DIGICALL

A6 - ROLES AND RESPONSIBILITIES 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	20.02.2021	Ameet Ranchod	Final Draft
1.0	14.02.2021	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	01.09.2024	Donald Fraser	2024 Revision, template change

Table of Contents

1 Policy Scope

This policy applies to all Digicall Group companies, their employees and contractors involved in the management of company-related information assets.

2 Policy Statement

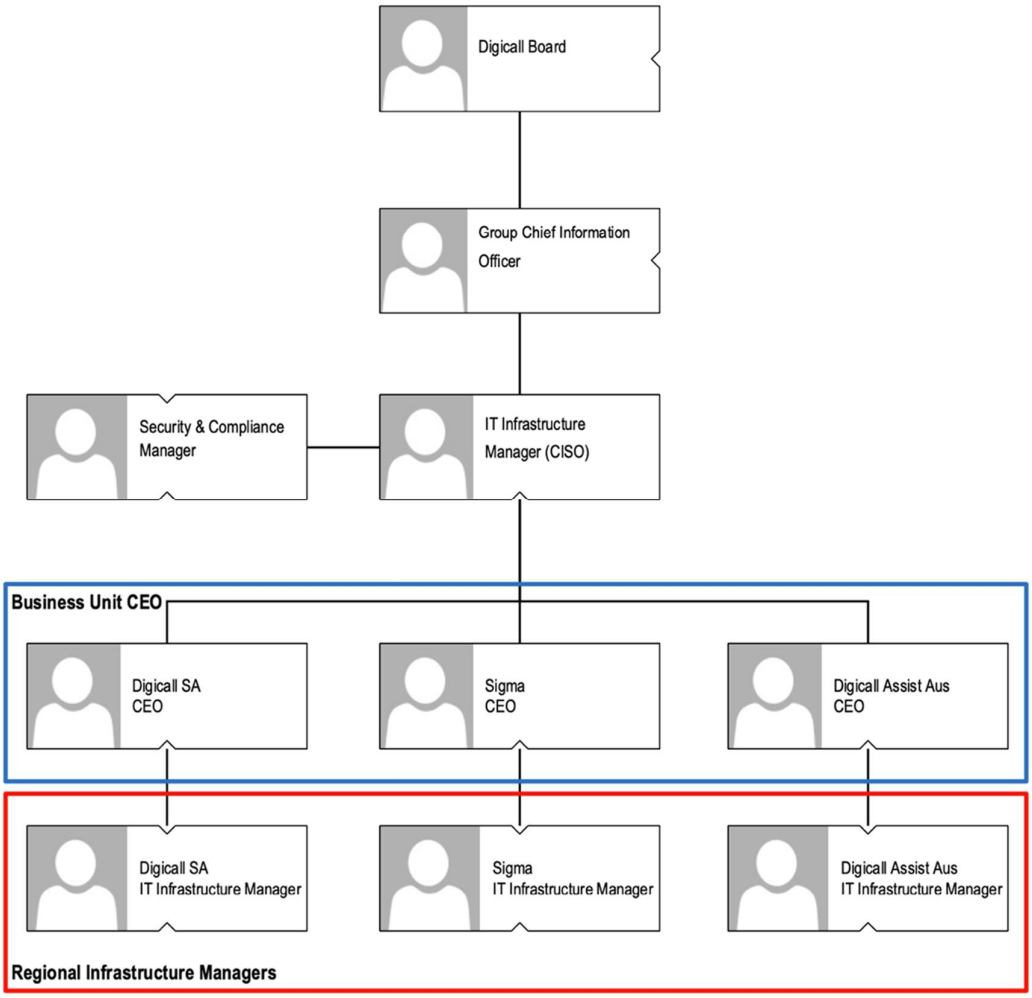
All information assets will be managed at the organisation level. The ownership of the information assets will reside with the organisation and individuals will be assigned and made responsible and accountable for these information assets. Specific individuals will be assigned with the ownership, custodianship or operational usage and support rights of the information assets.

3 General

Informational asset management responsibilities will be categorized as follows:

Entity	Responsibility
Digicall Board	Legal Owner
Group Chief Information Officer	Delegated Owner
IT Infrastructure Manager	Information Security Management
IT Security and Compliance Manager	IT Security Compliance and Enforcement
Business Unit CEO	Information Custodian
Regional IT Infrastructure Manager	Information Security and Enforcement
End Users	Staff, Contractors, Third Parties
Digicall Group Business Information Owners	Information Owner
Asset Custodians	Daily management of Information Assets

Information Security Roles and Responsibilities Logical Organogram:



4 Roles and Responsibilities

4.1 Digicall Board

The Digicall Board will be the legal owner of the information assets. No individual can claim Intellectual Property (IP) rights of an Information asset, unless and otherwise specifically agreed to and approved by the board in a contractual agreement.

4.2 Group Chief Information Officer

The Group Chief Information Officer ensures that strategic planning processes are undertaken so that information requirements, supporting systems and infrastructure are aligned to legislative requirements and strategic goals. The Group Chief Information Officer ensures that information security policies and governance practices are established to ensure the quality and integrity of the group's information resources and supporting IT systems. They oversee the development of tools, systems, and information technology infrastructure to maximise the access and use of the group's information resources.

1. The Group Chief Information Officer will have authority to represent the organisation for the protection and security of the information asset, as ownership of Information assets is delegated to this organisational role.
2. The Group Chief Information Officer and the IT Infrastructure Manager or the IT Security and Compliance Manager will approve the Group Information Security Policy, and all policies related to the Information Security Management System.
3. The Group Chief Information Officer may delegate full or partial ownership along with the defined responsibilities to any officer, contractor or third-party with operational rights and responsibility.

The Group Chief Information Officer is responsible for:

1. Interpreting the business and information needs and wants of the organisation and translating them into ICT initiatives.
2. Setting the strategic direction for information and communications technology and information management.
3. Ensuring that ICT and information management investment is aligned with the strategic goals of the organisation.
4. Ensuring that projects and initiatives are aligned and coordinated to deliver the best value.
5. Ensuring ICT planning is integrated into business planning.
6. Assist business units to define and understand their responsibilities in relation to information management.
7. Assist business units to identify their information needs and requirements.

8. Identifying opportunities for information sharing and cross-collaboration on projects and initiatives.

4.3 IT Infrastructure Manager

The IT Infrastructure Manager ensures that the information resources of the organisation are managed as a corporate asset and assists in establishing the strategic direction of information management for the organisation. They provide support and leadership to those responsible for managing information resources on a day-to-day basis.

The IT Infrastructure Manager will:

1. Assume the responsibilities of the Chief Information Security Officer.
2. Provide specialist advice relating to information management practices.
3. Contribute to the strategic direction of information management within the organisation.
4. Coordinate the development and implementation of information management practices including policies, standards, guidelines, procedures, evaluation, and review thereof.
5. Work with the Regional IT Infrastructure Manager(s) to plan and implement systems to effectively manage the group's information assets.
6. Reviews company IT Risk in line with the IT Risk Management Policy.

4.4 IT Security and Compliance Manager

The IT Security and Compliance Manager is responsible for developing, implementing, and reviewing information security policies designed to protect information and any supporting information systems from any unauthorised access, use, disclosure, corruption, or destruction.

The IT Security and Compliance Manager will:

1. Develop policies, procedures, and standards to ensure the security, confidentiality, and privacy of information, which is consistent with organisations Group Information Security Policy.
2. Monitor and report on any information intrusion incidents and activate strategies to prevent further incidents.
3. Work with IT Infrastructure Manager(s) to ensure that information assets have been assigned appropriate security classifications.
4. Ensure the information asset inventory register is maintained.
5. Identify the classification level of information asset.
6. Ensuring access is removed from those who no longer have a business need for the information.
7. Evaluate and review policies on a regular basis.

4.5 Infrastructure Backoffice Manager

1. Maintenance and upkeep of the asset as defined by the asset owner.
2. System Restart and recovery.
3. Implementing any changes as per the change management procedure.
4. Backup of the information.
5. Capacity and Availability management.
6. Defining and implementing appropriate safeguards to ensure the confidentiality, integrity, and availability of the information asset.
7. Assessing and monitoring safeguards to ensure their compliance and report situations of non-compliance.
8. Authorising access to those who have a business need for the information, and
9. Ensuring access is removed from those who no longer have a business need for the information.

4.6 End Users

1. Employees, Third Parties and Contractors authorised by the Information Custodians to access information and use the safeguards established by the Infrastructure Manager. Being granted access to information does not imply or confer authority to grant other users access to that information.
2. The users are bound by the Acceptable Use Policy.
3. All members of staff must read and acknowledge their understanding of Digicall's Information Security policy upon hire.
4. All members of staff must comply with Digicall's Information Security policy.
5. Upon termination, the member of staff's ongoing confidentiality responsibilities to Digicall will remain.
6. All members of staff are responsible for IT Security, particularly to their assigned accounts, passwords, and other authentication methods.

4.7 Digicall Group Business Information Owners

1. Identify and collect all sensitive data and personally identifiable information within their respective systems.
2. Describe the purpose(s) for which personally identifiable information is collected, used, maintained, and shared in its privacy notices.
3. Retain personally identifiable information for timelines identified in legislative or compliance specified record retention schedules to fulfil the purpose(s) identified in these schedules.
4. Dispose of, destroy, erase, and/or anonymize the personally identifiable information, regardless of the method of storage, in accordance with a legislative or compliance

specified record retention schedules and in a manner that prevents loss, theft, misuse or unauthorized access.

5. Use industry best practice techniques and guidelines for media sanitization, to ensure secure deletion or destruction of personally identifiable information (including originals, copies, and archived records).
6. Ensure terms of service and other contractual agreements satisfy the security and privacy requirements applicable to Digicall Group information systems and information for services for non-enterprise services obtained.
7. Assist with controlling access to sensitive data for prevention of loss and protection.

4.8 Management Responsibilities

1. Actively support security through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities.
2. Ensure that all information security roles and responsibilities are clearly allocated.
3. Ensure that the Information Security Policy and all supporting procedures have been effectively implemented for their areas of responsibility.
4. Identify and define positions of trusts to ensure that personal background checks are conducted accordingly.
5. Ensure that appropriate resources are applied to information security.
6. Management will review the ISMS on a periodic basis.

4.9 Asset Custodians

1. Responsible for the day-to-day management of Information Assets as per the classification assigned by the Information Owner.

4.10 IT Steering Committee (IT SteerCo)

1. Committee responsible for decision making relating to IT infrastructure and systems, consisting of at minimum the following members:

    - Group COO – Irene Nel
    - Group CIO - Johan Kriel
    - IT Infrastructure Manager - Ameet Ranchod

    Optional Members:

    - IT Security & Compliance Manager – Donald Fraser
    - Infrastructure Backoffice Manager - Jaco Van Tonder
    - Service Delivery Manager – Jacques Agenbach

All employees onboarded must be competent to comply with the responsibilities listed above commensurate to their role and the position description.

5 Segregation of Duties.

The execution and management of information technology assets, incidents and changes are limited to the Local and Group Information technology staff. For staff to gain access to information systems two levels of access needs to be obtained, the first being domain access which will solely be granted by the IT staff and the second being Line of business system access which will be granted by the non-IT business managers. Within the information system, different level of access control will be granted based on the role of the users. Within the information system segregation of duties will be applied to ensure that risks are managed.

6 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.

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.