NATIONAL DATA
MANAGEMENT AUTHORITY

Data Backup & Recovery Plan Guideline

Prepared By:
National Data Management Authority
July 2023

Document Status Sheet

	Signature	Date
Policy Coordinator (Cybersecurity)	**Muriana McPherson**	**20-07-2023**
General Manager (NDMA)	**Christopher Deen**	**20-07-2023**

Document History and Version Control

Date	Version	Description	Authorised By	Approved By
20-07-2023	**1.0**		**General Manager, NDMA**	**National ICT Advisor**

Summary

1. This Guideline addresses industry standards and best practices for developing data backup strategies.
2. It was adapted from Tech Target.
3. This is a living document which will be updated annually or as required.
4. Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

1. **Purpose**

Performing data backups is critical to ensuring business continuity in an organisation since it aids the recovery process after unfavourable circumstances such as hardware failure, malware infection, cyber-attacks, power failure and disasters. The purpose of this data backup & recovery plan guideline is to outline measures which must be implemented to ensure that the Government of Guyana's Agencies and Ministries can safely and securely back up mission-critical data, systems, databases, and other technologies so that it will be available in the event of a disruption affecting business operations. All Ministry/Agency locations are expected to implement data backup measures wherever possible to minimise operational disruptions and to recover as rapidly as possible when an incident occurs. Of note, this guide represents the minimum requirements for a successful data backup and recovery plan and should be tailored to meet the specific needs of your organisation.

2. **Authority**

The Permanent Secretary, Administrative Head, or their designated representative of the Public Sector Organisation is responsible for the implementation of this guideline. Please contact the Policy Coordinator – National Data Management Authority (NDMA) for further information regarding the foregoing.

3. **Scope**

This guideline encompasses all Government of Guyana's Agencies/Ministries' data backup operations in all locations and is limited to data backup activities and is not a daily problem resolution procedures document.

4. **Model**

This guide has been compiled following industry standards and best practices for developing backup strategies, including the recommended and widely recognised 3-2-1-1 backup model, which was originally formulated by the Cybersecurity and Infrastructure Security Agency (CISA) and has since evolved to deal with emerging threats such as ransomware.

The model requires keeping (3) three copies of data, with (2) two copies being stored on separate media types (for example, local storage and cloud storage), where one is stored off-site, and is either immutable or stored offline once the backup jobs are completed. Immutable storage refers to a data storage method where once data is written, it cannot be altered or deleted for a specified retention period. The 3-2-1-1 method ensures data recoverability by safeguarding against hardware failures, data corruption and ransomware attacks. Following the guide below will help you comply with the recommended model.

5. Backup & Recovery Plan Guideline

5.1. Objectives of a Backup Plan

5.1.1. Defines the requirements for planning, executing, and validating backups and includes specific activities to ensure that critical data is backed up to a secure storage media in a secure location.

5.1.2. Ensures the recoverability of servers, network components and other infrastructure devices as well as critical applications, databases, and important files.

5.1.3. Serves as a guide for the Government of Guyana's Agencies/Ministries' IT data backup teams.

5.1.4. References and points to the location(s) of backed-up data, systems, applications, and other mission-critical data resources.

5.1.5. Provides procedures and resources needed to back up data, systems, and other resources.

5.1.6. Identifies stakeholders that must be notified in the event of a disruption that may necessitate recovering backed-up data and other resources.

5.1.7. Minimises operational disruptions by documenting, testing, and reviewing data backup procedures.

5.1.8. Identifies alternate sources for data backup activities.

5.1.9. Documents data storage, backups and retrieval procedures for vital records and other relevant data.

5.2. Assumptions

5.2.1. Key IT employees (e.g., lead data backup administrator, team leaders, technicians, and alternates) will be available to restore data following a disaster.

5.2.2. The backup plan and related documents are stored in a secure off-site location and not only survived the disaster but are accessible immediately following the disaster.

5.2.3. The Agency/Ministry will have a disaster recovery (DR) plan that aligns with the data backup plan.

5.2.4. The data backup plan includes the agency/ministry's established classification of systems and data and their associated restore point objectives (RPOs) and restore time objectives (RTOs).

5.3. Data Backup and Related Teams

5.3.1. Data Backup Team

5.3.1.1. Responsible for overall planning, management and execution of data backup activities and providing regular reports to management on backup performance according to specific data backup metrics.

5.3.1.2. Support Activities:

5.3.1.3. Analyses data backup performance against specific metrics.

5.3.1.4. Sets backup priorities based on collaboration with IT Technical Support and user departments.

5.3.1.5. Provides management with ongoing status and performance data.

5.3.1.6. Works with vendors and IT Technical Support to ensure continuous operation of backups.

5.3.2. **IT Technical Support (ITS)Team**

Supports the performance of data backup and related data storage activities.

Support Activities:

5.3.2.1. Assist with data backup activities as needed.

5.3.2.2. Provide guidance on equipment, systems, and other services, as required.

5.3.2.3. Coordinate testing of data backup operations to ensure they are functioning normally, and that data can be restored in keeping with Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)

5.4. **Team Member Responsibilities**

5.4.1. Each team member will designate an alternate/backup.

5.4.2. All team members should keep an updated calling list of team members 'work, home, and cell phone numbers both at home and at work.

5.4.3. All team members should keep the backup plan for reference at home in case a disruption occurs after normal work hours.

5.4.4. All team members should familiarise themselves with the contents of the backup plan.

5.5. **Backup Policy**

All departments are responsible for specifying their data management, data retention, data destruction and overall records management requirements, and must:

5.5.1. Specify data management, data retention, data destruction and overall records management requirements.

5.5.2. Specify the recovery point objective (RPO) metric that defines how long data should be stored before it must be backed up again, and the recovery time objective (RTO) metric that defines the overall length of time an information system's components can be in the recovery phase before negatively impacting the organisation's mission or mission/business processes.

5.5.3. Establish data backup schedules which define what should be backed up, types of backups to be performed, storage locations for backed-up data and other resources, the frequency of backups, backup media to be used, time frames for executing backups, duration of backup storage, recovery of backed up data and systems, and a mechanism for confirming that backups were successful.

5.5.4. Perform Full and incremental backups to protect and preserve corporate network information such as databases, system logs, and all organisational data that are not easily replaced, have a high replacement cost, or are considered critical.

5.5.5. At a minimum, maintain two backup copies: one to enable on-site recovery and a second copy for vaulting to a secure off-site facility which is geographically separate from the original and isolated from environmental hazards.

5.5.6. Ensure backed-up data is secure and protected from unauthorised access.

5.5.7. Backup network components, cabling and connectors, power supplies, spare parts and relevant documentation and store same in a secure area on-site as well as at other corporate locations.

5.5.8. Test to ensure the recoverability of servers, network components, and other infrastructure devices, as well as critical applications, databases, and important files.

IT Technical Support follows these standards for data backup and archiving:

5.5.9. **System Databases**

5.5.9.1. A copy of the most current mission-critical databases must be made based on the frequency of changes and your organisation's Recovery Point Objective (RPO), i.e., the amount of data you can afford to lose per system.

5.5.9.2. Backups must be stored off-site.

5.5.9.3. The lead data administrator is responsible for this activity.

5.5.10. **Mission-Critical Data**

5.5.10.1. Current mission-critical data and databases must be backed up according to the established recovery point objectives (RPOs) and must be mirrored or replicated to secure backup locations within the RPO time frames.

5.5.10.2. Copies of backups must be stored off-site at one or more secure immutable cloud locations (disconnected from the network) or on an immutable media at an alternate company data centre or office, or a combination of these. It is a good practice to store 1 copy of backup data onsite to allow for timely recovery.

5.5.10.3. The lead data administrator is responsible for this activity.

5.5.11. **Non-Mission-Critical Data**

5.5.11.1. Current non-mission-critical data and databases must be backed up according to the established RPOs and can be mirrored or replicated to secure backup locations within the RPO time frames.

5.5.11.2. Alternatively, copies of current data and databases must be made based on RPO metrics and the frequency of changes made.

5.5.11.3. Copies of backups may be stored on-site in secure storage facilities or stored off-site at one or more secure cloud locations or at an alternative agency's data centre or office, or a combination of these.

5.5.11.4. The data administration team is responsible for this activity**.**

Backup media must be stored at locations that are secure, isolated from environmental hazards, and geographically separate from the location housing network components.

5.5.12. **Off-site Storage Procedures**

5.5.12.1. Tapes and disks and other suitable media are stored in environmentally secure facilities.

5.5.12.2. Tape or disk rotation occurs on a regular schedule coordinated with the storage vendor.

5.5.12.3. Access to backup databases and other data is tested at least annually.

5.5.13. **5.1.6 Tapes (if used)**

5.5.13.1. It is crucial to know the lifespan of backup tapes in use and to adhere to the manufacturer-specified temperature and other environmental conditions for the storage of tapes to ensure their reliability in data recovery efforts.

5.5.13.2. Tapes must be stored locally off-site.

5.5.13.3. The system supervisor is responsible for the transition cycle of tapes.

5.6. **Performing Data Backups**

Data backups are to be scheduled daily, weekly, and monthly depending on the nature of the backup. Data administrators are to use the approved data backup technology to prepare for, schedule, execute and verify backups. Backups may be made to local storage resources (e.g., disk, tape) locally and to off-site secure locations (e.g., cloud data backup service providers, backup-as-a-service providers) approved by IT management.

5.7. **Data Backup Activities**

The following table lists data backup activities to be performed on a regularly scheduled basis.

	Action	Who Performs
1.	Review the backup plan with IT management; secure approvals as needed	Lead data backup admin, Head of IT Ops
2.	Identify and categorise data to be backed up	Lead backup admin; backup team
3.	Identify and categorise systems to be backed up	Lead backup admin; backup team
4.	Identify and categorise other resources to back up	Lead backup admin; backup team
5.	Schedule backup activities, e.g., date, time, frequency, type of resource to back up, destination for backups	Lead backup admin; backup team

6.	Configure backup systems and resources according to schedule and plan	Lead backup admin; backup team
7.	Schedule tape backup and rotation activities	Lead backup admin; backup team
8.	Execute backups of data, systems, and other resources	Lead backup admin; backup team
9.	Ensure that tapes are secured for pickup and are properly labelled; verify pickup	Lead backup admin; backup team
10.	Verify that backups were completed, and all backed-up resources are unchanged	Lead backup admin; backup team
11.	Prepare and distribute backup reports	Lead backup admin; backup team
12.	Schedule and conduct tests of data backups	Lead backup admin; backup team
13.	Schedule and perform patching of backup resources	Lead backup admin; backup team
14.	Update backup systems and technologies as needed	Lead backup admin; backup team

5.8. **Data Recovery**

Procedures are to be established, documented, and periodically tested to recover data, databases, systems, applications and other information assets if a disruptive event occurs that necessitates the recovery of those assets and resources.

5.9. **Data Backup Plan Review and Maintenance**

The data backup plan must be reviewed periodically, and the procedures validated (and updated as needed) to ensure that backups will occur as needed and when needed. As part of this activity, it is advisable to review the listings of data backup team personnel, data backup service vendors and cloud data backup vendors, and update contact details as needed.

The hard-copy version of the data backup plan will be stored in a common location where it can be viewed by IT personnel, such as data administrators. Electronic versions will be available from IT Technical Support.

6. **Compliance**

This guideline shall take effect upon publication. Compliance is expected with all organisational guidelines, policies, and standards. Failure to comply with these guidelines may (at the full discretion of the Permanent Secretary or Administrative Head of the Public Sector Organisation) result in the suspension of any or all privileges and further action may be taken by the Ministry of Public Service.

7. **Exceptions**

Requests for exceptions to this guideline shall be reviewed by the Permanent Secretary, Administrative Head of the Public Sector Organisation, or the Policy Coordinator, NDMA. Departments requesting exceptions shall provide written requests to the relevant personnel. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a timeframe for achieving the minimum compliance level with the policies set forth herein.

8. **Definitions of Key Terms**

Term	**Definition**
3-2-1 Backup Strategy	The 3-2-1 backup is a time-tested data protection and recovery methodology for ensuring that data is protected adequately, and up-to-date backup copies of the data are available when needed.[1]
Backup	A copy of files and programs made to facilitate recovery if necessary. It refers to the copying of physical or virtual files or databases to a secondary location for preservation in case of equipment failure or catastrophe. [2]
Cloud backup, also known as online backup or remote backup,	A strategy for sending a copy of a physical or virtual file or database to a secondary, off-site location for preservation in case of equipment failure, site catastrophe or human malfeasance. [3]
Cyber Attack	Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. [4]
Data restore	The process of copying backup data from secondary storage and restoring it to its original location or a new location. [5]
Disaster	A disaster is any disruptive or catastrophic event (e.g., power outage, weather, natural disaster, vandalism) that causes an interruption in technology relating to data, databases, systems, archived data, and other resources provided by Government of Guyana's IT operations.
Removable media	Any type of storage device that can be removed from a computer while the system is running. [6]
Off-site backup	A method of backing up data to a remote server or to media that is transported off site. [7]
Recovery Point Objective (RPO)	The point in time to which data must be recovered after an outage. [8]
Recovery Time Objective (RTO)	The overall length of time an information system's components can be in the recovery phase before negatively impacting the organisation's mission or mission/business processes. [9]
Recovery Procedures	Actions necessary to restore data files of an information system and computational capability after a system failure. [10]

[1] https://www.techtarget.com/searchdatabackup/definitions#
[2] Retrieved from NIST Glossary of Terms https://csrc.nist.gov/glossary/term/backup
[3] https://www.techtarget.com/searchdatabackup/definitions#
[4] Retrieved from NIST Glossary of Terms https://csrc.nist.gov/glossary/term/cyber_attack
[5] https://www.techtarget.com/searchdatabackup/definitions#
[6] Ibid.
[7] Ibid.
[8] Retrieved from: NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/recovery_point_objective
[9] Retrieved from NIST Glossary of Terms https://csrc.nist.gov/glossary/term/recovery_time_objective
[10] Retrieved from NIST Glossary of Terms https://csrc.nist.gov/glossary/term/recovery_procedures

Tape backup	The practice of periodically copying data from a primary storage device to a tape cartridge so the data can be recovered if there is a hard disk crash or failure. [11]

9. Contact Information

Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

10. Effective Date

July 21st, 2023

11. Amendments

This guide will be updated periodically.

[11] https://www.techtarget.com/searchdatabackup/definitions#

Data Backup & Recovery Plan Guideline Appendixes

Appendix A: Data Backup Team Contact Lists

Data Backup Team (DBT)

Name	Address	Home	Mobile/Cell Phone

IT Technical Support (ITS) Team

Name	Address	Home	Mobile/Cell Phone

Appendix B: Approved Vendor Contact List

Name	Contact	Email	Mobile/Cell Phone
Backup vendor 1			
Backup vendor 2			
Backup vendor 3			

Appendix C: Data Backup Locations

Backup Resource 1 – <Location Name>

Primary: Address:
City:
Room:
Contact:

Alternate: Address:
City:
Room:
Contact:

Backup Resource 2 – <Location Name>

Primary: Address:
City:
Room:
Contact:

Alternate: Address:
City:
Room:
Contact:

Data Storage Facilities (e.g., Tape, Disk, Clouds, NAS, SAN, RAID)

Company Name	Contact	Work	Mobile/Cell Phone

Appendix D: Inventory of Data Resources, Databases to Back Up

Provide list of resources

Appendix E: Inventory of Hardware and Software to Back Up

Provide list of resources

Appendix F: Inventory of Network Services and Equipment Configuration to Back Up

Provide list of resources