DIGiCALL

A5 - GROUP INFORMATION SECURITY 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		05.09.2024
Ameet Ranchod	IT Infrastructure Manager		30/09/2024
Johan Kriel	Group CIO		24/10/2024

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

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
0.1	17.02.2021	Ameet Ranchod	Document Creation
0.9	17.02.2021	Ameet Ranchod	Final Draft
1.0	26.02.2021	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	01.08.2024	Donald Fraser	2024 Revision, updated template

Table of Contents

1 Policy Scope 4

2 Policy Statement 4

3 Purpose 4

4 General 4

5 Responsibilities 5

6 Monitoring, Measuring, Analysis, Evaluation and Remediation. 5

7 Policy Compliance Monitoring 5

7.1 Compliance 5

7.2 Exceptions 5

7.3 Non-compliance 5

7.4 Remediation of Non-compliance 6

8 Policy Governance 6

9 Audit and Review Process 6

10 Appendices 7

1 Policy Scope

This policy applies to all employees and contractors during the performance of company-related business and duties.

2 Policy Statement

This policy establishes the Digicall Group's position on information security management together with ensuring business continuity, and the management of the risk associated with handling customer data and reducing potential impact because of security incidents.

3 Purpose

The purpose of this policy is to protect the Digicall Group's informational assets (data stored on devices or magnetic, optical, or solid-state media; transmitted via fax, email, post, or voice; printed or written), against all internal, external, deliberate and/or accidental threats. The policies below are intended to assist in fulfilling this purpose.

4 General

The Group Chief Information Officer has approved this group information security policy.

As the Digicall Group has been considered as being risk averse, as per the Digicall Group Risk Management Policy, we assess, evaluate, remediate and or mitigate IT risk in line with our IT Risk Management Policy.

This Group Information Security policy ensures that the Information Security Management System's objective is defined as:

- Information will be protected against unauthorized access.
- Confidentiality of information will be assured.
- Integrity of information will be maintained.
- Availability of information for business purposes will be maintained.
- Legislative and regulatory requirements will be met.
- Business continuity plans will be maintained and tested.
- Information security training will be provided for all employees.
- All information security breaches will be reported to the Group Chief Information Officer / IT Security and Compliance Manager and will be thoroughly investigated.

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 directly responsible for implementing the policy and ensuring staff compliance.

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

6 Monitoring, Measuring, Analysis, Evaluation and Remediation.

System Logs will be collected, collated, and analysed automatically by the chosen SIEM tool. Evaluation will be performed weekly, and abnormalities will be investigated and remediated on the day identified. Non-conformities / violations are addressed in each policy and enforcement is carried out accordingly.

7 Policy Compliance Monitoring

7.1 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).

7.2 Exceptions

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

7.3 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.

7.4 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 Officer.

8 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

9 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.

10 Appendices

None included with this policy.