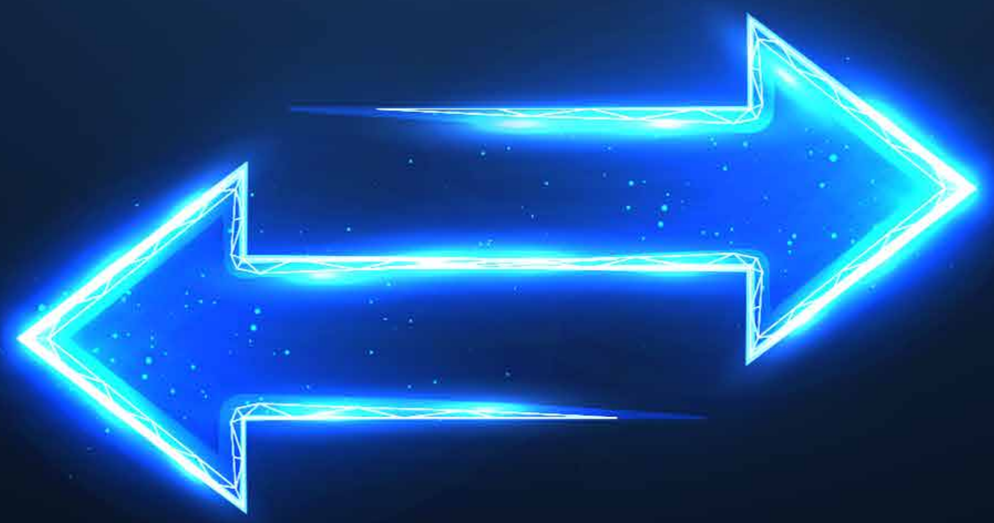
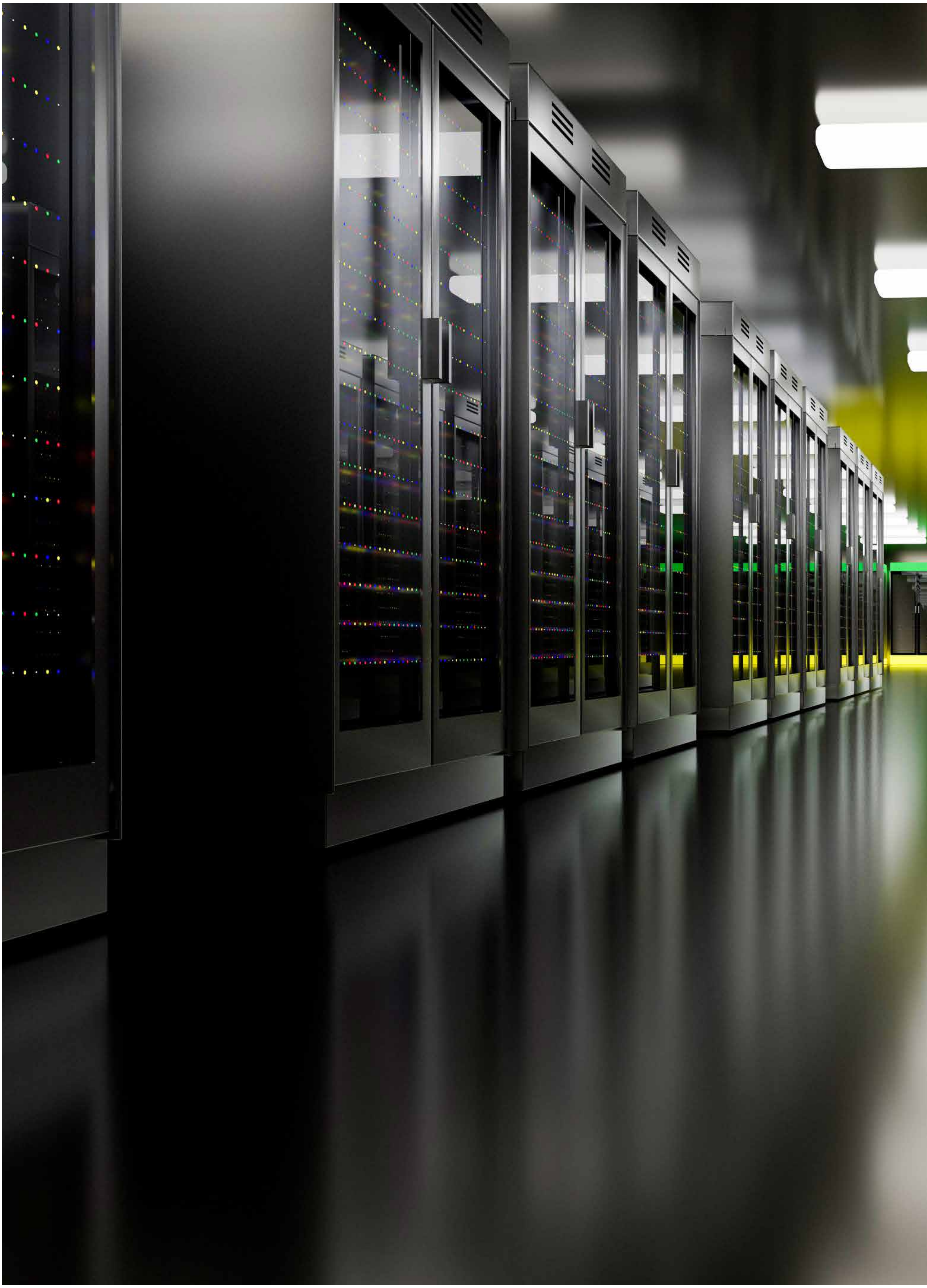


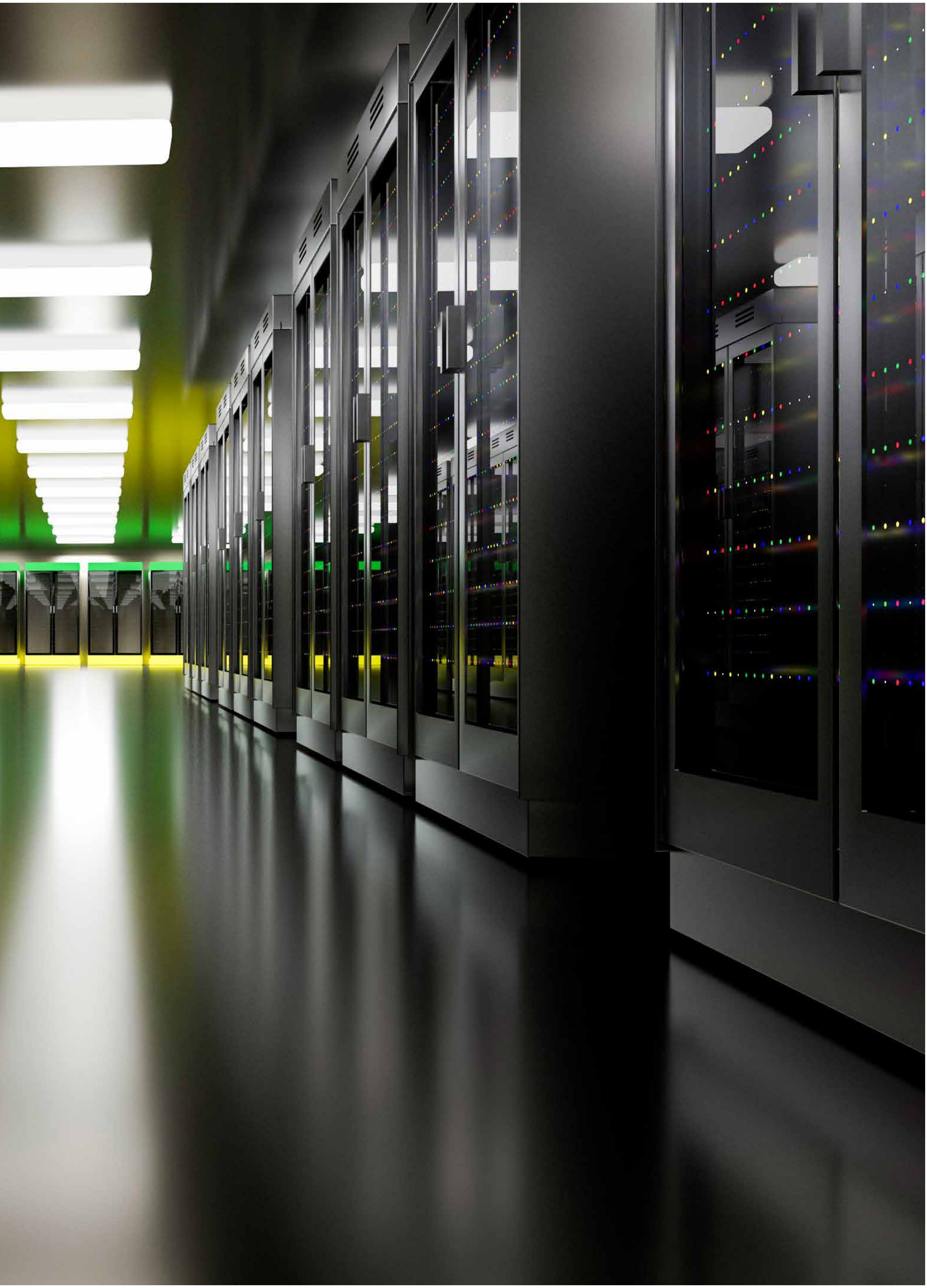
DISASTER RECOVERY AND BACKUP POLICY

FOR GOVERNMENT

MINISTRY OF COMMUNICATIONS AND DIGITALISATION
GOVERNMENT OF GHANA

NITA
National Information Technology Agency
GHANA



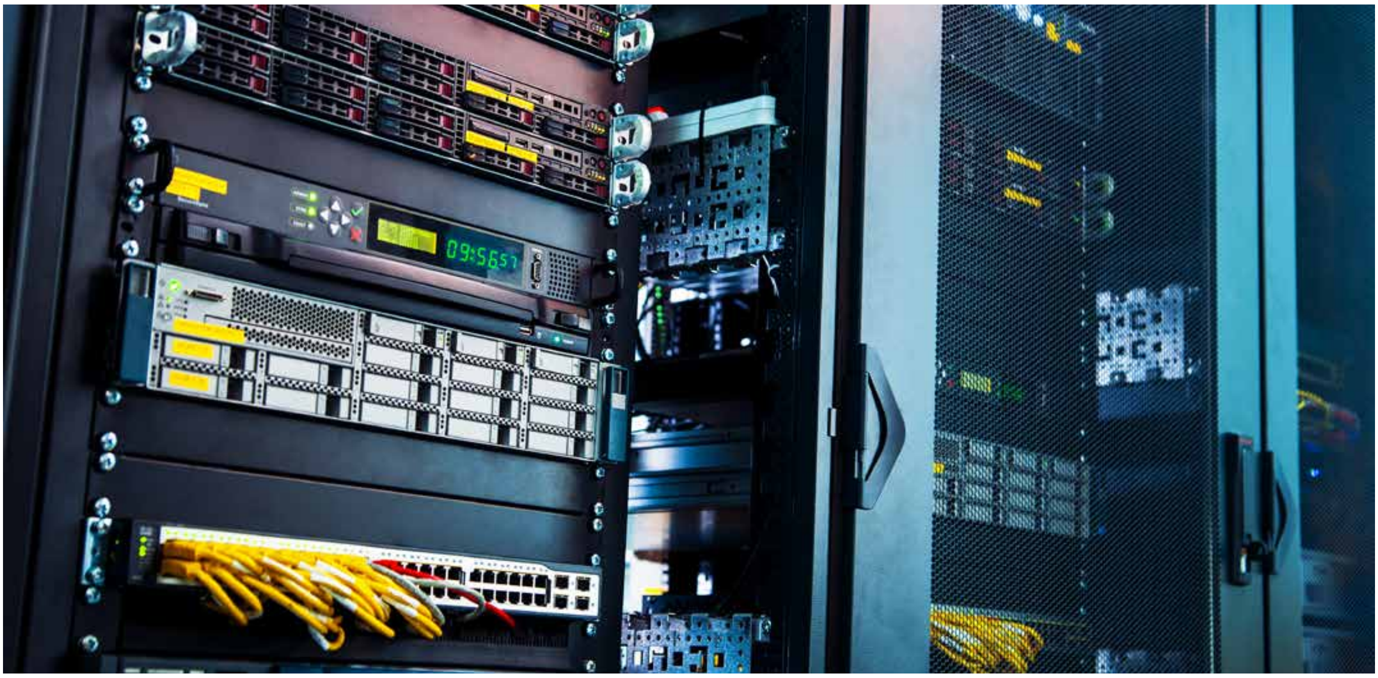


Contents

Abbreviations

ABBREVIATION	DESCRIPTION
AD	Active Directory
HR	Human Resources
UI	User Information
LTO	Linear Tape Open
	8.1.4 Wrist strap ports shall be attached to the rack by a means that ensures electrical continuity to ground for static discharge.

TERMINOLOGY	DESCRIPTION
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 medium	Medium on which backups are stored egg. Tapes, hard disks, CD/DVD 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.
Integrity	Data integrity is defined as is the assurance that data is consistent and correct.
Pseudo generation	Randomly created.
Storage capacity	Amount of space (Tb; Gb; Mb) utilized.



1.0 Disaster Recovery and Backup Policy

1.1 Introduction

Information security is becoming increasingly important to the country, driven in part by changes in the regulatory environment and advances in technology. Information security ensures that Ghana's ICT systems, data and infrastructure are protected from risks such as unauthorized access, manipulation, destruction or loss of data, as well as unauthorized disclosure or incorrect processing of data.

The National Information Technology Agency (NITA), in line with the object of Acts 772 and 771, request MDAs to observe best practices of ICT adoption and usage in their daily processes to ensure business continuity.

Making backups of systems/files ensures that original data files can be restored from backup copies, should there be any interruption due to:

- hardware faults or failure
- software or media faults
- virus infection or malicious hacking
- power failure
- human errors by changing or deleting files

A lot of MDAs have had their data lost due to a few of the above reasons. Choosing a backup strategy depends on local circumstances, the value of the data, and the levels of risk appropriate for the circumstances and a risk analysis helps define backup needs.

1.2 Objective of the Policy

Disaster recovery planning is an important activity that the Agency requires MDAs to undertake to maximize the potential of ICT in their business processes. The purpose of this planning process is to ensure that cost-effective controls to prevent possible IT disruptions and to recover the IT capacity of the MDAs in the event of a disruption are in place.

The availability of business data and the ability to process and handle them are vital to the sustainable development and/or survival of any MDA. Planning for disasters is, therefore, an important part of the risk management and business continuity planning (BCP) processes that shall be enforced in reference to provisions of the law (Act 772 sections 59 and 104).

The primary objective of the policy is to protect government data and seeks to outline the data backup and recovery controls for MDAs so as to ensure that the data is correctly and efficiently backed up and recovered in line with best practice in the event of any interruption.

1.3 Aims of the Policy

The aim of this policy is to ensure that the Ministries, Departments and Agencies conform to a standard backup and recovery control process in such a way that it achieves a balance between ensuring legislative compliance and best practice controls. 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.

1.4 Scope

This ICT Data Backup and Recovery Policy has been created to guide and assist the MDAs and MMDAs to align with internationally recognized best practices, regarding data backup, recovery controls and procedures. This policy recognizes that MDAs and MMDAs are diverse in nature, and therefore 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 every MDA and MMDA, including their service providers and consultants. This policy is regarded as crucial to the effective protection of data, of ICT systems of the various MDAs and MMDAs. MDAs and MMDAs must develop their own Data Backup and Recovery controls and procedures by adopting the principles and practices put forward in this policy.

1.5 Breach of Policy

Any failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach. All misconduct and/or breaches will be assessed and evaluated on its level of severity. Appropriate disciplinary action or punitive recourse will be instituted against any MDA or MMDA, who contravenes this policy.

Data Backup Standards

Critical databases are collections of critical data in an electronic form kept in a site from where the data may be accessed, reproduced or extracted. The following explains critical data, data with;

a. importance to national security
b. economic or social well-being of its citizens.
c. data that is essential to the daily functioning of an MDA/MMDA

Critical databases include data that the interruption or destruction of which could have widespread effects and consequently result in or generate grave consequences to the organization. At a governmental level, an interruption or destruction of critical databases could hamper and/or delay the delivery of services.

Critical data, which is critical to the MDAs and MMDAs, must be defined and backed up.

i. Backup data must be stored at a location that is physically different from its original creation and usage location, along with a "battle box".
ii. Data restores must be tested monthly.
iii. 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 definition of the specific data to be backed up;

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

2.1 Data Backup Selection

All data and software essential to the continued operation of the MDA/MMDA, as well as all data that must be maintained for legislative purposes, must be backed up.

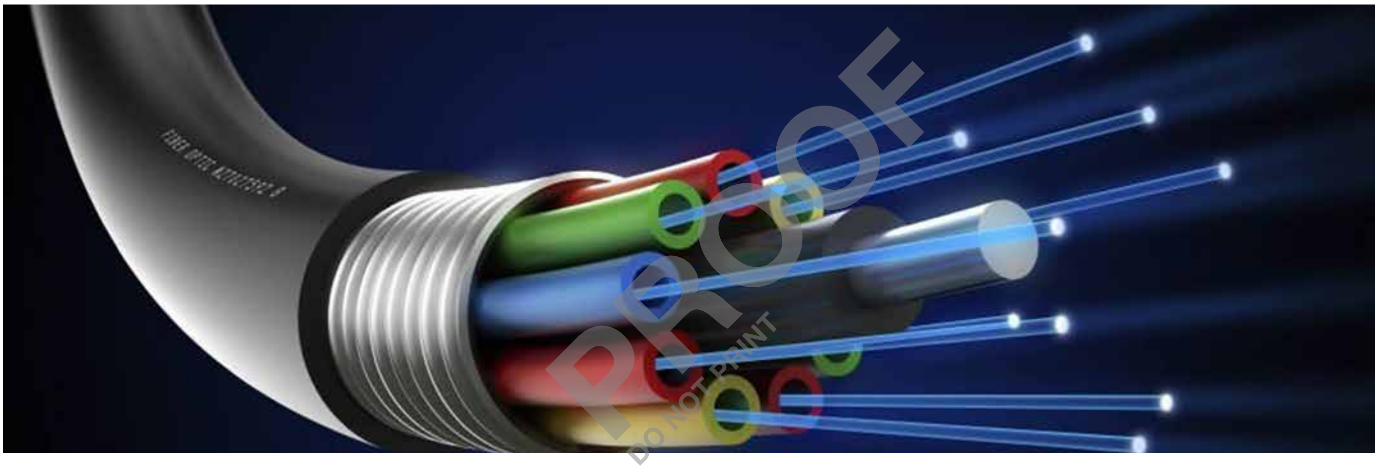
All supporting material required to process the information must be backed up as well. This includes programs; control files, install files, and operating system software.

The application owner, together with the ICT Manager, will determine what information must be backed up, in what form, and how often

2.2 Backup Types

Full backups should be run weekly as these datasets will be stored for a longer time period. This will also aid in ensuring that data can be recovered with the minimal set of media used at that time. Once a month, a full backup should be stored off site. This statement will need to be reviewed once the ICT DR Business Impact and Risk Analysis requirements are updated with input from Line Managers and MDA operations

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. In the event that a system requires a high degree of skill to recover from backup, consider taking full images of the servers as a backup. This will ensure that the system can be recovered with minimal knowledge of the system configuration.



2.3 Backup Schedule

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.

Frequency and time of data backup:

(a) When the data in a system changes frequently, backups needs to be taken more frequently to ensure that data can be recovered in the event of a system failure.

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

Previous versions:

(a) The previous two versions of operating systems and applications must be retained at the off-site storage location.

(b) Annual, monthly and weekly backups must be retained at the off-site facility. Monthly backups may be re-used to take new backups, when annual backups are successfully taken.

2.4 Data Backup Procedures

The Head, ICT may 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:

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

Table 1: Advantages and disadvantages of manual and automated backups

The Head, ICT may 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:

Type	Detail	Advantages	Disadvantages
Centralized Backups	The storage location and the performance of the data backup are carried out on a central ICT system by a small set of trained administrators.	Allows for more economical usage of data media	There is added exposure to confidential data. Confidential and non-confidential information may be combined requiring more stringent security controls for handling the backups.
Decentralized Backups	Performed by ICT users or administrators without being transferred to a central ICT system.	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.

Table 2: Advantages and disadvantages of centralized and decentralized backup procedures

2.4 Storage Medium

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.

Should high availability be required, a compatible and fully operational reading device (e.g. tape drive, CD, DVD) must be obtainable on short notice to ensure that the data media is usable for restoration even if a reading device fails.

2.5 Data Backup Owner

a. MDAs/MMDAs should ensure that sufficient ICT capacity is available to maintain the Backup and Disaster Recovery procedures, so to ensure a segregation of duties and responsibilities and to mitigate the risk of systems and data losses.

b. The Head, ICT has the discretion to assign at least two ICT staff (One primary, one secondary) to ensure each backup schedule is maintained.

2.6 Offsite Storage Site

I. 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.

II. Off-site backups must be a minimum of 6 kilometres from the on-site storage area in order to prevent a single destructive event from destroying all copies of the data.

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

IV. Minimum requirements are to store the weekly, monthly and or yearly backup sets off site.

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

VI. Weekly and monthly backups must be stored offsite for the entire duration of the retention period.

VII. Receipts of media being collected and delivered must be kept for record keeping purposes and must be signed by ICT staff in attendance.

VIII. Should an off-site media set be required to perform a restore, the data media must be returned to the offsite facility for the remainder of the retention period

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

2.7 Transport Modes

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

a. Time constraints;
b. Capacity requirements; and
c . Security and encryption.

2.8 Retention Considerations

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.

3.0 Recovery Of Backup Data

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.

Documentation of the restoration process must include:

a. Procedures for the recovery
b. Provision for key management should the data be encrypted. 18.3 Recovery procedures must be tested monthly.

Recovery tests must be documented and reviewed by the ICT Manager.

ANNEX 1: 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.	Saves storage capacity and shortens the time required for the data backup. Very effective for disaster recovery.	Restoration times for data is generally high, as the relevant files must be	Daily configuration
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.

ANNEX 2: Backup Strategy

Data Set	Full Backup			Differential Backup	Incremental Backup
	Monthly	**Weekly**	**Yearly**	**Daily**	**Daily**
Financial Systems	Weekend after Financial Year end	Last day of the week	Weekend after Financial Year end	Monday to Friday	
HR Systems T&A (Payroll, Leave, etc)	Last Weekend in the month	Last day of the week	Weekend after Financial Year end	Monday to Friday	Monday to Friday
Files and Print Services	Last weekend in the month	Last day of the week	Weekend after Financial Year end	Monday to Friday	
Business Enablers (Mail, eDirectory, AD, SQL, etc.)	Last Weekend in the month	Last day of the week	Weekend after Financial Year end	Monday to Friday	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	

Table 4: Backup Strategy

ANNEX 3: Roles and Responsibilities

Backup Component	Responsible	Accountable	Contribute	Inform
Data Criticality "Rating"	ICT System Administrator	ICT System Administrator	ICT Team	ICT Backup Operator
Detailed Application/Server Build Documentation	ICT System Administrator	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, System	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 5: Roles and Responsibility

Annex 4: Systems Backup

Data Retention

During the Assessment and Design session, the following Data Retention requirements have been outlined:

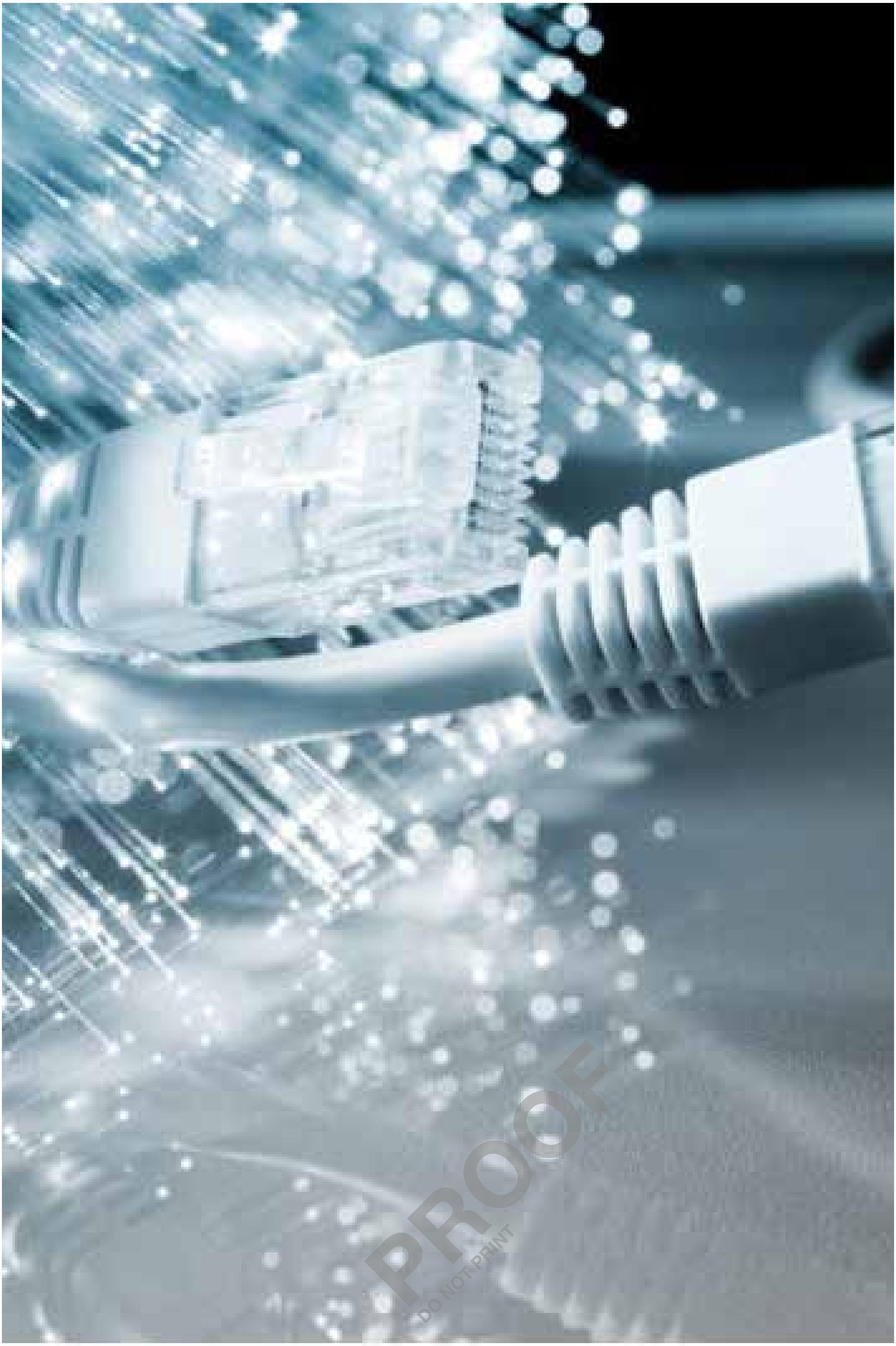
- All backups will be targeted to Disk and a copy of the data will be maintained on Disk and Tape at DR for short-term and long-term retention respectively.
- As per the best practices and upon reviewing the data retention requirements, data retention requirements are outlined in the table below;

Job Type	Retention on Disk	Retention Offsite/at DR
All Incremental Backups	15 Days	15 Days Disk
Daily Full Backups (All Non- Database)	15 Days	15 Days Disk
Weekly Full Backups (All Non-Databases)	15 Days	90 Days Disk
Monthly Full	356 Days	Tape
Yearly Full	1825 Days	Tape
Media Management	ICT Backup Operator	ICT Backup Operator
Offsite Storage	Offsite Data Custodians	ICT Backup Operator

Table 6: Data Retention

To summarize, all the backups will be performed to Disk as primary target and retained for a period of 15 Days on Premises. A Synchronous copy of all backups will be maintained on disk at the DR Site for 15 Days along with separate copy of Weekly Full on Tape for 90 Days and extended retention for Monthly Full on Tape forever.

Sufficient disk space will be required to achieve the Retention on Disk requirements at a growth rate of 30% per annum.



Business Processes

Key business processes and the agreed backup strategy for each are listed below. The strategy chosen is for Full Disaster Recovery for Core Systems is a fully mirrored recovery site at the National Data Centre.

This strategy entails the maintenance of a fully mirrored duplicate site which will enable instantaneous switching between the live site at the MDA/MMDA level and the backup site at the National Data Center and backups for the recovery of single or multiple systems at the main site.

Core System		Retention Offsite/at DR
Type	Name	
Works Order Systems	HRMIS, NaMEIS, EMIS etc	Daily, Fully, mirrored recovery site
Messaging	Smartworkplace	Daily, Fully, mirrored recovery site
Financial Systems	GIFMIS, PIMS (including Web Services)	Daily, Fully, mirrored recovery site for the MSSQL and Front-End Services. Refer to GIFMIS documentation for GIFMIS Classic backup schedule
Other systems	EMIS, DHIMS 2, GIFMIS, HRMIS	Daily, Fully, mirrored recovery site
HR, Collaboration, Correspondence	and YOANA	Daily, Fully, mirrored recovery site
Payroll and ESS (Employee Self Service)	Collaborator	Daily, Fully, mirrored recovery site
Time & Attendance	(including SharePoint / Web Services / Front End Services)	Daily, Fully, mirrored recovery site
GIS	ePayslip	Daily, Fully, mirrored recovery site
MicroFocus Application Services	(Novell / MicroFocus) e.g. Filr	Daily, Fully, mirrored recovery site
Windows, Unix\Linux File System & NFS	*NIX/NFS: Novell / MicroFocus OES Windows: Microsoft Servers	Daily, Fully, mirrored recovery site
AD / E-Directory	E-Directory: Novell / MicroFocus	Daily, Fully, mirrored recovery site
Database	MS SQL	Daily, Fully, mirrored recovery site
Virtual Infrastructure	VMWare, VMVCenter	Daily, Fully, mirrored recovery site

Table 7: Core Business System

Data Retention	Daily backups: Media set is retained for 2 weeks Weekly backups: Media set is retained for 1 month Monthly backup: Media set is retained for 1 year Yearly backup: Media set is retained for 5 years
Offsite Storage	All media is moved and stored offsite at a secured facility after the successful completion of the backup. The same facilitator providing the offsite storage, is used to provide transport of the media to the secure site. All media is moved and stored offsite at a secured facility after the successful completion of the backup.
Data Backup Owner	The Tape backup is monitored and media is inserted on a daily basis

Annex 5: Tape Backup Rotation

MDA/MMDA IT is responsible for:

1. Changing tapes: Once a month the disk backups are migrated to tape. These tapes are then removed and taken offsite and new tapes added to the library. IT must ensure that these migrations have taken place and logs must be kept of these migrations.

2. The backup tapes are stored offsite at the MDA/MMDAs DR Site

3. All backup notifications are sent to three support personal, two MDA/MMDA IT Administrators and Lateral Dynamics to ensure the success of the backups and the recovery of any failures.

Verification of Backup Status

Every morning, the backup notifications are verified by the Administrator: It

Backup Log

A daily backup log is issued (emailed) to keep a report of backups, their status, which tapes are used and housekeeping of the backup system. These logs are stored within the Backup System and Administrator email.

House-keeping of the Backup System

Regular maintenance of the backup device is carried out to ensure it is kept in good working order. Cleaning tapes are used in accordance with manufacturer's instructions. DLT tape drives should be cleaned monthly.

Managing Backup Failure

In the event of an unsuccessful backup, the staff responsible for checking the backup must immediately:

a. Note any messages / information in the log file

b. Contact the senior IT/IM Officer/or Senior IT/IM Officer to report the failure

c. Record the failure in the backup log and any actions taken as a result

d. Restart the backup or ensure that the cause of failure is solved before next backup schedule (if this is a viable course of action). If not, the affected business unit or department will be informed and a new course of action will be mutually agreed.

If the backup fails repeatedly, it may be necessary to perform a manual backup. This takes time, and must be performed when all users are logged out. This will include logging the call with the Backup Vendor to identify the underlying cause and report back to management.

Storage of Backup Tapes

The backup tapes, when removed from the server, are stored securely in an off-site secure location (locked fire-proof safe). At any time there should be:

1. Two or more complete backups, 7 days old stored, at the MDAs DR site/premises

2. Two or more complete backup tapes, 30 days old stored, off-site at a secure location.

Validation of Backup Tapes

A backup tape is validated by the IT/IM Officer/or Senior IT/IM Officer every 3 months. As part of this process the IT/IM Officer/or Senior IT/IM Officer will check to ensure data can be fully restored from the tape.

Management of Tapes

Backup Volumes are clearly labelled with a month or server and used in strict rotation to ensure even wear and immediate identification of any problems with a specific tape.

Annex 6: Systems Protection Strategy

Windows File System

Windows File System Agent will be used to protect File System & System State data on local disks of Physical Servers.

Weekly Synthetic Full and Daily Incremental backup schedule will be implemented. Paths & Shares to be protected will specified.

File System Protection:	Physical Servers (Windows File System)
Data Protection Summary:	Daily DE duplicated backup Weekly Synthetic(DASH) Full
Service Account Requirements (Permissions/Rights)	Local Administrator Read\Write Access to Shared Folders

Unix\Linux File System & NFS

Unix/Linux File System Agent will be used to protect File System & System State data on local disks of Physical Servers.

Weekly Synthetic Full and Daily Incremental backup schedule will be implemented.
Paths & Shares to be protected will specified.

File System Protection:	Physical Servers (Windows File System)
Data Protection Summary:	Daily deduplicated backup Weekly Synthetic(DASH) Full
Service Account Requirements	Local Administrator Read\Write Access to Shared Folders

Active Directory and eDirectory

The Microsoft Active Directory Domain of Overstrand is hosted on a Domain Controller. Domain Controllers are Virtual Machines in VMWare environment and Domain Controller is hosted at the National Data Center Site.

The MicroFocus E-Directory for the MDA/MMDA are hosted on various UNIX machines as a Federated Directory Service. E-Directory Controllers are Virtual Machines in VMWare environment hosted at the National Data Center Site as well as at each Administration for fault tolerance.

File System Protection:	Domain Controller
Data Protection Summary:	Daily Full with Active Directory Agent

Microsoft SQL Server

The Overstrand has MSSQL Servers, which are both Standalone MSSQL Servers and host instances & databases. Backup Schedule will include a Daily Full and Transaction Log backup every 6 hours for all MSSQL Instances.

File System Protection:	MSSQL Databases
Data Protection Summary:	Daily Full Backup Transaction Log Backup every 1Hr
Service Account Requirements (Permissions / Rights)	Local Administrator SQL Admin System Account

Microsoft SharePoint Server

The MDA/MMDA environment consists of SharePoint Server(s) in Production and Development environments; with a mix of Web App Servers and Front-End Servers.

MDAs/MMDAs are to utilise a Microsoft SharePoint Agent on the SharePoint Application Servers in Production environment to enable granular backup & recovery of Site Collections and Documents, VM Level Backup will also be configured for the SharePoint servers to provide full system recovery capabilities. SharePoint Databases are hosted on MSSQL database which will be protected with an MSSQL Agent.

The database or farm level backup protects all databases within the SharePoint environment as well as IIS configuration and customisations residing as files on the Windows file system.

SharePoint Data	Data Protection Summary:
Application	Weekly DASH Full & Daily Incremental backup
SharePoint Databases	Backup using the SQL Agent installed on the SQL 2014 SQL client.Daily Full TLog backup every 6hrs
Web & App Servers	Weekly DASH Full & Daily Incremental Backup
Service Account Requirements (Permissions / Rights)	A Windows AD domain user account with the following privileges: Local administrative rights (Part of local Administrators group) FARM administrator rights Full permission to additional settings (registry key) SP Shell administrator permissions Full control under Policy for Web Application for every Web Application SQL System Admin Server Role for the instance where SharePoint Databases resides Site Administrator permissions for all Site Collections Full permissions to the Job Results and Log Files folders

SQL server Services account for SharePoint instance. **SharePoint Services Timer Account** **All Web Application Pools Accounts**	Full permissions to the Job Results and Log Files folders

Smart workplace

To secure a Smart workplace database at the MDA/MMDA, the (Unix) OES File System Agent will be used. Any other agent (e.g., Windows File System) cannot be used to secure a Smart workplace).

Clients need to be scheduled to perform weekly one full backup and daily incremental backups.

File System Protection:	**Smart workplace Databases**
Data Protection Summary:	Backup using the OES Agent installed on the Servers Weekly Full & Daily Incremental Backup
Service Account Requirements (Permissions / Rights)	User account for Smart workplace User account credentials to log onto Smart workplace (Storage Management Services). User account for Target Service Agent (TSA)

VMWare Infrastructure

The MDA/MMDA has VMWare ESX hosts in cluster configuration in the MDA/MMDA domain, managed by a single vCenter server per site, which needs to be protected with Virtual Server Agents. All the VMs are to be protected with VM Level backup.

VMWare Protection:	**VM Guests utilising VHD based disks (VM Level backups)**
Data Protection Summary:	Daily deduplicated Incremental backup Weekly DASH Full
VMWare Requirements (Permissions / Rights)	User account for Local Administrator VMWare Administrator

Annex 7: References

•Electronic Transactions Act, Act 772 of 2008

•National Information Technology Agency Act, Act 771 of 2008

•Data Protection Act, 2012 (Act 843)

•Financial Administration Act 2003, ACT 654

•BS ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls. (2013).

•Control Objectives for Information Technology (COBIT) 5. (2012). ISACA.

Abdul Diouf Road, Ridge
3rd Floor,
Ministry of Communications Office Complex
Digital Address: GA-079-0539
PMB Ministries Post Office, Accra-Ghana

🌐 www.nita.gov.gh ✉ info@nita.gov.gh
☎ +233 0302 661 777 | +233 0302 661 833 (Fax)