Province of the
EASTERN CAPE
COOPERATIVE GOVERNANCE
& TRADITIONAL AFFAIRS

INFORMATION COMMUNICATION AND TECHNOLOGY DATA BACKUP AND RECOVERY POLICY AND PROCEDURES

Departmental Contact Details	
Physical Address	**Tyamzashe Building** **Phalo Avenue** **Bhisho** **5605**
Postal Address	**Department of Cooperative Governance and Traditional Affairs** **Private Bag X0035** **Bhisho** **5605**
Document Number	**1**
Document Name	**ICT Data Backup and Recovery Policy**
Custodian	**Ms T.M. Luke**
Designation	**Director: Information Management Services**
Component	**DGITO**
Telephone No.	**040 940 7235**
Cell Phone No.	**076 141 1749**
E-mail Address	**tswakai.luke@eccogta.gov.za**
Date Completed	**16 February 2022**
Date of Approval	
Date Last Amended	
Date For Next Review	**February 2027**
Related Policies	**ICT Acceptable Use Policy**

SIGN OFF

Head of Department

This Policy has been recommended by Mr. AA Fani in my capacity as Head of Department of Department Cooperative Governance and Traditional Affairs.

I am satisfied and concur with the contents of this Policy.

The development of the policy on ICT Data Backup and Recovery Policy to preserve the data and information of the department even for use in future purposes.

Signed	
Designation	Mr. A.A Fani, Head of Department: Cooperative Governance and Traditional Affairs
Date	07/03/2022

Executive Authority

The Department of Cooperative Governance and Traditional Affairs has an unprecedented opportunity to improve the livelihoods of the people by effectively rendering the many services that it is expected to provide. We have envisaged a Department that has the required capacity to respond adequately to challenges of its people.

I therefore trust that guidance from this ICT Data Backup and Recovery Policy will contribute to the effective utilisation of the policy by the staff of the Department.

Signed	
Designation	MEC: Honourable XE Nqatha of Cooperative Governance and Traditional Affairs
Date	10/03/2022

1. CONTENTS

1. PREAMBLE 6
2. PURPOSE OF POLICY 6
3. DEFINITIONS 6
4. APPLICATION AND SCOPE 7
5. LEGISLATIVE FRAMEWORK 7
6. CONSULTATION PROCESS WITH STAKEHOLDERS 8
7. POLICY STATEMENT 8
8. DATA BACKUP AND RECOVERY STANDARDS 8
9 DATA BACKUP SELECTION 9
10 BACKUP TYPES 9
11 BACKUP SCHEDULE 10
12 DATA BACKUP PROCEDURES 10
13 STORAGE MEDIUM 11
14. DATA BACKUP OWNER 11
15. OFFSITE STORAGE SITE 12
16. TRANSPORT MODES 12
17. RETENTION CONSIDERATIONS 12
18. RECOVERY OF BACKUP DATA 13
19. THE ROLE OF BACKUPS IN RECORDS MANAGEMENT 13
20. POINTS GENERAL RULES FOR RETENTION PERIODS 16
21. ANNEXURE A: IMPLEMENTATION ROADMAP 21
22. ANNEXURE B: IMPLEMENTATION GUIDE 22
23. ANNEXURE C: TEMPLATE EXAMPLES 23
24. ANNEXURE D: BACKUP TYPES 25
25. ANNEXURE E: RESTORE TESTING TEMPLATE 26
26. ENFORCEMENT PROCEDURES 27

27. MONITORING AND EVALUATION OF THE IMPLEMENTATION OF THE POLICY....27
28. COMMUNICATION / EDUCATION OF THE POLICY 27
29. DISPUTE RESOLUTION MECHANISM....27
30. APPROVAL OF THE POLICY....27
31. REVIEW OF THE POLICY....27
32. VERSION CONTROL AND CHANGE HISTORY 28

1. PREAMBLE

The Department is committed in ensuring that ICT systems, data and infrastructure are protected from risks such as unauthorised access (see ICT Security Policy for further detail), manipulation, destruction, or loss of data, as well as unauthorised disclosure or incorrect processing of data.

2. PURPOSE OF POLICY

The purpose of this policy is to ensure that the department conforms to a standard backup and recovery control processes in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, service delivery efficiency. In addition, it seeks to define controls to enforce regular backups and support activities; so that any risks associated to the management of data backups and recovery are mitigated. This policy supports the Department Corporate Governance of ICT Policy for Department of Public Service and Administration to ensure effective protection and proper usage of the computer systems and its peripherals by all within the Department.

3. DEFINITIONS

Terminology	Definition
Ad hoc	As and when requested.
Availability	The proportion of time a system is in a functioning condition.
Backup time window	Time slot during a 24hour day that backups are allowed to run in.
Battle box	A battle box is comprised of all the required software and detailed documented information per application, server or data set on how to recover the service in the case of a disaster at the main site.
Critical data	Data that is required to be retained for a set period as determined by law, or data that can severely disrupt services when lost. Examples include: financial data, client personal data etc.
Data referencing	Data that defines the set of permissible values to be used by other data sets.
Downtime	Defined as the periods when a system is unavailable.
Generations	Structural term designating the grandfather-father-son (Full differential-incremental) backup relationship.

Terminology	Definition
Employees	Any person excluding independent contractor who works for another person or for the State and who receives, or is entitled to receive, any remuneration and who assists in carrying on or conducting the business of an employer
Integrity	Data integrity is defined as is the assurance that data is consistent and correct.
SAN	Storage Area Network, a device that has large amounts of space
Storage capacity	Amount of space (TB Terabyte; GB Gigabyte; MB Megabyte, KB Kilobyte) utilized
Virtual Machine	A software machine that is hosted by a physical host

4. APPLICATION AND SCOPE

This Policy has been created to guide and assist the department to align with internationally recognised best practices, regarding data backup, recovery controls and procedures; It recognizes that government institutions are diverse in nature, and therefore each adopts the approach of establishing and clarifying principles and practices to support and sustain the effective control of data backup and recovery.

The policy applies to employees in the department, including contract workers, interns, seconded workers, service providers. This policy is regarded as crucial to the effective protection of data and information, of ICT systems of the department. Departments must develop its own Data Backup and Recovery controls and procedures by adopting the principles and practices put forward in this policy.

5. LEGISLATIVE FRAMEWORK

I. Constitution of the Republic of South Africa Act, Act No. 108 of 1996.

II. Copyright Act, Act No. 98 of 1978

III. Protection of Personal Information Act (POPI Act) of 2013

IV. Electronic Communications and Transactions Act, Act No. 25 of 2002

V. Minimum Information Security Standards, as approved by Cabinet in 1996

VI. National Archives and Record Service of South Africa Act, Act No. 43 of 1996

VII. National Archives Regulations and Guidance

VIII. The National Archives and Records Service of South Africa Regulations

IX. Promotion of Access to Information Act, Act No. 2 of 2000 (PIAIA)

X. Promotion of Administrative Justice Act, Act No. 3 of 200(PAJA)

XI. Protection of Personal Information Act, Act No. 4 of 2013 (POPI)

XII. Regulation of Interception of Communications Act, Act No. 70 of 2002

XIII. Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.

XIV. Corporate Governance of Information and Communication Technology Governance Policy Framework

XV. Public Service Act

XVI. Public Service Regulations of 2016

6. CONSULTATION PROCESS WITH STAKEHOLDERS

The Departmental Senior Management Service members have been consulted for inputs during the review of this policy.

7. POLICY STATEMENT

The Department is committed to ensure that the departmental employees implement data backup and recovery controls and the data/information is correctly and efficiently backed up (stored) and recovered in line with best practice(s).

8. DATA BACKUP AND RECOVERY STANDARDS

8.1 Critical data, which is critical to the department must be defined by the department and must be backed up.

8.2 Backup data must be stored at a location that is physically different from its original creation and usage location.

8.3 Data restores must be tested monthly (see attached template in Annexure E).

8.4 Procedures for backing up critical data and the testing of the procedures must be documented. These procedures must include, as a minimum, for each type of data:

(a) A definition of the specific data to be backed up;

(b) The type(s) of backup software to be used (e.g. full back up, incremental backup, differential backup etc.);

(c) The frequency and time of data backup;
(d) The number of generations of backed up data that are to be maintained (both on site and off site);
(e) Responsibility for data backup;
(f) The storage site(s) for the backups;
(g) The storage media to be used;
(h) Any requirements concerning the data backup archives;
(i) Transport modes; and
(j) Recovery of backed up data

9 DATA BACKUP SELECTION

9.1 All data and software are essential to the continued operation of the department, as well as all data that must be maintained for legislative purposes, must be backed up.
9.2 All supporting material required to process the information must be backed up as well. This includes programs; control files, install files, and operating system software.
9.3 The application owner, together with the Director: ICT will determine what information must be backed up, in what form, and how often (by application of the Backup Types template, Annexure D).

10 BACKUP TYPES

10.1 Full backups should be run weekly preferably on weekends, along with daily machine replication. This will also aid in ensuring that data can be recovered and when necessary full machine recovery can be performed.
10.2 Differential/Incremental backups must be used for daily backups. This ensures that the backup time window is kept to a minimum during the week while allowing for maximum data protection
10.3 Machine replication is the process of cloning a Virtual Machines and copying it to a different location so that at any stage one can restore a crashed, failed, or problematic version of the Virtual Machines. In the event of a restore the process is very easy to follow and depending on the size of the machine can be quick.
10.4 A summary of backup types, along with their advantages, disadvantages and frequency can be found in Annexure D

11 BACKUP SCHEDULE

11.1 Choosing the correct Backup Schedule:

(a) Backup schedules must not interfere with day-to-day operations. This includes any end of day operations on the systems.

(b) A longer backup window might be required, depending on the type of backups chosen or occurring at that particular time.

11.2 Frequency and time of data backup:

(a) When the data in a system change frequently, backups can be large in size and may take longer.

(b) Immediate full data backups are recommended when data is changed largely or the entire database need to be made available at certain points in time. Regular, as well as event-dependent intervals need to be defined.

11.3 Previous versions:

(a) Depending on the size of the data as well as the SAN space available the backup system can have varying "restore points" to restore data from.

(b) Replicated machines are kept at an off-site location and when necessary are used for machine restoration.

12 DATA BACKUP PROCEDURES

12.1 The Director and ICT team must choose between automated and manual backup procedures based on their requirements and constraints. Both procedures are in line with best practice. The table below outlines the two procedures with their advantages and disadvantages:

Table 1 : Advantages and disadvantages of manual and automated backups

Type	Detail	Advantages	Disadvantages
Manual Backups	Manual triggering of the backup procedures.	The operator can individually select the interval of data backup based on the work schedule.	The effectiveness of the data backup is dependent on the discipline and motivation of the operator.
Automatic Backups	Triggered by a program at certain intervals.	The backup schedule is not dependent on the discipline and reliability of an operator.	There is a cost associated with automation. The schedule needs to be monitored and revised to include any non-standard updates and/or changes to the work schedule.

12.2 The Director and ICT team must choose between centralized and decentralized backup procedures based on their requirements and constraints. Both procedures are in line with best practice. The table below outlines the two procedures with their advantages and disadvantages:

Table 2 : Advantages and disadvantages of centralised backups

Type	Detail	Advantages	Disadvantages
Centralised Backups	The storage location and the performance of the data backup are carried out on a central ICT system by trained administrators.	Allows for more economical usage of data media.	There is added exposure to confidential data.
Decentralized Backups	Performed by ICT users.	ICT users can control the information flow and data media, especially in the case of confidential data.	The consistency of data backup depends on the reliability and skill level of the user. Sloppy procedures can result in data exposure or loss.

13 STORAGE MEDIUM

13.1 When choosing the data media format for backups, it is important to consider the following:

(a) Time constraints around identifying the data and making the data available;
(b) Storage capacity;
(c) Rate of increasing data volume;
(d) Cost of data backup procedures and tools vs. cost if restored without backup;
(e) Importance of data;
(f) Life and reliability of data media;
(g) Retention schedules; and
(h) Confidentiality and integrity.

13.2 Today the SAN device one chooses is of relative importance and must consider the criteria above. There are devices that are designed specifically for data storage and restoration that have features like data deduplication for optimum space utilization, redundancy to make sure data is always available under any circumstances, data line speed boost and more.

14. DATA BACKUP OWNER

The Director: ICT has delegated the two Network Administrators to commit and adhere to each backup schedule.

15. OFFSITE STORAGE SITE

15.1. Data backups must be stored in two locations:

(a) One on-site with current data in machine-readable format in the event that operating data is lost, damaged or corrupted; and

(b) One off-site to additionally provide protection against loss to the primary site and on-site data.

15.2 Off-site backups must be a minimum of 30 kilometres from the on-site storage area in order to prevent a single destructive event from destroying all copies of the data.

15.3 Should high availability be required, additional backup copies should be stored in the immediate vicinity of the ICT system.

15.4 Daily machine replication is performed to keep the amount of data to a minimum.

15.5 The site used for storing data media off-site must meet Physical Security requirements defined within the ICT Security Controls Policy.

15.6 All data media used to store confidential information must be disposed of in a manner that ensures the data is not recoverable.

16. TRANSPORT MODES

16.1 When choosing the transport mode for the data (logical or physical), it is important to consider the following:

(a) Data line constraints.

(b) Capacity requirements; and

(c) Security and encryption.

17. RETENTION CONSIDERATIONS

17.1. Data should be retained in line with current legislative requirements, as defined in sections 19 and 20 of this document.

17.2. An example of a possible retention schedule is as follows:

(a) A full system backup will be performed weekly. Weekly backups will be saved for a full month.

(b) The last full backup of the month will be saved as a monthly backup. The other weekly backup media will be recycled by the backup system.

(c) Monthly backups will be saved for one year, at which time the media will be reused.

(d) Yearly backups will be retained for five years and will only be run once a year at a predetermined date and time.

(e) Differential or Incremental backups will be performed daily. Daily backups will be retained for two weeks. Daily backup media will be reused once this period ends.

18. RECOVERY OF BACKUP DATA

18.1 Backup documentation must be maintained, reviewed and updated periodically to account for new technology, business changes, and migration of applications to alternative platforms. This includes, but is not limited to:

(a) Identification of critical data and programs; and

(b) Documentation and support items necessary to perform essential tasks during a recovery process.

18.2 Documentation of the restoration process must include:

(a) Procedures for the recovery.

(b) For key management should the data encrypt provision.

(c) Recovery procedures must be tested monthly.

(d) Recovery tests must be documented and reviewed by the Director: ICT.

19. THE ROLE OF BACKUPS IN RECORDS MANAGEMENT

19.1 The National Archives and Records Service of South Africa Act, Act 43 of 1996 requires sound records management principles to be applied to electronic records and e-mails created or received in the course of official business and which are kept as evidence of the department functions, activities and transactions. The detail of these requirements can be found in:

(a) The internet and e-Mail Usage of the department; and

(b) The National Archives and Records Service of South Africa Regulations.

19.2 The Records Manager is responsible for the implementation of sound records management principles and record disposal schedules for the department. The Records Manager is also responsible for maintaining the retention periods indicated on the file plan and disposal schedule.

19.3 The Director: ICT must work with the Records Manager to ensure that public records in electronic form are managed, protected and retained for as long as they are required.

19.4 Backups are not ideal, but not excluded, as a means of electronic record and e-mail retention for the prescribed periods. It is difficult to implement a proper file plan using backup media and therefore it is difficult to arrange, retrieve and dispose of records.

19.5 The role of backups in records management is more suited as a means to recover electronic records management systems and e-mail systems in the event of a disaster or technology failure.

19.6 The Director: ICT is responsible for the following, when backing up electronic records or e-mails that are regulated under the National Archives and Records Service of South Africa Act:

(a) Backups must be made daily, weekly and monthly;
(b) Backups must cover all data, metadata, audit trail data, operating systems and application software;
(c) Backups must be stored in a secure off-site environment;
(d) Backup files of public records must contain the subject classification scheme if files need to be retrieved from the backups;
(e) Backups must survive technology obsolescence by migrating them to new hardware and software platforms when required. An additional option to ensure that data can be read in the future is to store electronic records and e-mails in a commonly used format e.g. PDF or XML.
(f) The backup and retrieval software must also be protected to be available in the event of a disaster;
(g) Backups must be included in disaster recovery plans;
(h) The integrity of backups must be tested using backup test restores and media testing.

19.7 The Director: ICT must ensure that systems prevent the deletion of electronic records or e-mails without consulting the Records Manager.

19.8 The Director: ICT and Records Manager must implement the most practical method to retain e-mails e.g. file inside e-mail application, transmit to document management solution, transfer to e-mail archiving solution, save to shared network drive, print to paper etc.

19.9 Officials are responsible for filing e-mails. It is the responsibility of the sender or their designated official to file e-mails unless the e-mail is received from outside in which case the recipient or designated official is responsible for filing it. The Tables below assists with determining responsibility for retaining e-mail messages.

Table 3: Example decision sequence to assist with determining responsibility for retaining e-mail messages (Source: National Archives. Managing electronic records in governmental bodies: Policy, principles and requirements National Archives)

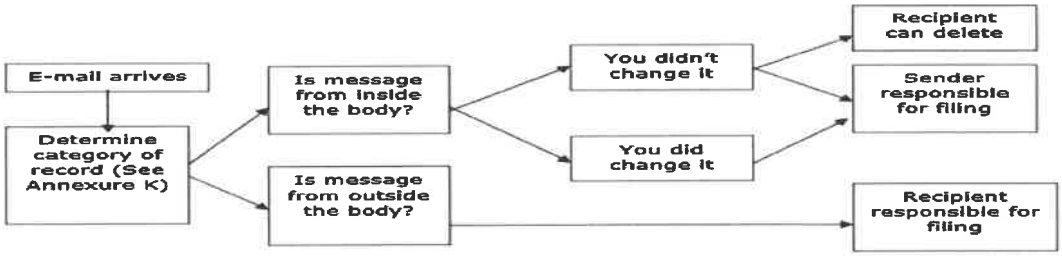
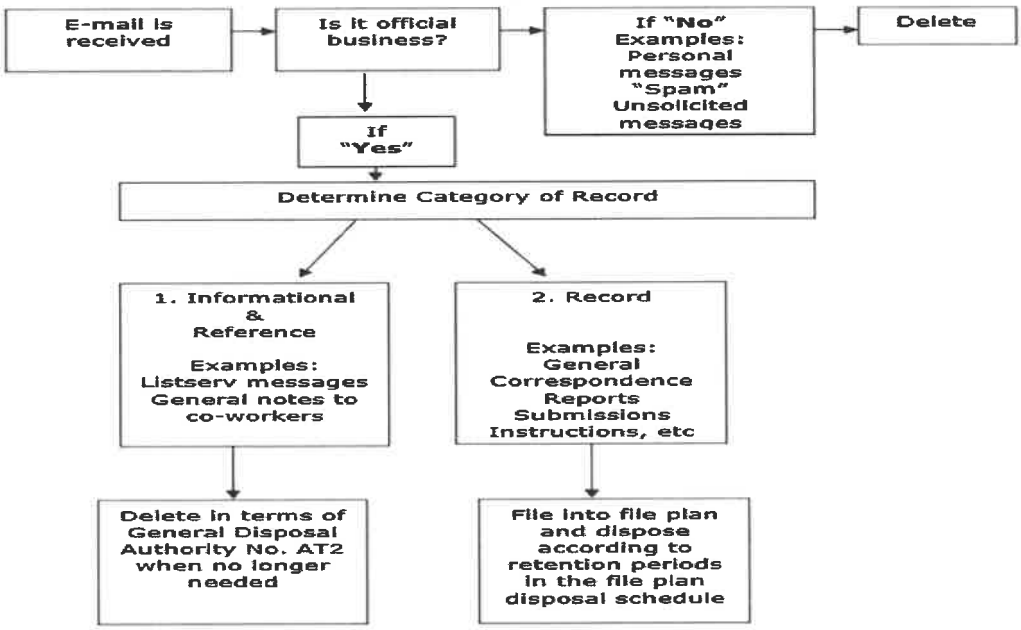


Table 4: Example of a decision sequence for determining e-mail retention (Source: National Archives. Managing electronic records in governmental bodies: Policy, principles and requirements National Archives)



19.10 The Records Manager must create awareness with Officials of the importance of e-mail as public records. This include, but are not limited to:

(a) E-mails must be properly contextualised and meaningful over time;
(b) Subject lines are very important and must be descriptive;
(c) The reference number of the subject folder in the file plan must be included in the top right hand corner of the message box;
(d) Auto-signatures must be used and shall contain full details of the sender; and
(e) Attachments must be filed into the file plan in the document management system before it is attached to the e-mail.

19.11 The Director: ICT must ensure that the e-mail system is set up to capture the sender and the recipient(s), and the date and time, the message was sent and/or received. When an e-mail is sent to a distribution list, information identifying all parties on the list must be retained for as long as the message is retained.

19.12 The Records Manager may dispose of any electronic records and e-mails if retention is not required under any Act or General Disposal Authority.

20. POINTS GENERAL RULES FOR RETENTION PERIODS

20.1 The National Archives provides the primary considerations when defining retention periods of electronic records and e-mails. This supports the goals of the Promotion of Administrative Justice Act, Act. No. 3 of 2000, which is to ensure that public records are available as evidence to ensure that administrative action is lawful, reasonable, and procedurally fair.

Table 5: Retention periods specified by the National Archives

Act or National Archive Regulations and Guidance	Item	Retention period
National Archives and Record Service of South Africa Act, Act No. 43 of 1996 Promotion of Administrative Justice Act, Act No. 3 of 2000	Public records and e-mails created or received in the course of official business and which are kept as evidence of the Department's functions, activities and transactions.	Records may not be disposed of unless written authorisation have been obtained from the National Archivist or a The National Archivist against records classified against the file plan has issued standing Disposal Authority.
General Disposal Authority PAP1 Disposal of personal files of local authorities	Personal case files of local authorities	At the discretion of the department, taking into consideration any Special circumstances.
General Disposal Authority No. AE1 for the destruction of ephemeral electronic records and related documentation	Electronic records with no enduring value	16 Categories of records. Refer to AE1 for details.

Act or National Archive Regulations and Guidance	Item	Retention period
General Disposal Authority No. AT2 on the destruction of transitory records of all governmental bodies	Electronic records not required for the delivery of services, operations, decision-making or to provide accountability	Refer to AT2 for details.
Managing electronic records in governmental bodies Policy, principles and requirements Managing electronic records in governmental bodies Metadata requirements	E-mails, and attachments therein, must be retained if they: • Are evidence of department transactions; • Approve an action, authorize an action, contain guidance, advice or direction; • Relate to projects and activities being undertaken, and external stakeholders; • Represent formal business communication between staff; or • Contain policy decisions.	E-mails fall into one of the 4 categories above and must be retained as such.

20.2 Public 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 Legal Services Manager has indicated that the destruction hold can be lifted.

20.3 The Public Finance Management ACT states that government records must be retained in the manner prescribed by legislation. However, the Act does not specify retention periods. National and Provincial retention periods for financial records are prescribed within National Treasury.

Regulations, Regulation 17 to the Public Finance Management Act, No. 1 of 1999, Section 40(1) (a). For the purposes of this policy, the Treasury Regulations, Regulation 17, will be used as guidance only without intervening National Archivist legislation, regulations, and guidance.

Table 6: Retention periods specified by Treasury Regulations, Regulation 17 (guidance only)

Act or National Archive Regulations and Guidance	Item	Retention period
Treasury Regulations, Regulation 17	Internal audit reports, system appraisals and operational reviews.	10 years
Treasury Regulations, Regulation 17	Primary evidentiary records, including copies of forms issued for value, vouchers to support payments made, pay sheets, returned warrant vouchers or cheques, invoices and similar records associated with the receipt or payment of money.	5 Years
Treasury Regulations, Regulation 17	Subsidiary ledgers, including inventory cards and records relating to assets no longer held or liabilities that have been discharged.	5 Years
Treasury Regulations, Regulation 17	Supplementary accounting records, including, for example, cash register strips, bank statements and time sheets.	5 Years
Treasury Regulations, Regulation 17	General and incidental source documents not included above, including stock issue and receivable notes, copies of official orders (other than copies for substantiating payments or for unperformed contracts), bank deposit books and post registers.	5 Years

20.4 In accordance with Treasury Regulations, Regulation 17(2), financial information must be retained in its original form for one year after the financial statements and audit report has been presented to the Auditor General.

20.5 Financial information may be stored in an alternative form, after expiry of one year from submission of the financial statements to the Auditor General, under the following conditions:

(a) The records must be accessible to users. This requires data referencing, a search facility, a user interface or an information system capable of finding and presenting the record in its original form.

(b) The original form may have reasonable validations added, which is required in the normal course of information systems communication, storage or display.

20.6 The Electronic Communication and Transaction Act, No 25 of 2005 regulates the storage of personal information:

Table 7: Retention periods specified by the Electronic Communication and Transaction Act, No 25 of 2005

Act	Item	Retention period
Electronic Communication and Transaction Act, No 25 of 2005	The person who electronically requests, collects, collates, processes or stores the information must keep personal information and the purpose for which the data was collected.	As long as information is used, and at least 1 year thereafter.
Electronic Communication and Transaction Act, No 25 of 2005	A record of any third party to whom the information was disclosed must be kept for as long as the information is used.	As long as the information is used and at least 1 year thereafter.
Electronic Communication and Transaction Act, No 25 of 2005	All personal data, which has become obsolete.	Destroy

20.7 The Protection of Personal Information Act, No. 4 of 2013 ("POPIA") will regulate the retention of personal information when it becomes active:

Table 8: Retention periods specified by the Protection of Personal Information Act, No. 4 of 2013

Sections	Item	Retention period
Sections 9 to 18	Gender, sex, marital status, age, culture, language, birth, education, financial, employment history, identifying number, symbol, e-mail address, physical address, telephone number, location, online identifier, personal opinions, views, preferences, private correspondence, views or opinions about a person, or the name of the person if the name appears next to other personal information or if the name itself would reveal personal information about the person.	Do not collect or retain unless the person have been given notice and consent obtained. Exceptions apply. Personal information may not be retained for longer than agreed with the person, unless a law requires the retention of the record. (This principle is applicable to all items in this table. The retention of items that follow is expressly prohibited unless Exceptions apply.)

Sections	Item	Retention period
Sections 6, 34 to 37	Children's information	Destroy unless, exceptions apply e.g. establishment or protection of a right of the child.
Sections 6 & 28	Religious or philosophical beliefs	Destroy unless, exceptions apply e.g. to protect the spiritual welfare of a community.
Sections 6 & 29	Race or ethnic origin	Destroy unless, exceptions apply e.g. protection from unfair discrimination or promoting the Advancement of persons.
Sections 6 & 30	Trade union membership	Destroy unless, exceptions apply e.g. to achieve the aims of trade union that the person belongs to.
Sections 6 & 31	Political persuasion	Destroy unless, exceptions apply e.g. to achieve the aims of a political institution that the person belongs to.
Sections 6 & 32	Health or sex life	Destroy unless, exceptions apply e.g. provision of healthcare services, special support for pupils in schools, childcare or support for workers.
Sections 6 & 33	Criminal behaviour or biometric information	Destroy unless, exceptions apply e.g. necessary for law enforcement.

21. ANNEXURE A: IMPLEMENTATION ROADMAP

No	Action	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6	Month 7	Month 8	Month 9	Month 10
1	Review current backup and recovery policy										
2	Assess compliance to ICT Data Backup and Recovery Policy										
3	Implement changes to procedures										
4	Train staff in new procedures										
5	Test newly implemented procedures										

22. ANNEXURE B: IMPLEMENTATION GUIDE

The Department will need to standardise its backup solutions and backup medium across all sites to implement the policy. The backup medium may include data replication to another site.

Where possible, the below Table 9 backup strategy must be strictly adhered to:

	Full Backup			**Differential Backup**	**Incremental Backup**
Data Set	**Monthly**	**Weekly**	**Yearly**	**Daily**	**Daily**
Financial (BAS , LOGIS) Systems	Last weekend in the month inline with systems closure dates	Last day of the week inline with systems closure dates	Weekend after Financial Year end inline with systems closure dates	Monday to Friday	
HR (Persal) Systems	Last weekend in the month	Last day of the week	Weekend after Financial Year end	Monday to Friday	
File and Print Server	Last weekend in the month	Last day of the week	Weekend after Financial Year end	Monday to Friday	Monday to Friday
Business Enablers (Mail, Active Directory etc.)	Last weekend in the month	Last day of the week	Weekend after Financial Year end	Monday to Friday	
Security Access	Last weekend in the month	Last day of the week	Weekend after Financial Year end	Monday to Friday	
Supporting Material (Application installation files)	Last weekend in the month	Last day of the week	Weekend after Financial Year end	Monday to Friday	

23. ANNEXURE C: TEMPLATE EXAMPLES

Table 10: Example roles and responsibilities

Backup Component	Responsible	Accountable	Contribute	Inform
Data Criticality "Rating"	ICT Application Team	ICT Application Team	ICT Team	ICT Backup Operator
Detailed Application/Server Build Documentation	ICT Application Team	ICT Team	ICT Backup Operator	ICT Backup Operator
Data Backup Selection List	ICT Team	ICT Application Team	ICT Backup Operator	ICT Backup Operator
Backup Monitoring	ICT Backup Operator	ICT Backup Operator	ICT Team	ICT Application Team
Backup Reporting	ICT Backup Operator	ICT Backup Operator	ICT Team	ICT Application Team
Media management	ICT Backup Operator	ICT Backup Operator	ICT Team	ICT Application Team
Offsite Storage	Offsite Data Custodians	ICT Backup Operator	ICT Team	ICT Application Team

Table 11: Example backup timeline

Backup Component	Daily	Weekly	Monthly	Quarterly	Ad hoc
Selection List Modifications					X
Backup Monitoring	X				
Backup Reporting		X	X		
Backup Capacity Reporting		X	X		
Backup Media Handling	X	X	X		
Restore Testing				X	

Table 12: Example items and action descriptions

Item	Action
System being backed up	Data Classification: Business critical data Server role: File and print server
Backup Selection	The data required to be backed up is determined and identified by the owner of the data set on this server.
Media used	• SAN device • No data encryption enabled
Backup Schedule	• Daily backups: Runs Monday – Friday from 17:00 till finished • Weekly backups: Runs every Saturday from 17:00 till finished • Yearly backup: Is manually run after financial yearend
Data Retention	• Largely depends on the amount of space on the SAN device as well as the amount of data backed up
Offsite Storage	• The data line must be highly available and fast enough to accommodate the amounts of data to be replicated • SAN device space must available
Data Backup Owner	• The backup is monitored and media is inserted on a daily basis by 2 identified onsite contacts.

24. ANNEXURE D: BACKUP TYPES				
Type	Detail	Advantages	Disadvantages	Frequency
Full data backup	All data requiring backup is stored on an additional data medium without considering whether the files have been changed since the last backup.	Simple and quick restoration of data due to the fact that all relevant and necessary files can be extracted from the latest full data backup.	Requires a high storage capacity. If full data backups are not carried out regularly, extensive changes to a file can result in major Updating requirements.	Weekly and monthly.
Incremental data backup	This procedure stores the files, which have been changed since the last incremental/full backup. Incremental data backups are always based on full data backups and must be combined periodically with full data backups. During restoration, the latest full backup is restored first, after which incremental backups are restored to the most current state of the backed-up data.	Saves storage capacity and shortens the time required for the data backup.	Restoration time for data is generally high, as the relevant files must be extracted from backups made at different stages.	Daily.
Differential data backup	This procedure stores only the files that has been changed since the last full data backup. During restoration, the latest full backup is restored first, after which differential backups are restored to the most current state of the backed-up data.	Files can be restored quicker and easier then incremental backups.	Requires more capacity on the backup medium than incremental backups.	Daily.
Image backup	This procedure backs up the physical sectors of the hard disk rather than the individual files on it.	Full backup, which allows for very quick restoration of hard disks of the same type. Very effective for disaster recovery.	Not useful for Restoration of individual files.	Used for systems with very specific and specialized configuration.

25. ANNEXURE E: RESTORE TESTING TEMPLATE

RESTORE TESTING TEMPLATE

a) Responsible person: *b) Location / dept.:* *c) Date:*

SERVER BACKUPS TESTED:

1.□ server OS: .....

2.□ server OS: .....

3.□ server OS: .....

4.□ server OS: .....

DATABASE BACKUPS TESTED:

1.□ database: .....

2.□ database: .....

3.□ database: .....

4.□ database: .....

OTHER BACKUPS TESTED:

1.□ Other: .....

OFF-SITE BACKUPS TESTED:

1.□ server OS: .....

2.□ server OS:.....

□ *Backups can be used for disaster recovery*

h) Reviewed: *i) Date:*

26. ENFORCEMENT PROCEDURES

- Implementation of group policies

27. MONITORING AND EVALUATION OF THE IMPLEMENTATION OF THE POLICY

DGITO will report any challenges that arise in the implementation of this policy to the ICT Steering Committee.

28. COMMUNICATION / EDUCATION OF THE POLICY

The Policy will be communicated to Departmental employees through induction workshops / policy rollout sessions, internal news bulletin and available on the departmental intranet for sharing information.

29. DISPUTE RESOLUTION MECHANISM

In the event of disputes arising out of this policy, such disputes will be dealt with in terms of the grievance procedure and labour legislation applicable in the Public Service.

30. APPROVAL OF THE POLICY

The policy will be approved by Member of Executive Council (MEC) on the recommendation of the Head of Department.

31. REVIEW OF THE POLICY

This policy will be reviewed on every fifth year from the date of approval and/or when there are changes in legislation or the operating environment.

32. VERSION CONTROL AND CHANGE HISTORY

Version Control	Date Effective	Approved By	Amendment
Start from	YYMMDD (the date the policy takes effect	Contact person – full name & title.	Include any superseded procedures and what the amendment is to the document.