DIGICALL

A12 - BACKUP AND DATA RECOVERY POLICY V1.3

DOCUMENT CLASSIFICATION	Internal Use Only
VERSION	1.3
DATED	01 September 2024
DOCUMENT AUTHOR	Ameet Ranchod
DOCUMENT OWNER	Johan Kriel

Approval

NAME	POSISTION	SIGNATURE	DATE
Donald Fraser	IT Security & Compliance Manager		03/10/2024
Ameet Ranchod	IT Infrastructure Manager		04/10/2024
Johan Kriel	Group CIO		09/10/2024

This policy supersedes and replaces all previous versions of this policy.

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
0.1	21.07.2021	Ameet Ranchod	Document Creation
0.9	21.07.2021	Ameet Ranchod	Final Draft
1.0	21.07.2021	Ameet Ranchod	Version 1.0
1.1	31.05.2022	Celeste Ramnarayan	Version 1.1
1.2	01.07.2023	Donald Fraser	Updated personnel & roles
1.3	01.09.2024	Donald Fraser	2024 Revision, template change

Table of Contents

1 Policy Scope

This policy applies to all Digicall Group staff that use, deploy, or support Digicall Group backup resources.

2 Policy Statement

Information Technology recognizes that the backup and maintenance of data for servers are critical to the viability and operations of the Digicall Group. It is essential that certain basic standard practices be followed to ensure that data files are backed up on a regular basis.

3 Purpose

The unprecedented growth in data volumes has necessitated an efficient approach to data backup and recovery. This document is intended to provide details on the stipulations of data backup and retrieval operations.

4 General

4.1 Procedure

1. The relevant regional Digicall IT Department and Back Office team should ensure that all backups are completed successfully, and failed backups should be restarted.
2. Logs should be maintained to verify the amount of data backed up and for unsuccessful backup occurrences.
3. Weekly system and file restore should be performed to ensure backup continuity & integrity.
4. Backups should be replicated from the primary datacentre to a secondary datacentre, on a schedule as defined in the Digicall Business Continuity Plan.

4.2 Backup Strategy

1. All backup data is stored on online media. No physical media is to be used to store backup data. Backup data is to be encrypted to comply with security requirements.
2. Virtual Machine Backups are to be performed on a two (2) hourly rotation and synchronized to a secondary location every four (4) hours.
3. Backups containing client data are retained for the following periods:
    a. Daily seven (7) Days
    b. Weekly four (4) Weeks
    c. Monthly two (2) Months
    d. Or longer where legislatively required.
4. Backups containing Digicall data are retained for the following periods:
    a. Daily seven (7) Days

b. Weekly four (4) Weeks
c. Monthly twelve (12) Months
d. Quarterly four (4) Quarters
e. Annually five (5) Years
f. Or longer where legislatively required.

4.3 Disaster Recovery Strategy

a. Disaster recovery infrastructure provides the ability to have a quick and efficient means of getting business back up and running in the event of a disaster.
b. Refer to the Digicall Business Continuity Plan for updated details, processes, and procedures to be followed to classify if an event is to be considered for Business Continuity.

5 Responsibilities

The IT Security and Compliance Manager is responsible for maintaining this policy and providing support and advice during its implementation in line with the IT Risk Management Policy

All Managers are personally responsible for implementing the policy and ensuring staff compliance.

Compliance with this Information Security and all subsequent policies is mandatory.

6 Policy Compliance Monitoring

6.1 Compliance

Group IT will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

If any user is found to have breached this policy, they may be subject to the Digicall Group's disciplinary procedures. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

6.2 Exceptions

Any exception to this policy must be approved by the Group Chief Information Officer in advance.

6.3 Non-compliance

All users (employees, contractors, vendors) are required to adhere to this Policy. Failure to comply may result in disciplinary action up to and including termination from employment, termination of contract, and civil penalties and/or criminal sanctions, depending on the circumstances.

6.4 Remediation of Non-compliance

Where non-compliance has been identified, dependent on the severity, criticality, and impact, opportunities may be provided to correct identified non-compliance. This corrective action will be evaluated on a case-by-case basis and timelines will be imposed and strictly enforced to ensure timeous remediation.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Human Resources Department or the IT Security and Compliance Manager.

7 Policy Governance

The following table identifies who within the Digicall Group is **Accountable, Responsible, Informed** or **Consulted** with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	IT Security and Compliance Manager
Accountable	Group Chief Information Officer
Consulted	IT Infrastructure Manager, Regional IT Infrastructure Managers
Informed	All Employees, All Temporary Staff, All Contractors, All Vendors and All Suppliers

8 Audit and Review Process

This policy and compliance there to, will be audited and reviewed internally at least once every 12 months depending on the changes or requirements within the group which will be reviewed by Management, or as required by significant changes in business operations or regulatory requirements.

For Group companies' pursuing certification, policies are required to be audited externally at least once in a 36-month cycle or sooner depending on changes or requirements within the group. Any employees or contractors with suggestions should refer these to their line manager in the first instance so they can be considered for implementation. Whenever changes are made to this policy the final draft will be shared with the Group CIO, IT Infrastructure Manager and the IT Security & Compliance Manager for review and approval before publication.

The IT Security and Compliance Manager will undertake annual policy reviews.

9 Appendices

None included with this policy.