers have for requesting updates or corrections to the information Departmental digital channels/platforms/systems collects depend on their relationship with ECDHS. Personnel may update or correct their information as detailed in our internal Departmental employment policies and other applicable legislations.

Customers/end-users have the right to request the restriction of certain uses and disclosures of personally identifiable information as follows. Customers/end-users can contact ECDHS in order to:

- (1) update or correct their personally identifiable information,
- (2) change their preferences with respect to communications and other information internal/external stakeholders/individuals receive from ECDHS, or
- (3) delete the personally identifiable information maintained about them on ECDHS digital channels/platforms/systems (subject to the following paragraph), by cancelling their account/subscription where applicable. Such updates, corrections, changes and deletions will have no effect on other information that ECDHS maintain, or information that we have provided to third parties in accordance with this Privacy Policy prior to such update, correction, change or deletion. To protect their privacy and security, we may take reasonable steps (such as requesting a unique password) to verify their identity before granting end-users/customers profile access or making corrections. End-users/customers are responsible for always maintaining the secrecy of their unique password and account information where applicable.

End-users/customers should be aware that it is not technologically possible to remove each and every record of the information they have provided to us from our digital channels/platforms/systems. The need to back up our systems to protect information from inadvertent loss means that a copy of end-users/customers information may exist in a non-erasable form that will be difficult or impossible for us to locate. Promptly after receiving their request, all personal information stored in databases we actively use, and other readily searchable media will be updated, corrected, changed or deleted, as appropriate, as soon as and to the extent reasonably and technically practicable.

(i) Personnel

With regards to Departmental internal worker or applicant, we collect information they voluntarily provide to us. We use the information collected for Human Resources purposes in order to administer benefits to workers and screen applicants.

Internal/external stakeholders/individuals/applicants may contact us in order to:

- (1) update or correct their information,
- (2) change their preferences with respect to communications and other information they receive from us, or
- (3) receive a record of the information we have relating to them. Such updates, corrections, changes and deletions will have no effect on other information that we maintain, or information that we have provided to third parties in accordance with this Privacy Policy prior to such update, correction, change or deletion.

(j) Governing Law

This Privacy Policy is governed by the laws of South Africa without regard to its conflict of laws provision.

Internal/external stakeholders/individuals/applications consent to the exclusive jurisdiction of the courts in connection with any action or dispute arising between the parties under or in connection with this Privacy Policy except for those individuals who may have rights to make claims under Privacy Shield, or the Swiss-US framework.

The laws of South Africa, excluding its conflicts of law rules, shall govern this policy and end-users/customers use of the ECDHS digital channels/platforms/systems. The use of the ECDHS digital channels/platforms/systems may also be subject to other local, state, national, or international laws.

By using ECDHS digital channels/platforms/systems or contacting us directly, end-users/customers signify their acceptance of this Privacy Policy. If end-users/customers do not agree to this Privacy Policy, they should not engage with our digital channels/platforms/systems or use our services. Continued use of the ECDHS digital channels/platforms/systems, direct engagement with us, or following the posting of changes to this Privacy Policy that do not significantly affect the use or disclosure of end-users/customers personal information will mean that they accept those changes.

(k) End-users/customers Consent

We've updated our Privacy Policy to provide you with complete transparency into what is being set when you visit our site and how it's being used. By using our website, registering an account, or making a purchase, you hereby consent to our Privacy Policy and agree to its terms.

Links to Other Websites

This Privacy Policy applies only to the Services. The Services may contain links to other websites not operated or controlled by Departmental Website. We are not responsible for the content, accuracy or opinions expressed in such websites, and such websites are not investigated, monitored or checked for accuracy or completeness by us. Please remember that when you use a link to go from the Services to another website, our Privacy Policy is no longer in effect. Your browsing and interaction on any other website, including those that have a link on our platform, is subject to that website's own rules and policies. Such third parties may use their own cookies or other methods to collect information about you.

Cookies

Departmental Website uses "Cookies" to identify the areas of our website that you have visited. A Cookie is a small piece of data stored on your computer or mobile device by your web browser. We use Cookies to enhance the performance and functionality of our website but are non-essential to their use. However, without these cookies, certain functionality like videos may become unavailable or you would be required to enter your login details every time you visit the website as we would not be able to remember that you had logged in previously. Most web browsers can be set to disable the use of Cookies. However, if you disable Cookies, you may not be able to access functionality on our website correctly or at all. We never place Personally Identifiable Information in Cookies.

Blocking and disabling cookies and similar technologies

Wherever you're located you may also set your browser to block cookies and similar technologies, but this action may block our essential cookies and prevent our website from functioning properly, and you may not be able to fully utilize all of its features and services. You should also be aware that you may also lose some saved information (e.g. saved login details, site preferences) if you block cookies on your browser. Different browsers make different controls available to you. Disabling a cookie or category of cookie does not delete the cookie from your browser, you will need to do this yourself from within your browser, you should visit your browser's help menu for more information.

Changes To Our Privacy Policy

We may change our Service and policies, and we may need to make changes to this Privacy Policy so that they accurately reflect our Service and policies. Unless otherwise required by law, we will notify you (for example, through our Service) before we make changes to this Privacy Policy and give you an opportunity to review them before they go into effect. Then, if you continue to use the Service, you will be bound by the updated Privacy Policy. If you do not want to agree to this or any updated Privacy Policy, you can delete your account.

Third-Party Services

We may display, include or make available third-party content (including data, information, applications and other products services) or provide links to third-party websites or services ("Third- Party Services").

You acknowledge and agree that Departmental Website shall not be responsible for any Third-Party Services, including their accuracy, completeness, timeliness, validity, copyright compliance, legality, decency, quality or any other aspect thereof. Departmental Website does not assume and shall not have any liability or responsibility to you or any other person or entity for any Third-Party Services.

Third-Party Services and links thereto are provided solely as a convenience to you and you access and use them entirely at your own risk and subject to such third parties' terms and conditions.

Tracking Technologies

- Google Maps API

Google Maps API is a robust tool that can be used to create a custom map, a searchable map, check-in functions, display live data synching with location, plan routes, or create a mashup just to name a few.

Google Maps API may collect information from You and from Your Device for security purposes.

Google Maps API collects information that is held in accordance with its Privacy Policy

- Local Storage

Local Storage sometimes known as DOM storage, provides web apps with methods and protocols for storing client-side data. Web storage supports persistent data storage, similar to cookies but with a greatly enhanced capacity and no information stored in the HTTP request header.

- Sessions

Departmental Website uses "Sessions" to identify the areas of our website that you have visited. A Session is a small piece of data stored on your computer or mobile device by your web browser.

What is personal data?

Any data that relates to an identifiable or identified individual. GDPR covers a broad spectrum of information that could be used on its own, or in combination with other pieces of information, to identify a person. Personal data extends beyond a person's name or email address. Some examples include financial information, political opinions, genetic data, biometric data, IP addresses, physical address, and ethnicity.

The Data Protection Principles include requirements such as:

- Personal data collected must be processed in a fair, legal, and transparent way and should only be used in a way that a person would reasonably expect.
- Personal data should only be collected to fulfil a specific purpose and it should only be used for that purpose. Organizations must specify why they need the personal data when they collect it.
- Personal data should be held no longer than necessary to fulfil its purpose.
- People covered by the GDPR have the right to access their own personal data. They can also request a copy of their data, and that their data be updated, deleted, restricted, or moved to another organization.

Individual Data Subject's Rights - Data Access, Portability and Deletion

We are committed to helping our customers meet the data subject rights requirements of GDPR. Departmental Website processes or stores all personal data in fully vetted, DPA compliant vendors. We do store all conversation and personal data for up to 6 years unless your account is deleted. In which case, we dispose of all data in accordance with our Terms of Service and Privacy Policy, but we will not hold it longer than 60 days.

We are aware that if you are working with EU customers, you need to be able to provide them with the ability to access, update, retrieve and remove personal data. We got you! We've been set up as self service from the start and have always given you access to your data and your customers data. Our customer support team is here for you to answer any questions you might have about working with the API.

Contact Us

Don't hesitate to contact us if you have any questions.

- Via Email: administrator@ecdhs.gov.za
- Via Phone Number: 043 711 9999
- Via this Link: <https://www.ecdhs.gov.za/>
- Via this Address: 31-33 Phillip Frame Road, Waverly Park, Chiselhurst, East London, Eastern Cape, REPUBLIC OF SOUTH AFRICA



RECORDS MANAGEMENT POLICY

Definitions

Act:

The Provincial Archives and Records Service Act No. 7 of 2003

Appraisal

The archival function of determining the eventual disposal of records

Archives

Records in the custody of an archive's repository

Archival Value

Those value, administrative, fiscal, legal, evidential and/or informational, which justify the indefinite or permanent retention of records

Archives repository:

The building in which records with archival value are preserved permanently.

Authentic records:

Authentic records are records that can be proven to be what they purport to be. They are also records that are considered by the creators to be their official record.

Authoritative records:

Authoritative records are records that are authentic, reliable, trustworthy and useable and are complete and unaltered.

Case file:

The most detailed (or specific) division in a file plan that create a separate file for each person, place, institution or item. etc.

Closed Volume:

1. Volumes of records in a current paper-based file plan that have reached a thickness of 3cm or have become full, after which a new volume has been opened.
2. In an electronic system a folder which was segmented into parts.

Classified information:

Classification given to information that may be used by hostile / opposing / malicious elements to disrupt the objectives and functions of an institution and / or state.

Confidential information:

Should be limited to information that may be used by hostile / opposing / malicious elements to harm the objectives and functions of an individual and / or institution

Correspondence system:

A set of paper-based and electronic communications and associated documents, sent, received, generated, processed and stored during the conduct of business.

Custody:

The control of records based upon their physical possession.

Current records

Records that form part of a records classification system still in use.

Disposal:

The action of either destroying/deleting a record or transferring it into archival custody.

Disposal authority:

A written authority issued by the National / Provincial Archivist specifying which records should be transferred into archival custody or specifying which records should be destroyed/deleted or otherwise disposed of.

Disposal authority number:

A unique number identifying each disposal authority issued to a specific office.

Disposal instruction

The specific instruction regarding disposal allocated to each record e.g. D for delete/destroy and A for transferring into archival custody

Electronic Document Management System:

A system that provides the ability to capture, describe and categorise, store and retrieve, share and reuse electronic documents regardless of specific format.

Electronic records:

Information which is generated electronically and stored by means of computer technology. Electronic records can consist of an electronic correspondence system and electronic record systems other than the correspondence system.

Electronic records system:

This is the collective noun for all components of an electronic information system, namely: electronic media as well as all connected items such as source documents, output information, software applications, programmes and metadata (background and technical information i.r.o. the information stored electronically) and in hard copy. All these components are defined as records by the Act. They must therefore be dealt with in accordance with the Act's provisions.

File plan:

A pre-determined classification plan by which records are filed and/or electronically indexed to facilitate efficient retrieval and disposal of records.

File reference

A unique identifier for a file. This can be a numerical, alphanumerical or alphabetical identifier. It is used to link a record to its specific subject file and subject grouping.

Filing system:

The collective noun for a storage system (like files, boxes, shelves or electronic applications and storage systems) in which records are stored in a systematic manner according to a file plan.

Folder:

1. An organized arrangement of records on the same subject accumulated in chronological order within the same cover/ container.

2. A physical action of allocating file reference numbers to records and placing them inside the cover/ container.

Functional subject file plan:

A pre-determined logical, systematic and hierarchical structure based on business' function that then used to determine subject groups and subject according to which records are filed and/or electronically indexed. Its purpose to

1. Facilitate efficient retrieval and disposal of records; and
2. To link the records back to the functions, activities and transactions that generated them.

Governmental body:

Any legislative, executive, judicial or administrative organ of state (including a statutory body) at the national level of government and until provincial archival legislation takes effect also all provincial administrations and local authorities.

Head of governmental body:

The chief executive officer of a governmental body or person who is acting as such.

Integrated Document Management and Records Management

A set of methods and technologies consisting of messaging & calendaring, imaging & scanning, file/document tracking, electronic document management, electronic records management, workflow and search & retrieval functionalities used to manage the classification, location, movement, security, auditing. Retention and disposal of an organization's records regardless of format.

Non-archival records:

Records with a short lived interest or usefulness.

Public record:

A record created or received by a governmental body in pursuance of its activities, regardless of form or medium.

Records other than correspondence systems:

Records that do not form part of a correspondence file, or a case file e.g. registers, maps, plans, electronic records, audio-visual records, etc.

Record:

- 1) Recorded information regardless of form or medium.
- 2) Evidence of a transaction preserved for the evidential information it contains.

Records classification system:

A plan for the systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules represented in the classification system.

Recording:

Anything on which sounds or images or both are fixed or from which sounds or images or both are capable of being reproduced, regardless of form.

Records other than correspondence systems:

Records do not form part of a correspondence file, or a case file e.g. registers, maps, plans, electronic records, audio-visual records, etc.

Record keeping:

Making and maintaining complete, accurate and reliable evidence of official business in the form of recorded information.

Records management

Records management is a process of ensuring the proper creation, maintenance, use and disposal of records throughout their life cycle to achieve efficient, transparent and accountable governance.

Retention period:

1. The length of time that records should be retained in offices before they are either transferred into archival custody or destroyed/deleted.
2. In an electronic document management system, the length of time a record is kept online before it is moved to near-line or off-line storage in a hierarchical storage management systems.

Schedule for records other than correspondence systems:

A control mechanism for records other than correspondence files (other records), which contains a description and the disposal instructions and retention periods of all other records. It consists of the following parts:

- Schedule for paper-based records other than correspondence files;
- Schedule for electronic records systems other than the electronic correspondence system;
- Schedule for microfilm records;
- Schedule for audio-visual records.

Scheduled Records

Records that have been issued with a written disposal authority and are due for disposal on a specific date

Secret information:

Classification given to information that may be used by hostile / opposing / malicious elements to disrupt the objectives and functions of an institution and / or state.

System technical manual:

A manual containing information regarding the hardware, software and network elements that comprise the system and how they interact. Details of all changes to a system should also be documented.

System procedures manual:

A manual containing all procedures relating to the operation and use of the electronic system, including input to, operation of and output from the system. A system procedures manual would contain detailed procedures regarding -

- Document capture
- Document scanning
- Data capture
- Indexing
- Authenticated output procedures
- File transmission
- Information retention
- Information destruction

- Backup and system recovery
- System maintenance
- Security and protection
- Use of contracted services
- Workflow
- Date and time stamps
- Version control
- Maintenance of documentation

A systems procedures manual should be updated when new releases force new procedures.

Terminated Records

Records which were created or received by a governmental body and which were managed by a records classification system no longer in use.

Unscheduled Records

Records that have not yet been issued with a written disposal authority and that can thus not be disposed of

Vital/Essential Records

- 1) Records that protect the enduring civil, legal, financial, property and other rights of the citizens of a country
- 2) Records that are needed to continue operational responsibilities under disaster conditions;
- 3) Records that protect the legal and financial rights of the Government.

Top Secret information:

Classification given to information that can be used by enemies or hostile / opposing / malicious elements to neutralize the objectives and functions of institutions and / or state.

Transitory records:

Transitory records are those records created by officials but not required by the governmental bodies for which they work to control, support or document the delivery of services, or to carry out operations, to make decisions, or give account of the activities of government. Such records are needed by official for only a limited time to facilitate the completion of routine actions or to prepare a subsequent record requires by a government body for the above-mentioned reasons.

Purpose

- 1.1 Section 13 of the National Archives and Records Service of South Africa Act, 1996 requires the Department of Human Settlements to manage its records in a well-structured record keeping system, and to put the necessary policies and procedures in place to ensure that its record keeping and records management practices comply with the requirements of the Act.
- 1.2 Information is a resource of the same importance to good management as other standard resources like people, money and facilities. The information resources of Human Settlements Department must therefore be managed as a valuable asset. Appropriate records management is a vital aspect of maintaining and enhancing the value of this asset. Human Settlements Department considers its records to be a valuable asset to:
 - enable the department to find the right information easily and comprehensively.
 - enable the department to perform its functions successfully and efficiently and in an accountable manner.
 - support the business, legal and accountability requirements of the department.
 - ensure the conduct of business in an orderly, efficient and accountable manner.
 - ensure the consistent delivery of services.
 - support and document policy formation and administrative decision-making;
 - provide continuity in the event of a disaster;
 - protect the interests of the department and the rights of employees, clients and present and future stakeholders;
 - support and document the department's activities, development and achievements;
- 1.3 Records management, through the proper control of the content, storage and volume of records, reduces vulnerability to legal challenge or financial loss and promotes best value in terms of human and space resources through greater co-ordination of information and storage systems.

2 Policy statement

- 2.1 All records created and received by Human Settlements Department shall be managed in accordance with the records management principles contained in section 13 of the National Archives and Records Service Act, 1996.
- 2.2 The following broad principles apply to the record keeping and records management practices of Human Settlements Department:
 - follows sound procedures for the creation, maintenance, retention and disposal of all records, including electronic records.
 - The records management procedures of the department comply with legal requirements, including those for the provision of evidence.
 - follows sound procedures for the security, privacy and confidentiality of its records.
 - Electronic records in the department are managed according to the principles promoted by the National Archives and Records Service.
 - Has performance measures for all records management functions and reviews compliance with these measures.

3. Relationship with other policies

- 3.1 Human Settlements Department's Records Management Policy consist of this policy as well as additional parts that cover the unique nature of the broad spectrum of records generated by the department. These policies are managed by the records manager. The following parts exist:
 - a) ICT Policy managed by Director: GICTM (Government Information Communication and Technology Management).
 - b) The Security Management Policy which is managed by the Security Manager

Where contradictions are to be perceived between the Records Management Policy and other Policies, the Records Management Policy shall take precedence in all application and interpretation.

- 3.2 Other policies that are closely related to the Records Management Policy are
- a. Promotion of Access to Information Policy which is managed by the Information Officer in terms of PAIA, the empowering provision.
 - b. Protection of Personal Information Act

4. Scope and intended audience

This policy impacts upon all staff members (including Interns and Contract workers) of Department of Human Settlements who:

- create records including electronic records;
- have access to records;
- have any other responsibilities for records, for example storage and maintenance responsibilities;
- Have management responsibility for staff engaged in any of these activities; or manage, or have design input into, information technology infrastructure.

5. Regulatory framework

- 5.1 By managing its paper-based records effectively and efficiently Department of Human Settlements strives to give effect to the accountability, transparency and service delivery values contained in the legal framework established by:

- **Constitution, 1996**

Section 195 of the Constitution provides amongst other of the:

- Effective, economical, and efficient use of resources;
- Provision of timely, accessible and accurate information; and requires that
- The public administration must be accountable.

- National Archives and Records Service of South Africa Act (Act No 43 of 1996 as amended);

- Section 13 of Act contains specific provisions for efficient records management in governmental bodies. It provides for the National Archivist-
- To determine which records keeping systems should be used governmental bodies;
- To authorise the disposal of public records or their transfer into archival custody; and
- To determine the conditions-
 - According to which records may be microfilmed or electronically reproduced;
 - According to which electronic records systems should be managed.

- **National Archives and Records Service of South Africa Regulations;**
- Public Finance Management Act (Act No 1 of 1999);

The purpose of the act is to regulate financial management in the government and to prevent corruption.

Efficient records management practices are imperative if a body want to give effect to the provisions of this act.

- **Promotion of Access to Information Act (Act No 2 of 2000);**

The Act gives effect to the access to information right in the 1996 Constitution, section 32. The purpose of the Act is to promote transparency, accountability and effective governance by empowering and educating the public

1. To understand and exercise their rights;
2. To understand the functions and operation of public bodies; and
3. To effectively scrutinise, and participate in, decision-making by public bodies that affect their rights.

As far as the Promotion of Access to Information Act is concerned, the definition of a record is similar to that in the National Archives and Records Service Act, namely "recorded information regardless of form or medium". Governmental bodies cannot refuse access on grounds that a record is in an electronic form (including an e-mail). This implies that an electronic record (including an e-mails) like any other record should be managed in such a manner that it is available, accessible, and rich

in contextual information. By implication electronic records (including e-mails) should be managed in proper record keeping systems and the disposal of electronic records (including e-mails) should be documented and executed with the necessary authority.

- **Promotion of Administrative Justice Act (Act No 3 of 2000);**

The purpose of this Act is to ensure that administrative action is lawful, reasonable and fair and properly documented.

To enable governmental bodies to comply with the provisions of this Act, they would keep proper records of administrative actions and decisions.

The Promotion of administration Justice Act imposes a duty on the state to ensure that administrative action is lawful, reasonable and procedurally fair; and everyone whose rights have been adversely affected by administrative action has a right to be given written reasons for such an action. A person who is of the opinion that his/her rights have been materially and adversely affected by administrative action may request that he/she be provided with reasons for such an action. If an administrator to whom a request was made fails to furnish adequate reasons for administrative action, because the history of that action was documented in e-mail messages or records that were destroyed, it could be presumed that the administrative action was taken without good reason. The administrator then runs the risk of legal action being taken against him/her or his/her organisation. Relating this back to the management of records – authorised destruction of records (including e-mail) could be considered a deliberate action to conceal the reasons for administrative actions. Any destruction of public records should be done in accordance with a written disposal authority issued by the National Archives and Records Services or its provincial equivalents. Governmental bodies should do a risk assessment to determine the risk of not managing their records (including e-mail) properly against the risk of being held accountable for unreasonable administrative actions.

- **Electronic Communications and Transactions Act (Act No 25 of 2002)**

The purpose of the Act is to legalize electronic communications and transactions, and to build trust in electronic records. To provide for the facilitation and regulation of electronic communications and transactions.

According to the Electronic Communications and Transactions Act data messages are legally admissible records, provided that their authenticity and reliability as true evidence of a transaction can be proven beyond any doubt. The evidential weight of the electronic records (including e-mails) would depend amongst others on the reliability of the manner in which the messages were managed by the originator and the receiver. Should bodies not have a properly enforced records management and e-mail policy and reliable and secure record keeping system, they run the risk that the evidential weight of their electronic records (including e-mails) might be diminished.

Besides the above-mentioned acts, several laws compel governmental bodies to manage information and records so that they are readily available and accessible when needed. The legislation and standards mentioned laws that applies to specific governance clusters and governmental bodies and although not mentioned specifically these should also be kept in mind when reading this document.

- **Protection of Personal Information Act, Act 4 of 2013**
- **Minimum Information Security Standards (MISS)**
- **Minimum Physical Security Standards (MPSS)**
- **Regulation of interception of communication and provision of communication-related information Act 70 of 2002**



RECORDS MANAGEMENT POLICY

Introduction

Records are the output of the business and administrative processes of Government. The need for effective management of records is enhanced by the Public Finance Management Act, 1999, The Promotion of Access of Information Act, 2000, POPIA Act 4 of 2013, and the Electronic Communication and Transactions Act, 2000 to provide access contained in records, provide reasons for administrative decisions and ensure the authenticity of records.

Records management is a process of ensuring the proper creation, maintenance, use and disposal of records through their life cycle to achieve efficient, transparent and accountable department.

3.1.4 Roles and responsibilities

Head of Department duties and responsibilities

- 6.1.1 According to the Records Management Policy, Part V (10)(1), states that The Head of Department shall be responsible for ensuring that all records of the Department of Human Settlements
 - (a) receive appropriate physical care
 - (b) are protected by appropriate security measures: and
 - (c) are managed in terms of standing orders of that body and other relevant legislation
- 6.1.2 The Head of Department is committed to enhance accountability, transparency and improvement of service delivery by ensuring that sound records management practices are implemented and maintained.
- 6.1.2 The Head of Department supports the implementation of this policy and requires each staff member to support the values underlying in this policy.
- 6.1.3 In terms of section 13(5) of the National Archives Act, Act 43 of 1996 the Head of Department shall appoint the Records Manager in accordance with section 12 of the National Archives Regulations R1458 of 2002.
- 6.1.4 In terms of section 32 of Promotion of Administrative Justice Act, The Head of Department shall emphasize why it is paramount that records are captured accurately and kept secure in case requested even by external stakeholders.
- 6.1.5 In terms of section 15 of PAIA, the Head of Department shall allow voluntary disclosure and automatic availability of certain records.
- 6.1.6 In terms of the Minimum Information Security Standards, 1996 (MISS), the Accounting Officer or his delegate should ensure the overall security (i.e. physical and information security) of the Department of Human Settlements and therefore should:
 - 6.1.6.1 Develop and implement a Security Plan and Security Policy within the Department of Human Settlements.
 - 6.1.6.2 Ensure that all employees have undergone security screening Investigation and ensure that all employees are re-vetted every 5 years in cases of Secret and Top Secret clearances and 10 years in the case of confidential clearances.

6.2 National or Provincial Archivist

- 6.2.1 In terms of Section 13(2)(b) of the National Archives Act, Act 43 Of 1996, the Provincial Archivist shall valuate, approve and monitor the implementation of the approved record classification system.
- 6.2.2 The Provincial Archivist must issue and approve disposal authorities and approve destruction and transfer of records
- 6.2.3 The Provincial Archivist must conduct Records Management inspection at the Department Human Settlements and for such inspection the Head of Department must grant access to the Provincial Archivist to Records to be inspected to ensure compliance and proper Records Management.
- 6.2.4 The Provincial Archivist must appraise Records and issue disposal authorities thereof.
- 6.2.5 The Provincial Archivist must provide training in Archival techniques and Management of Records in terms of section 5(2)(a) of the National Archives Act, Act 43 of 1996.
- 6.2.6 The Provincial Archivist should determine the conditions subject to which electronic records systems should be managed.
- 6.2.7 The Provincial Archivist must collect, arrange, describe and preserve A20 or records that have endure value or A20 in the archives repository in terms of section 11 of the National Archives Act, Act 43 of 1996.
- 6.2.8 The Provincial Archivist must make the Records accessible for consultation by the researchers or

users in terms of section 12 of the National Archives Act, Act 43 of 1996.

- 6.2.9 The Provincial Archivist must conduct Public outreach or awareness programmes in terms of section 5(1) (c) of the National Archives Act, Act 43 of 1996
- 6.2.10 In terms of section 14(1) of the National Archives Act, Act 43 of 1996 the Provincial Archivist may acquire by purchase or donation or on loan for a temporary period or in perpetuity, either unconditionally of subject to such conditions as may be agreed upon, non-public records which, in his or her opinion, have enduring value of national significance and which cannot be more appropriately preserved by another institution.
- 6.2.11 In terms of Act No. 4 of 2013 or POPI Act, POPIA stands for the Protection of Personal Information Act, the purpose of the Protection of Personal Information Act (POPIA) is to protect people from harm by protecting their personal information. Much of the Personal Information that is kept is in the form of documents or records. Managing these correctly is imperative under POPIA.

6.3 Records Manager

6.3.1 File Plans:

A structured classification scheme should be developed so that records can be easily identified, stored, retrieved and managed. This should be designed to cater for records on all formats and in all locations. This is essential if records are to be managed correctly in terms of POPIA.

The records manager is responsible for the overall control over the compilation, implementation, maintenance and utilization of approved file plans and the records file according to these systems. During the compilation of a new file plan the records manager should liaise with the Provincial Archives and Records Service for assistance and advice during the process. Once the file plan has been compiled, the records manager should submit it to the Provincial and National Archivist for approval. The records manager should keep a master copy of the file plan updated to always reflect the functions of the body. The records manager must ensure that the approved file plan is maintained and that all additions and amendments are reported to the Provincial Archivist. As the functions and activities of a body develop, a similar development should occur in the file plan. The records manager should ensure that changes in the file plan are reflected in the physical files and in the electronic system if the body is using an electronic system.

The records manager should ensure that the registry staff is trained in the allocation of reference numbers and in file plan maintenance procedures. The records manager should also ensure that all the users of the system are trained to allocate reference numbers to correspondence, to ensure that records are not misplaced. Supervisions over the implementation and maintenance of the filing system (the storage system for records) must be ensured. The correct placement of documentation should be monitored and particular attention should be paid to policy, archival, routine enquiry and parent files in both the paper-based and the electronic system to ensure that they are used correctly.

6.3.2 Schedule of records other than correspondence systems:

The records manager is responsible for the overall control over the compilation, maintenance and utilization of the approved schedules for records other than correspondence systems as well as the records themselves.

The records manager must ensure that the schedule for other records systems is compiled and submitted in duplicate to the Provincial Archivist for the issuing of a disposal authority. The records manager should ensure that the master copy of the schedule is maintained and updated and must ensure that all revisions and additions are reported to the Provincial Archivist, to facilitate the issuing of a disposal authority for the records.

The records manager should ensure that the disposal authority is applied at least once a year to ensure that archival records are transferred into archival custody and that non-archival records no longer needed are destroyed. The records manager should also ensure that all staff is aware of the penalty for the unauthorized destruction or mismanagement of records.

6.3.3 Destruction of records:

A disposal programme needs to be implemented and then rigidly followed. It is highly risky under POPIA to keep records and not destroy them when their purpose is finished. This does of course apply to all records and shouldn't be limited to Personal Information records.

A key element of disposal is to ensure that duplicates are also destroyed as they are also Personal Information. A process of identifying and removing duplicates should be adopted. Duplicates could be in paper or electronic formats. The destruction of non-archival records must occur in the presence of the records manager. He/she must before destroying non-archival records ensure that:

- No work is outstanding
- No litigation or investigation is being conducted which concerns the records in question
- The records have not been requested in terms of the Promotion of Access to Information Act or the Promotion of Administrative Justice Act.

The records manager must also ensure that destruction of archival records do not occur.

Records managers must ensure that all destruction actions are properly documented. They must submit destruction certificates to the Provincial Archivist once records have been destroyed and ensure that the body keeps a record of all destruction actions taken regarding records.

See Annexure 1

6.3.4 Transfer of records:

The records manager should supervise the transfer of the archival records to an appropriate archives repository when the time is right. The records manager must inform the Provincial Archivist in writing when records are permanently transferred to another governmental body. A complete list of the records should also be submitted to the Provincial Archivist.

The records manager must ensure that no public records are transferred to off-site storage facilities without the permission of the Provincial Archives and Records Service. The records manager, in conjunction with Provincial Archives and Records Service's Records Management Division, should inspect the off-site storage facility before any records are transferred into its custody. The records manager should inspect the facility regularly after transfers have taken place. The records manager should notify the Provincial Archivist when such inspections are planned and should submit copies of the inspection reports to the Provincial Archivist. The records manager should ensure that the off-site storage facility is familiar with the requirements of the Provincial Archives and Records Service Act before records are transferred into its custody.

See Annexure 2

6.3.5 Records in all formats:

The records manager is responsible for ensuring the safe custody and storage of all records in all formats.

The records manager should conduct regular inspections in the individual components to ensure that their records management practices conform to the standards promulgated in the Act. Copies of these reports should be submitted to the Provincial Archivist. The records manager should liaise with the IT manager to share information regarding the proper storage of electronic records and should be involved in the regular maintenance of records stored on electronic storage media. He/she should ensure that regular inspections are done and that the results of these inspections are also reported to the Provincial Archives and Records Service.

Buildings and storage areas should be regularly monitored in order to maintain a stable, protective environment for records. The records manager should develop a programme whereby the building, temperature, humidity, air quality, and light in storage areas are monitored, pests are controlled, fire protection and safety equipment are checked, and the presence of magnetic fields is monitored. The records manager should also inspect the records themselves to monitor for signs of deterioration.

The records manager should ensure that a proper disaster management programme is in place and communicated throughout the organization.

The records manager should ensure that all staff are aware of the importance of security in the building and records storage areas.

6.3.6 Training:

The records manager is responsible to implement and manage a suitable training programme for managers, employees, contractors and records management staff. He/she should supervise the training of staff regarding records management matters and regularly evaluate the success of the training programme against the effectiveness of the records management programme.

The records manager should ensure that records management consultants and suppliers of electronic records management and related products employed by the governmental body are familiar with the requirements of the national Archives and Records Service Act.

Every registry in a governmental body should have a registry procedure manual to facilitate the training of registry staff.

The records manager is responsible for ensuring that the registry head is trained and has attended the Provincial Archives and Records Service's Records Management Course. He/she should ensure that the registry head and registry staff are aware of and adhere to the standards, procedures and methods of records management promulgated in the National Archives and Records Service of South Africa Act.

The records manager is responsible to ensure that all staff members are made aware of their joint responsibility in maintaining sound records management practices. He/she should conduct awareness campaigns in this regard.

The records manager should arrange with the Provincial Archives and Records Service's Records management Division to conduct implementation workshops whenever new file plans are implemented to ensure that all members of staff know how to read and use the file plan.

6.3.8 Status of the Records Manager in the organization:

The following criteria should be applied regarding the positioning of the Records Manager in the organization:

- The official should occupy a relatively central position in the organization
- The official should occupy a senior enough position to ensure ready liaison with division heads and senior management
- The official should be able to make responsible decisions concerning all aspects of records management practices and implement them to the highest level in the office.
- It is therefore undesirable for the Registry Head and the Records manager to be one and the same person.
- Where an office has sub-offices or comprises several departments or divisions, a Records Manager should be appointed for each component. These officials should be answerable to a Records Manager for the body, i.e. an overall Records manager for the body as a whole. (No need for this)

6.3.9. Non-delegatable duties of the Records Manager:

To prevent the delegation of authority the following non-delegatable duties should be assigned to the Records Manager and the following duties should be reflected on the official's duty sheet:

- Control over the maintenance and application of the filing system and Records Control Schedule
- Disposal of all records
- Safe custody of all records
- Control over staff in the registry, and
- Application of policy of document economy.

The specific duties assigned to the Records manager flow from the foregoing.

6.3.10 Records Classification Systems:

- i) Ensure that the filing systems, Records Control Schedules and classification systems for electronic systems of all components the body is submitted to the Provincial Archivist for approval.
 - Compilation of new Records Classification Systems
 - Keeping Master Copies
 - Maintenance of filing system

- i) Disposal Authority
- ii) Transfer of records to appropriate archives repository or records centre's
- iii) Destruction Certificates by the Provincial Archives
- iv) Inspection by Officials of the Provincial Archives
- v) Surveys by Officials of the Provincial Archives
- vi) Inspections by the Records manager
- vii) Physical Care
- viii) Registry Procedure Manuals
- ix) Training and Selection of Staff

6.4 Chief Information Officer being the Head of Department

- 6.4.1 The Chief Information Officer is responsible for approval of requests for information in terms of the Promotion of Access to Information Act.
- 6.4.2 The Chief Information Officer shall inform the records manager if a request for information necessitates a disposal hold to be placed on records that are due for disposal.

6.5 IT Manager

- 6.5.1 The IT manager is responsible for the day-to-day maintenance of electronic systems that stores records.
- 6.5.2 The IT manager shall work in conjunction with the records manager to ensure that public records are properly managed, protected and appropriately preserved for as long as they are required for business, legal and long-term preservation purposes.
- 6.5.3 The IT manager shall ensure that appropriate systems technical manuals and systems procedures manuals are designed for each electronic system that manages and stores records.
- 6.5.4 The IT manager shall ensure that all electronic systems capture appropriate systems generated metadata and audit trail data for all electronic records to ensure that authentic and reliable records are created.
- 6.5.5 The IT manager shall ensure that electronic records in all electronic systems remains accessible by migrating them to new hardware and software platforms when there is a danger of technology obsolescence including media and format obsolescence.
- 6.5.6 The IT manager shall ensure that all data, metadata, audit trail data, operating systems and application software are backed up on a daily, weekly and monthly basis to enable the recovery of authentic, reliable and accessible records should a disaster occur.
- 6.5.7 The IT manager shall ensure that back-ups are stored in a secure off-site environment.
- 6.5.8 The IT manager shall ensure that systems that manage and store records are virus free.
- 6.5.9 Comprehensive details regarding specific responsibilities of the IT Manager are contained in (check with IT)
 - the E-mail policy;
 - Information security policy.

6.6 Security manager

- 6.6.1 The security manager is responsible for the physical security of all records.
- 6.6.2 Details regarding the specific responsibilities of the security manager are contained in the information security policy.
- 6.6.3 Minimum Information Security Standards, 1996 requires that Employees or applicants and Service Providers who/that will have access to classified information intelligence in the possessions of the Department of Human Settlements should undergo security screening investigations or security screening to determine the security competence of the employee.

6.7 Legal services manager

The legal services manager is responsible for keeping the Records Manager updated about developments in the legal and statutory environment that may impact on the record keeping and records management practices of Human Settlements Department.

6.8 Chief Registry Clerk

The following tasks are entrusted to the Registry Head and should be recorded in the job description:

- Opening of files and replacement of worn covers
- Responsible for noting the correct reference number on all incoming correspondence and other material
- Responsible for the correct and neat filing of all material
- Keeps control over the filing to prevent unnecessary duplicates of bulky items being placed on the files
- Responsible for the custody of keeping of:
 - A register of files opened

- A destruction register and
- A register of authorities
- Responsible for all amendments/additions being brought to the notice of interested parties
- Responsible for the closure of records
- Controls the receipt and opening of post
- The recording of moneys and valuable documents that are received in the remittance register
- The tracing of files
- The despatch of outgoing items
- The pending of correspondence
- The training of registry personnel.

6.9 Employees

- 6.9.1 Every employee member shall create records of transactions while conducting official business.
- 6.9.2 Every employee member shall manage those records efficiently and effectively by:
- allocating reference numbers and subjects to paper-based and electronic records according to the file plan.
 - sending paper-based records to the registry for filing.
 - Ensuring that records are destroyed/deleted only in accordance with the written disposal authority issued by the Provincial Archivist via the Records Manager.
- 6.9.3 Records management responsibilities shall be written into the performance agreements of all staff members to ensure that staff is evaluated on their records management responsibilities.

7. Records classification systems and related storage areas

Human Settlements Department has the following systems that organize and store records:

7.1 Correspondence systems

7.1.1 File plan

Records Management Policy, Part.V(11) 1-3 states that:-

- (1) No governmental body shall use a records classification unless it has been approved by the Provincial Archivist.
- (2) Any application for the approval of a records classification system shall follow procedures determined by the Provincial Archivist
- (3) Any revision of and additions to an approved records classification system shall be submitted to the Provincial Archivist for approval in accordance with procedures set out by the National Archivist Act 13(2)6

7.1.1.1 Only the file plan approved and implemented shall be used for the classification of correspondence records. The file plan shall be used for the classification of paper-based and electronic (including e-mail) records.

7.1.1.2 Each staff member shall allocate file reference numbers to all correspondence (paper, electronic, e-mail) according to the approved subjects in the file plan.

7.1.1.3 When correspondence is created/received for which no subject exists in the file plan, the records manager should be contacted to assist with additions to the file plan. Under no circumstances may subjects be added to the file plan if they have not been approved by the records manager.

7.1.2 Storage areas

7.1.2.1 Paper-based correspondence files are kept in the custody of-

7.1.2.1.1 The central registry

7.1.2.1.1.1 All paper-based correspondence system records that are not HR related are housed in the central registry.

7.1.2.1.1.2 All these records are under the management of the records manager who is mandated to ensure that they are managed properly.

7.1.2.1.1.3 The registry is a secure storage area and only registry staff is allowed in the records storage area.

7.1.2.1.1.4 Staff members that need access to files in the registry shall place a request for the files at the counter.

7.1.2.1.1.5 The registry shall be locked when registry is not in operation.

7.1.2.1.2 The Human Resources registry

7.1.2.1.2.1 All Human Resources related records are housed in the HR Registry.

7.1.2.1.2.2 The general HR subject files as well as HR case files are under the management of the records manager who is mandated to ensure that they are managed properly.

7.1.2.1.2.3 The Department of Human Settlements maintains a set of paper-based case files for each staff member. These files are confidential in nature and are housed in a secure storage area in the HR registry.

7.1.2.1.2.4 The case files are managed as part of the List of Series of Separate Case Files that is maintained and managed by the records manager.

7.1.2.1.2.5 The files exist only in paper-based format and the physical tracking of the case files are

- managed with the file tracking system in the Integrated Document and Records Management System
- 7.1.2.2 Electronic correspondence records are stored in an electronic repository that is maintained by the IT section.
- 7.1.2.2.1 Access to storage areas where electronic records are stored is limited to the Information Technology staff that has specific duties regarding the Maintenance of the hardware, software and media.

7.2 Records other than correspondence systems

7.2.1 Schedule for records other than correspondence systems

- 7.2.1.1 The records manager maintains a schedule of all records other than the correspondence system. The schedule contains a description of each set of records other than the correspondence system and indicates the storage location and retention periods of these records regardless of format.
- 7.2.1.2 Should records be created/received that are not listed in the schedule, the records manager should be contacted to add the records to the schedule.

7.2.2 Storage areas

- 7.2.2.1 Paper-based
- 7.2.2.1.1 Department of Human Settlements has sets of paper-based records other than the correspondence systems that are in the custody of the various officials that use them on a daily basis.
- 7.2.2.1.2 These records are under the control of the records manager who is mandated to ensure that they are managed properly.
- 7.2.2.2 Micrographic records
- 7.2.2.2.1 Department of Human Settlements has sets of microfilmed records that are stored in the IT section.
- 7.2.2.2.2 These records are under the control of the records manager who is mandated to ensure that they are managed properly.
- 7.2.2.3 Audio-visual records
- 7.2.2.3.1 Department Human Settlements has sets of audio-visual records that are stored in the IT section.
- 7.2.2.4 Electronic systems other than the correspondence systems
- 7.2.2.4.1 Department of Human Settlements has a number of electronic records systems in operation which is not part of the correspondence system and that generate and store public records.
- 7.2.2.4.2 The IT manager is responsible for the day-to-day maintenance of these systems.
- 7.2.2.4.3 The records maintained in these systems are under the control of the records manager who is mandated to ensure that they are managed properly.

Management of Classified information in terms of MISS

- 7.2.3.1 All sensitive information must be categorized into one of the following categories:
- State Secret
 - Trade Secret
 - Personal Information
-
- And subsequently classified according to its level of sensitivity by using one of the recognized levels of classification:
- Confidential
 - Secret
 - Top Secret
- 7.2.3.2 Employees of Human Settlements who generates sensitive information are responsible for determining information classification levels and the classification thereof, subject to management review. This responsibility includes the labeling of classified documents.
- 7.2.3.3 Registry personnel do not deal with secret or confidential documents on their daily duties. (check with security)
- 7.2.3.4 The classification assigned to documents must be strictly adhered to and the prescribed security measures to protect such documents must be applied at all times. Classification levels assigned to information should strictly be observed and may not be changed without the consent of the Accounting Officer or his delegate.
- 7.2.3.5 Access to classified information will be determined by the following principles:
- Intrinsic secrecy approach
 - Need-to-know principle
 - Level of security clearance

Classified Information should be stored in following manner:

Confidential Documents should be store in a reinforced filing cabinet; Secret Documents should be stored in a safe of strong room (walk-in-Safe), and Top Secret Documents should be stored in a safe or strong room (walk-in-safe)

8. Disposal of records (Regulation Part V (10)(5))

- 8.1 No public records (including e-mail) shall be destroyed, erased or otherwise disposed of without prior written authorization from the Provincial Archivist.
- 8.2 The Provincial Archivist shall issue Standing Disposal Authority Number for the disposal of records classified against the file plan. The records manager manages the disposal schedule. (To be obtained, after approval) Reg Part V (10)(6)
- 8.3 The Provincial Archivist issue Standing Disposal Authority Number on the schedule of records other than correspondence systems. The records manager manages the disposal schedule.
- 8.4 Retention periods indicated on the file plan and schedule will be determined by taking the Department of Human Settlements legal obligations and functional needs into account. Should a staff member disagree with the allocated retention periods, the records manager should be contacted to discuss a more appropriate retention period.
- 8.5 Disposal in terms of these disposal authorities will be executed annually in December.
- 8.6 All disposal actions should be authorized by the records manager prior to their execution to ensure that archival records are not destroyed inadvertently.
- 8.7 Non-archival records that are needed for litigation, Promotion of Access to Information requests or Promotion of Administrative Justice actions may not be destroyed until such time that the Manager: Legal Services has indicated that the destruction hold can be lifted.
- 8.8 Paper-based archival records shall be safely kept until they are due to transfer to the Provincial Archives Repository. Transfer procedures shall be as prescribed by the National Archives in the Records Management Policy Manual.
- 8.8 Specific guidelines regarding the procedure to dispose of electronic records are contained in the electronic records management policy.

9. Storage and custody

- 9.1 See par. 7 for an identification of all record keeping systems and their storage locations.
- 9.2 All records shall be kept in storage areas that are appropriate for the type of medium. The National Archives and Records Services' guidelines contained in the Records Management Policy Manual shall be applied.

10. Access and security

- 10.1 Records shall at all times be protected against unauthorized access and tampering to protect their authenticity and reliability as evidence of the business of the Department of Human Settlements.
- 10.2 Security classified records shall be managed in terms of the Information Security Policy which is available from the security manager.
- 10.3 No staff member shall remove records that are not available in the public domain from the premises of the Department of Human Settlements without the explicit permission of the records manager in consultation with the information security manager.
- 10.4 No staff member shall provide information and records that are not in the public domain to the public without consulting the Chief Information Officer. Specific guidelines regarding requests for information are contained in the Promotion of Access to Information Policy which is maintained by the Chief Information Officer.
- 10.5 Personal information shall be managed in terms of the Promotion of Access to Information Act and Promotion of Access to Information
- 10.6 No staff member shall disclose personal information of any member of staff or client of Human Settlements Department to any member of the public without consulting the Chief Information Officer first.
- 10.7 An audit trail shall be logged of all attempts to alter/edit electronic records and their metadata.
- 10.8 Records storage areas shall at all times be protected against unauthorized access. The following shall apply:
 - 10.8.1 Registry and other records storage areas shall be locked when not in use.
 - 10.8.2 Access to server rooms and storage areas for electronic records media shall be managed with access control.

11. Legal admissibility and evidential weight

- 11.1 The records of Human Settlements Department shall at all times contain reliable evidence of business operations. The following shall apply:
 - 11.1.1 Paper-based records
 - 11.1.1.1 No records shall be removed from paper-based files without the explicit permission of the records manager.
 - 11.1.1.2 Records that were placed on files shall not be altered in any way.
 - 11.1.1.3 No alterations of any kind shall be made to records other than correspondence files without

- 11.1.1.4 the explicit permission of the records manager.
Should evidence be obtained of tampering with records, the staff member involved shall be subject to disciplinary action.

12. Training

- 12.1 The records manager shall successfully complete the Provincial Archives and Records Service's Records Management Course, as well as any other records management training that would equip him/her for his/her duties.
- 12.2 The records manager shall identify such training courses that are relevant to the duties of the registry staff and shall ensure that the registry staff is trained appropriately.
- 12.3 The records manager shall ensure that all staff members are aware of the records management policies and shall conduct or arrange such training as is necessary for the staff to equip them for their records management duties.

13. Monitor and review

- 13.1 The records manager shall review the record keeping and records management practices of the Department of Human Settlements on a regular basis and shall adapt them appropriately to ensure that they meet the business and service delivery requirements of Human Settlements Department.
- 13.2 This policy shall be reviewed on a regular basis and shall be adapted appropriately to ensure that it meets the business and service delivery requirements of Human Settlements Department.

Annexure 1

LIST OF TERMINATED CORRESPONDENCE FILES / RECORDS

Programme in which the files were used:

Period covered by the files:(year) to (year)

Number of boxes to be disposed

Official to be contacted in connection with proposed disposal instructions:

Name:

Office:

Tel:

Email address:

FILE NUMBER	DESCRIPTION	PERIOD DISPOSAL

Annexure 2

LIST OF TRANSFER OF RECORDS

Name of office:

Year of the files:(year)

Number of boxes transferring

Official to be contacted in connection with proposed transfer of records/ documents:

Name:
.....

Office:

Tel:

Email address:

NO. OF BOXES	FILE NUMBER	DESCRIPTION	PERIOD IN YEARS	PROPOSED DISPOSAL