DIGICALL

A12 - OPERATIONS SECURITY V1.4

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		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
1.0	06/05/2020	Ameet Ranchod	Version 1.0
1.1	11/11/2020	Ameet Ranchod	Updated Template
1.2	31/05/2022	Ameet Ranchod	Annual Review
1.3	01/07/2023	Donald Fraser	Updated personnel & roles
1.4	01.09.2024	Donald Fraser	2024 Revision, template change

Table of Contents

1 Introduction

1.1 Rationale

It is the responsibility of Digicall to have controls in place and in effect that provide reasonable assurance that the three guiding security principles, confidentiality, integrity and availability, are met. Digicall has the responsibility to exercise due diligence in the adoption of this framework. Agencies must achieve compliance with the overall information security goals including compliance with laws, regulations, policies and standards to which their technology resources and data, including but not limited to personal information, are subject.

1.2 Expected Objectives/Outcome

To outline the management and operational procedures to ensure the Confidentiality, Integrity and Availability of information while minimising the risks to the organisation. This segment ensures usability and that security controls can be maintained.

1.3 Definitions

Term	Definition
Asset Custodian	The manager of the group that administers and operates that information asset or system.
Asset Owner	The manager of the business group that uses that information or system to perform a business task.
Information Processing Facilities	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.
Change Administrator	Responsible for accurate, timely review and processing of CR/CO based on priority.
Capacity Management Processes	Processes to ensure that information technology resources are right sized to meet current and future business requirements in a cost-effective manner.
Critical Systems	Any system whose 'failure' could threaten human life, the system's environment or the existence of the organisation which operates the system. Also, any system which holds ‘Confidential’ data.

Risk Assessment	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.
Electronic Messaging Services	The creation, storage, exchange, and management of text, images, voice, telex, fax, e-mail, paging, and Electronic Data Interchange (EDI) over a communications network.

2 Principles

2.1 Operational Procedures and Responsibilities

2.1.1 Documented Operating Procedures

Information Custodians must ensure that approved operating procedures and standards are:

- Documented.
- Consistent with Digicall policies, standards and guidelines; and
- Reviewed and updated annually or when there are:
  - Alterations to building layouts,
  - Changes to equipment/systems located in the facility,
  - Changes in business services and the supporting information systems
  - Operations, and,
  - As part of any related security incident investigation.

2.1.2 Change Management

Changes to information processing facilities and systems must be controlled and follow the Change Management Policy. Extensions, modifications, or replacements to production operating system software and hardware must be made only if the written approval of the Change Administrator has been received in advance.

Where significant changes are made to production systems, a risk assessment of changes must be conducted.

Adequate roll back procedures must be developed for all changes to production systems.

All changes to information processing facilities must be communicated to all relevant personnel.

All network connections and changes to the firewall and router configurations must be tested and approved.

2.1.3 Capacity Management

Information Custodians are responsible for implementing capacity management processes by:

- Documenting capacity requirements and capacity planning processes.
- Identifying and managing storage requirements; Including capacity requirements in service agreements.
- Monitoring and optimizing information systems to detect impending capacity limits; and,
- Projecting future capacity requirements based on:
  - New business and information systems requirements,
  - Statistical or historical capacity requirement information, and,
  - Current and expected trends in information processing capabilities (e.g., introduction of more efficient hardware or software).

2.1.4 Separation of Development, Testing, and Operational Environment

Information Custodians must protect operational information systems by:

- Separating operational environments from development, testing, user acceptance, or any other non-production environments (e.g., using different computer rooms, servers, domains and partitions).
- Preventing the use of test and development identities and credentials for operational information systems.
- Storing source code (or equivalent) in a secure location away from the operational environment and restricting access to specified employees.
- Preventing access to compilers, editors and other tools from operational information systems.
- Using approved change management processes for promoting software from development/test to operational information systems.
- Prohibiting the use of personal or sensitive information as defined in *A8 - Information Classification Matrix and Handling Guide* in development, testing, user acceptance, or any other non-production environments

- Restricting access to production, development, test, or training systems as defined in *A14 - Secure Coding Matrix*.

2.2 Protection from Malware

2.2.1 Controls against Malware

Detection and prevention controls to protect against malicious software (antivirus) and appropriate user awareness procedures must be implemented on all systems across Digicall.

Any installed anti-virus must be configured to comply with the following at minimum:

- Download and install updates automatically as required
- Perform periodic scans
- Log all activities
- Ensure that the primary user cannot close the application

The reporting of actual or suspected malicious code incidents must be recorded in-line with the Digicall Incident Management Policy.

2.2.2 Information Backup

Digicall must ensure that back-up facilities are provided, backup strategies with system owners are developed and copies of essential business information and software are taken regularly.

All sensitive, valuable, or critical information must be backed up on a regular basis which would include but not limited to daily, weekly, monthly incremental backups and full annual back up.

All sensitive, valuable, or critical information recorded on backup media and stored outside Digicall offices must be given an appropriate level of physical and environmental protection.

A documented backup and restore procedure must be developed, and be easily accessible at all times.

Critical business information and critical software archived on computer storage media for a prolonged period must be tested at least annually.

2.3 Logging and Monitoring

2.3.1 Event Logging

For critical systems (e.g., those containing PII) audit logs must be produced which show production application start and stop times, system boot and restart times, system

configuration changes, system errors and corrective actions taken, and confirmation that files and output were handled correctly.

Audit trails must be retained for at least one year, with a minimum of three months available online.

All access to customer data must be audited and logged in a secure location. This includes access to raw and encrypted files.

2.3.2 Protection of Log Information

All system and application logs must be maintained in a form that cannot be readily viewed by unauthorised personnel and stored in a secure manner.

Authorised persons have a readily demonstrable need for access to perform their regular duties. All others seeking access to these logs must first obtain written approval.

Current audit trails must be promptly backed up to a centralised log server or media that is difficult to alter.

File integrity monitoring or change detection software must be used to ensure that existing audit log trail data cannot be changed without generating alerts.

2.3.3 Administrator and Operator Logs

Activities of administrators and operational staff must be logged. These logs must be kept, managed and should not be altered by anyone. These logs are subject to regular and independent checks.

2.3.4 Clock Synchronisation

All systems and devices must have system clocks and other times synchronised to the correct time using NTP or similar technology.

Access to time data must be restricted to only personnel with a business need and changes to the time settings on critical systems must be logged.

2.4 Control of Operational Software

2.4.1 Installation of Software on Operational Systems

Information Owners and Information Custodians must implement procedures to control software installation on operational information systems providing services to ensure that:

- Operations employees and end users have been notified of the changes, potential impacts and if required have received additional training.
- New releases of software are reviewed to determine if the release will introduce new security vulnerabilities.
- Modifications to operational software are logged.
- Development code or compilers are not present on operational information systems; and,
- Vendor supplied software is maintained at the supported level.

2.5 Technical Vulnerability Management

2.5.1 Management of Technical Vulnerabilities

Information Custodians must establish processes to identify, assess and respond to vulnerabilities that may impact information systems by:

- Monitoring external sources of information on published vulnerabilities.
- Assessing the risk of published vulnerabilities.
- Testing and evaluating options to mitigate or minimize the impact of vulnerabilities.
- Applying corrective measures to address the vulnerabilities.
- Completing a Security Threat and Risk Assessment to verify the risk has been mitigated; and,
- Reporting to the CISO and / or CIO on progress in responding to vulnerabilities.

2.5.2 Restrictions on Software Installations

Software installation must be consistent with the requirements of the Digicall Acceptable Use Policy.

2.6 Information Systems Audit considerations

2.6.1 Information Systems Audit Controls

Audits of operational systems must be planned and agreed to minimise the risk of disruptions to business processes. Audit requirements, scope and access other than read only must be authorised by Digicall and adequate resources must be provided. Procedures, requirements, responsibilities must be documented, and all access must be monitored and logged.

2.6.2 Protection of Information System Audit Tools

Access to system audit tools must be protected to prevent possible misuse or compromise and be separated from operational and development systems.

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 and criticality and possible 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.