DIGICALL

A15 - SUPPLIER RELATIONSHIPS

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	24.02.2021	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	01.07.2023	Donald Fraser	Updated personnel & roles
1.3	01.08.2024	Donald Fraser	2024 Revision, updated template

Table of Contents

1 Introduction

1.1 Rationale

The high degree of standardization and interconnectedness in information processing has fostered the need for many external service providers. However, the security risks associated with service providers also have an impact on an organization's own infrastructure.

1.2 Expected Objectives/Outcome

The supplier relationships policy sets out the conditions that are required to maintain the security of Digicall assets. Suppliers may be required to use, create, access and store Digicall assets (information or equipment).

1.3 Definitions

Term	Definition
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.
Critical Components	Services, systems which if made unavailable can have a detrimental effect on Digicall's main service offerings.
Service Management Relationship Process	Activities directed by policies, organized and structured in processes and supporting procedures that are performed by Digicall to design, plan, deliver, operate and control information technology (IT) services supplied by suppliers.

2 Principles

2.1 Information Security in Supplier Relationships

2.1.1 Information Security Policy for Supplier Relationships

A Digicall third party evaluation process must exist to assess external parties that will provide services to Digicall. The following elements must be considered during the supplier evaluation process:

a. Third party financial status (i.e., annual turnover).

b. The effect of the contract (that will be signed between the two parties) on the third-party turnover.
c. Third party reputation and client portfolio.
d. Third party organisational structure, personnel profile/workforce, resumes for all IT professional services, consultative services or other service-related engagements and demonstrated domain capability/expertise.
e. Third party insurances.
f. Third party Quality Assurance and quality control framework (includes compliance with policies, standards, procedures and guidelines and formal accreditations, for example ISO9001).
g. The ability of the third party to comply with national and international statutory and regulatory requirements e.g., PCI DSS and privacy legislation.
h. The reliability, security and effectiveness of third-party IT systems.
i. The completeness of third parties technical support procedures (with respect to the offered services including review of offered SLA and KPI).
j. Third Party business continuity and disaster recovery plans.

Where there is a business need to provide external parties access to Digicall information facilities, a risk assessment is to be carried out to identify requirements for specific information security measures. Alternatively, Digicall may include clauses in contracts with external parties to mandate the security controls required.

The risk analysis will consider the type of access required, the value of the information, the information security measures employed by the external party and the implications of the access for the security of Digicall information and information systems. As part of the risk assessment the “Digicall Vendor Compliance Check” is completed by third parties providing details around their information security management system and control environment.

Access to Digicall facilities or data by external parties is not provided until the appropriate measures have been implemented and an agreement has been signed defining the terms and conditions for the connection.

The Digicall IT team is responsible for performing the risk assessments and evaluating third party’s security control environment.

An external party can demonstrate their information security credentials to Digicall in one of the following ways:

a. Certification—if the external party can produce a current certificate showing compliance to the relevant standard, ISO 27001, with a relevant scope, then they may be considered to have complied with this requirement.
b. External Audit—if the external party has had their information security policies and practices audited by a trusted and independent organisation, and they are able to

deliver a satisfactory report of that audit, then they may be considered to have complied with this requirement.

A third-party inventory must exist which describes the services provided along with the criticality of each third party (e.g., High/Medium/Low) based on the results of the risk assessment.

Contravention of the security conditions stipulated in the third-party contract can result in a breach of said contract and termination of services with immediate effect.

2.1.2 Addressing Security within Supplier Agreements

Digicall staff, responsible for agreeing contracts must ensure that the terms and conditions do not contravene the Information Security Management System (ISMS). In any event all contractual documents must be forward to the Digicall Legal department for vetting prior to signature by an authorised representative of Digicall.

All Digicall contracts must ensure boundaries of undertakings and protection of Digicall assets for the full duration of the contracted services. Contracts and services must:

a. Be monitored and reviewed annually to ensure that information security requirements are being satisfied.
b. Include appropriate provisions to ensure the continued security of information and systems if a contract is terminated or transferred to another supplier.
c. Be able to demonstrate compliance with Digicall's ISMS.
d. Include an undertaking that Digicall assets will be retained or transferred to Digicall upon completion of contracted works and that any sensitive data will be removed from the service provider's data sources.
e. Ensure the contract/agreement states Digicall data being transferred will only be used for the purposes of the collaboration and no data will be transferred to any third parties for any other purposes.
f. Include a right to audit clause on non-certified suppliers. Digicall must ensure the right to audit is agreed with the contracted service prior to acceptance of the contract.

2.1.3 Information and Communication Technology Supply Chain

All Digicall contracts must ensure boundaries of undertakings and protection of Digicall assets from security risks associated with information and communications technology services and product supply chain. Contracts and services must consider the following topics concerning supply chain security:

a. Additional information security requirements to be applied to information and information technology product or service need to be defined.

b. Monitoring acceptable methods to validate the delivered information and communication technology products needed to be implemented to make sure services are adhering to the stated security requirements.
c. A process needs to be implemented to identify the suppliers which are critical to maintain functionality and therefore require increased attention and scrutiny.
d. Obtaining assurance that critical components and their origin can be traced throughout supply chain.
e. Rules for the sharing of information regarding the supply chain and any potential issues need to be defined.
f. A process to manage information and communication technology component lifecycle and availability and associated risks needs to be defined.

2.2 Supplier Service Delivery Management

2.2.1 Monitor and Review of Supplier Services

A service management relationship process between Digicall and the suppliers is required to:

a. Monitor service performance levels to verify adherence to the agreements.
b. Review service reports produced by the supplier and arranged regular progress meetings.
c. Conduct audits of suppliers and review audit reports of independent auditors.
d. Provide information about security incidents as required by the agreements and supporting guidelines and procedures.
e. Review supplier audit trails and information security events records.
f. Ensure supplier maintains service capability with workable plans to ensure the agreed service continuity levels are maintained following major service failures or disasters.

Suppliers must be reviewed annually as per Supplier Relationship Agreement Register spreadsheet is to be updated.

2.2.2 Managing Changes to Supplier Services

Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and reassessment of risks.

The following changes need to be taken into consideration.

a. Changes to supplier agreements
b. Enhancements to the current services offered.
c. Development of any new applications and systems.
d. Modifications or updates of Digicall's policies and procedures.

e. New or changed controls to resolve information security incidents and to improve security.
f. Changes and enhancements to networks.
g. Use of new technologies.
h. Adoption of new products or newer versions.
i. Change to physical location of service facilities.
j. Change of suppliers.

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.