DIGICALL

A14 - SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

DOCUMENT CLASSIFICATION	Internal Use Only
VERSION	1.4
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
1.0	06.05.2020	Ameet Ranchod	Version 1.0
1.1	13.11.2020	Ameet Ranchod	Template updated.
1.2	31.05.2022	Celeste Ramnarayan	Version 1.2
1.3	01.07.2023	Donald Fraser	Updated personnel & roles
1.4	01.09.2024	Donald Fraser	2024 Revision, updated template

Table of Contents

1 Introduction

1.1 Rationale

Maintaining a strong information security posture and managing information security risks relies on many disparate controls within infrastructure, operating environments and applications. The threats facing Digicall are changing, and security attacks are focussed on security vulnerabilities in software applications as opposed to infrastructure devices, hence there is an increased focus on the way applications are developed.

1.2 Expected Objectives/Outcome

The purpose of this policy is to set out the baseline requirements for information security within the System Acquisition, Development and maintenance lifecycle, to reduce the risk of vulnerabilities being introduced by applications acquired or developed internally by Digicall.

1.3 Definitions

Term	Definition
Threats	Anything that has the potential to cause serious harm to a computer system. A threat is something that may or may not happen but has the potential to cause serious damage. Threats can lead to attacks on computer systems, networks and more.
Vulnerabilities	A flaw in a system that can leave it open to attack. A vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat
Information Systems	Any system, service, or infrastructure, or any physical location that houses these things. A facility can be either an activity or a place; tangible or intangible
Electronic Signatures	Symbols or other data in digital form attached to an electronically transmitted document as verification of the sender's intent to sign the document.
Secure Programming Techniques	Practice of developing software where attention and planning are given to producing robust and reliable applications that operate securely

Secure Coding Standards	Practices to develop computer software in a way that guards against the accidental introduction of security vulnerabilities.
Operating Platforms	Any hardware or software used to host an application or service.
Test Data	Data which has been specifically identified for use in tests, typically of a computer program.
Penetration Testing	An attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities may exist in operating systems, services and application flaws, improper configurations or risky end-user behaviour.
Secure Code Reviews	Process of auditing the source code for an application to verify that the proper security controls are present, that they work as intended, and that they have been invoked in all the right places.

2 Principles

2.1 Security in Project Management

Information security objectives must be included in project objectives.

Risk assessments must be conducted in early stages of the project. The identified risks should be treated, and security measures implemented.

Information security policies must be an integral part of all stages of the project.

2.2 Security Requirements in Information Systems

2.2.1 Information Security Requirements Analysis and Specifications

Statements of business requirements for new information systems (developed or purchased), or enhancements to existing information systems, shall specify requirements for security controls.

Security controls in business requirements shall include:

a. Consideration of business value and legal-regulatory-certificatory standards for information assets affected by the new/changed system.
b. Consideration of administrative, technical, and physical controls available to support security for the information system; and
c. Integration of security controls early in requirements specification and system design.

2.2.2 Securing Application Services on Public Networks

The following controls for application services passing over public networks should be considered:

a. Level of confidence each party requires in each other's claimed identity.
b. Authorization processes on who can approve contents, issue or sign key agreements.
c. Requirements for confidentiality, integrity, proof dispatch and receipt of key documents.
d. Level of trust required in the integrity of key documents.
e. Protection requirements of confidential information.
f. Degree of verification to verify payment information supplied by a customer.
g. Liability of any fraudulent transactions; and
h. Insurance requirements.

2.2.3 Protecting Application Services Transactions

The following controls for application service transactions should be considered:

a. Electronic signatures should be used by each party.
b. Communication path is encrypted.
c. Communication protocols are secured.
d. Transaction details stored outside of any publicly accessible environment; and
e. Security is embedded throughout the entire end-to-end certificate/signature management process.

2.3 Security in Development and Support Processes

2.3.1 System Change Control Procedures

System change controls must follow the Change Management Policy for all changes in Digicall's environment.

2.3.2 Technical Review of Applications after Operating Platform Changes

When operating platforms are changed, applications should be reviewed and tested. The process should include:

a. Review of application control and integrity procedures.
b. Ensuring that notification of operating system change is done in a timely manner to allow time for rests and reviews to take place; and
c. Ensuring that the required changes to business continuity plans are made.

2.3.3 Restrictions on Changes to Software Packages

Vendor supplied software packages should be used without modification. If software package needs to be modified the following controls need to be considered.

a. Assess risks of built-in controls and integrity processes being compromised.
b. Check if consent of the vendor is required.
c. Assess the possibility of obtaining required change as a software update.
d. If Digicall becomes responsible for maintenance of software the impact needs to be assessed; and
e. Assess compatibility with other software.

2.3.4 Outsourced Development

The development of software by third parties shall be done under the supervision of Digicall.

The development of software by third parties shall be governed by a contract or a Service Level Agreement (SLA) that includes security requirements.

Security and code reviews shall be conducted by an individual with certified security training before bringing new services into production.

2.3.5 System Security Testing

It is the responsibility of Digicall to ensure that systems are regularly tested.

2.3.6 System Acceptance Testing

It is the responsibility of Digicall to ensure that system acceptance testing is performed by the respective teams which are affected by the change prior to deployment.

2.4 Test Data

The use of operational databases containing confidential information for non-production purposes shall be avoided, and test data shall be selected carefully, and appropriately logged, protected, and controlled, and shall be in line with the requirements as set out in *A12 - Operations Security.*

If confidential data or internal use only data must be used for testing purposes, all sensitive details and content shall be sanitized or modified beyond recognition prior to use.

All deviations to this policy must be approved by the CISO and / or CIO in writing.

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.

7 Appendices

None included with this policy.