DIGICALL

A18 - COMPLIANCE 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		04/10/2024
Ameet Ranchod	IT Infrastructure Manager		07/10/2024
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	17/03/2021	Ameet Ranchod	Initial Draft
0.9	17/03/2021	Ameet Ranchod	Final Draft
1.0	23/03/2021	Ameet Ranchod	Version 1.0
1.1	31.05.2022	Celeste Ramnarayan	Version 1.1
1.2	01.07.2027	Donald Fraser	Updated personnel & roles
1.3	01.08.2024	Donald Fraser	2024 Revision, updated template

Table of Contents

1 Introduction

1.1 Rationale

Digicall must ensure appropriate security controls that meet or exceed the compliance requirements associated with information assets, and provide the confidentiality, integrity and availability of the data for which the Digicall is responsible, are in place. Digicall Executive must have controls in place that provide reasonable assurance that security objectives are addressed.

1.2 Expected Objectives/Outcome

This policy articulates requirements that assist management in defining a framework that ensures compliance with the overall information security goals of Digicall including without limitation compliance with security-related laws, regulations, policies, standards and contractual provisions to which their IT resources and data are subject to.

1.3 Definitions

Term	Definition
Asset Owner	The manager of the business group that uses that information or system to perform a business task.
Intellectual Property	Represents creations of the mind or intellect that can be legally owned.
Privacy Impact Assessments (PIA)	Process which helps an organisation to identify and reduce the privacy risks of a project. An effective PIA will be used throughout the development and implementation of a project, using existing project management processes.
Risk Assessments	An on-going process of discovering, correcting and preventing security problems. The risk assessment is an integral part of a risk management process designed to provide appropriate levels of security for information systems.
System Security Plans	Provides an overview of the security requirements of the system and describe the controls in place or planned,

	responsibilities and expected behaviour of all individuals who access the system.
Risk Management Plans	A document that a project manager prepares to foresee risks, estimate impacts, and define responses to issues. It also contains a risk assessment matrix.
Business Continuity Plans	A plan to help ensure that business processes can continue during a time of emergency or disaster.
Independent Reviews	A review designed to give an independent assessment of the existing Information Security posture.

2 Principles

2.1 Compliance with Legal and Contractual Requirements

Information Owners are responsible for ensuring that legislative statutory, regulatory, policy and contractual requirements of each information system are:

a. Identified and documented when commencing a system development or enhancement initiative.
b. Reviewed prior to, or concurrent with, changes to legislation, regulation or policy.
c. Explicitly identified in contracts and service agreements, and included in:
    i. Privacy Impact Assessments
    ii. Risk Assessments
    iii. System Security Plans
    iv. Risk Management Plans
    v. Business Continuity Plans.

2.2 Intellectual Property Protection

Information Owners and Information Custodians must protect intellectual property by:

a. Ensuring that information and software is only acquired from reputable vendors.
b. Maintaining proof or evidence of ownership or right to use.
c. Adhering to the terms and conditions of use associated with intellectual property.
d. Ensuring the maximum number of users permitted is not exceeded.
e. Implementing processes to detect unlicensed information (e.g., ISO standards documents) and software or expired licences.

f. Requiring the removal of unlicensed information and software from information systems.
g. Informing employees of policies, including the “Digicall - Acceptable Use Policy”
h. Ensuring licensed intellectual property is securely removed from electronic media prior to media disposition; and,
i. Complying with terms and conditions for information and software obtained from public networks (e.g., “free for personal use only”, open source).

2.3 Compliance with Security Policies and Standards

Information Owners and Information Custodians must monitor information system usage to prevent, detect and respond to unauthorized or inappropriate use by:

a. Ensuring audit logs contain sufficient detail to detect and trace inappropriate usage.
b. Implementing processes to analyse audit logs to identify potential misuse of information systems.
c. Implementing system rules to prevent access to undesirable Internet sites.
d. Implementing content inspection and filtering tools (e.g., for e-mail and web traffic).
e. Immediately notifying employees of detected misuse.
f. Ensuring that security incidents are investigated in accordance with policy; and,
g. Determining, in consultation with Human Resources, if disciplinary action, including dismissal, cancellation of contract and/or other legal remedies are warranted for employees who have made unauthorized or inappropriate use of information system resources.

Prior to implementing information system monitoring processes, Information Owners and Information Custodians must ensure:

a. Monitoring activities are compliant with legislative, legal, policy and contractual requirements and obligations.
b. Employees are informed that specific activities may be monitored.

Access to data gathered through monitoring processes is restricted on a ‘need-to-know’ and ‘least privilege’ basis to the fewest possible number of users.

2.4 Information Security Reviews

Independent reviews are necessary to ensure the continuing suitability, adequacy and effectiveness of the organization’s approach to managing information security. The review must include assessing opportunities for improvement and the need for changes to the approach to security, including the policy and control objectives.

The CIO must initiate an independent third-party review of the Information Security Program every year including:

a. Assessing the operational effectiveness of the Information Security Program.
b. Documenting the results.
c. Reporting the results of the review to senior management.

Information Owners and Information Custodians must address the identified weaknesses and noncompliant controls prior to the next review.

Information Owners must ensure security policies and processes are implemented and adhered to by:

a. Conducting periodic self-assessments.
b. Ensuring employees receive regular information security awareness updates.
c. Initiating independent assessments, reviews or audits to assess compliance with policy.

When review processes indicate non-compliance with policies, Information Owners must:

a. Determine cause(s).
b. Assess the threats and risks of non-compliant processes.
c. Document the marginal risks where required.
d. Develop plans to implement corrective action.

Information Owners must develop an annual plan which identifies information systems scheduled for a security review in each fiscal year.

Information Owners and Information Custodians must ensure that recommendations from information incident reports are addressed.

The CIO may perform compliance reviews or audits of the implementation of recommendations from information incident reports, when necessary.

Information Custodians must regularly test information system technical control compliance by using automated tools to:

a. Detect network intrusion.
b. Conduct penetration testing.
c. Determine if information system patches have been applied.
d. Confirm that system technical controls have been implemented and are functioning as designed.
e. Perform technical compliance checking as part of the system change management process to verify that unauthorized connections and/or systems changes have not been made.

Line Managers responsible for technical compliance checking and Information Custodians must ensure that:

a. Information Owners and operations employees are consulted prior to initiating tests.
b. The Infrastructure Manager is notified prior to testing to prevent triggering false security alarms from the infrastructure.
c. Automated testing of operational systems is conducted by employees authorized by the CIO.

Line Managers responsible for technical compliance checking and Information Custodians must:

a. Assess results of testing and promptly develop action plans to investigate and mitigate identified exposures.
b. Provide Information Owners and the CIO with copies of test results and action plans.
c. Provide the CIO with the internal or external audit reports immediately upon receipt.
d. Maintain records, in accordance with established records schedules, of tests for subsequent review by internal and external auditors.

3 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.

4 Policy Compliance Monitoring

4.1 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).

4.2 Exceptions

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

4.3 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.

4.4 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.

5 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

6 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.

7 Appendices

None included with this policy.