DIGICALL

A12 - DATA LOSS PREVENTION 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		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
0.1	17.02.2021	Ameet Ranchod	Document Creation
0.9	23.02.2021	Ameet Ranchod	Final Draft
1.0	02.03.2021	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, removed indicators of compromise.
1.3	01.09.2024	Donald Fraser	2024 Revision, template change

Table of Contents

1 Policy Scope

This policy applies to Digicall Group IT Department staff tasked with developing, maintaining and implementing IT processes and procedures. It also applies to Digicall Group Business Information Owners.

2 Policy Statement

Legislation and compliance require the Digicall Group to implement policies and procedures that provide for information security. Information security entails ensuring appropriate controls and measures are in place to protect the confidentiality, integrity, and availability of Digicall Group information. The Digicall Group has categorized its information by sensitivity and protection needs based on legislative and compliance requirements.

Differing information sensitivity requires varying controls that adequately protect its confidentiality, integrity and availability while enabling maximum use given its threat environment. The "loss" of information is defined as the compromise of its confidentiality, when information is inappropriately removed from, shared, or otherwise "leaked" from authorized to unauthorized systems, whether intentionally or unintentionally.

3 Purpose

This policy addresses the risk of intentional and unintentional leakage of Digicall Group classified information assets. This policy does not address risks of equipment failure, business continuity or disaster recovery.

4 General

1. Digicall Group documents containing sensitive information will be marked with an embedded security classification to facilitate technical measures within boundary controls to prevent data loss and indicate to information users its classification and handling requirements.
2. The following boundary controls will implement technical measures to prevent data loss:
    a. Email attachment filters (outgoing).
    b. Internet/web traffic filters (outgoing).
3. Data at rest on portable computers will be protected from theft/loss by use of assured encryption. (See the Digicall Group Data Encryption Policy).
4. Data at rest on portable data storage devices will be protected from theft/loss by use of assured encryption. (See the Digicall Group Data Encryption Policy).
5. Boundary controls shall be cognizant of the levels of classification that are/are not appropriate for each egress path. For example, some classifications may be permitted

for transmission over secure email systems, or for upload to secure websites within the Digicall Group network.

6. Boundary controls will block content that obfuscates electronic security classifications by encryption (e.g., zipped files).

5 Processes and Procedures

5.1 Discovery

1. Data discovery identifies what the data is, where it resides and how it is utilized. This information is used to define data characteristics, data types and data classifications further. Discovery results also assist with the identification of sensitive data. Metadata that results from the data discovery is integrated into the DLP policy.

5.2 Monitoring

1. Monitoring shall occur on a continuous basis and information gathered shall be used to refine data characteristics and classifications.
2. DLP systems will monitor information in-use, in-transit, and at-rest for indicators of compromise and policy and procedure violations. The system should be an active, as opposed to a passive, system:
    a. In-use sensitive information
        i. Monitoring endpoints used by Digicall Group personnel and contractors in their day-to-day use of Digicall Group data (e.g., servers, desktops, laptops, mobile devices, personal devices, removable media, etc.).
    b. In-transit sensitive information
        i. Monitoring information transmitted between endpoints both internal and external endpoints (e.g., cloud providers, email, mobile, network, social media, web).
        ii. Network monitoring shall be at the Digicall Group enterprise network boundary points and at internal enterprise network points separating networks or systems of different categorization or sensitivity and at other points as determined by risk analyses. Network traffic, to include encrypted traffic, shall be examined to prevent the loss of sensitive data or violation of digital rights.
    c. Storage level (at-rest) sensitive information
        i. Monitoring storage devices (e.g., cloud providers, collaboration servers, databases, removable media, servers, etc.). Storage devices shall be annually scanned to ensure sensitive data categories are stored on approved devices with an appropriate level of security controls.

3. System owners shall implement commensurate security controls and approved devices and capabilities and coordinate with Digicall Group IT to implement and maintain interoperability with the DLP solution.
4. Relevant regional Digicall Group IT Departments will control access to sensitive data for prevention of loss and protection. Access to sensitive data shall be granted under the concepts of 'least-privilege' and 'need-to-know'. These concepts shall be enforced by:
    a. Performing regular audits of access controls,
    b. Reviewing privileged user access and
    c. Responding to DLP indications of compromise and policy and procedures violations.
    d. Refer to policy number *A9 Account and Identity Management Policy* for details relating to how and when this is maintained.

5.3 Protection

1. Digicall Group controls are in place to minimize loss of data. These controls address the common data use cases: in-use, in-motion, at-rest, and loss modes including but not limited to destruction, disappearance, leakage, and theft.
    a. Sensitive information shall not be downloaded to storage devices or stored in locations not approved for that information type.
    b. Large volumes of sensitive information shall not be downloaded from Digicall Group systems or transmitted outside the Digicall Group enterprise network without explicit approval from the Group CIO.
    c. Sensitive information shall be handled in a manner consistent with Digicall Group information security procedures.
    d. Personally identifiable information shall be handled in a manner consistent with Digicall Group's privacy procedures. Sensitive personally identifiable information shall not be transmitted outside of the Digicall Group without explicit approval from the Group CIO.
    e. Users shall only have access to information for which they have a business need-to-know and appropriate clearance.
    f. Only devices approved for use by Digicall Group shall be used to process, store, or transmit Digicall Group information.
        i. The capability to process, store or transfer data to writable media or external devices on systems that do not require that capability for business purposes shall be disabled. For example, networked servers in a data centre may be configured without Universal Serial Bus (USB) ports. In addition, in situations where identified risks prohibit their use, the ability to use writable media or external devices will be disabled on systems used in that situation. For example, disabling USB ports on

laptops when travelling to high-risk locations. (Refer to the Digicall Group's Mobile Device Acceptable Use Policy and Data Encryption Policy).

ii. The relevant regional Digicall Group IT Department shall validate the authenticity of devices being used on the Digicall Group network.

g. Digicall Group information shall only be encrypted using Digicall Group approved encryption standards (refer to the Digicall Group's Data Encryption Policy). Digicall Group employees, contractors and all other users of Digicall Group data and information systems are prohibited from using unauthorized encryption capabilities to encrypt Digicall Group information.

h. Information systems that could write or store information on removable media (e.g., CDs, DVDs, USB drives) shall employ a mechanism that automatically encrypts the information stored on those devices using Digicall Group approved encryption standards when the storage devices are not an approved type that does the encryption natively.

i. Digicall Group's Acceptable Use Policy, Mobile Device Acceptable Use Policy, Data Encryption Policy and Account and Identity Management Policy shall be followed to minimize potential data loss resulting from personnel changes.

5.4 Response to Indicators of Compromise or Violation of Policies and Procedures

1. Indicators of compromise and violation of policies and procedures shall be treated as and reported as an information security incident. Incident reporting shall conform to procedures outlined in Digicall Group's Incident Management Policy.
2. Information transmissions and downloads that violate policies and procedures shall be blocked.
3. Sensitive information discovered on unapproved storage devices and on approved devices in violation of policy shall be removed from those devices moved to approved and appropriate devices.

5.5 Awareness

An effective DLP program depends upon an informed user community. Awareness is an element of the DLP program. DLP awareness training will be offered in two ways: 1) stand-alone classes on DLP, and 2) DLP capabilities will be interwoven into other Digicall Group training initiatives as appropriate.

6 Responsibilities

Information owners have the following responsibilities with respect to data protection:

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.

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 Manager.

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.