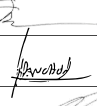
DIGICALL

A8 - ASSET MANAGEMENT POLICY V1.2

DOCUMENT CLASSIFICATION	Internal Use Only
VERSION	1.2
DATED	01 September 2024
DOCUMENT AUTHOR	Ameet Ranchod
DOCUMENT OWNER	Johan Kriel

Approval

NAME	POSISTION	SIGNATURE	DATE
Donald Fraser	IT Security & Compliance Manager		05.09.2024
Ameet Ranchod	IT Infrastructure Manager		30/09/2024
Johan Kriel	Group CIO		24/10/2024

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	02.03.2021	Ameet Ranchod	Final Draft
1.0	31.05.2022	Celeste Ramnarayan	Version 1.0
1.1	01.07.2023	Donald Fraser	Updated personnel & roles
1.2	30.05.2024	Donald Fraser	2024 Revision, template change

Table of Contents

1 Introduction

1.1 Rationale

Asset management should ensure that Digicall assets are identified, accounted for, and have a nominated owner assigned who is responsible for ensuring that the information asset is appropriately secured and protected. The owner may delegate the implementation of specific controls; however, the owner will remain responsible for the protection of the asset.

Digicall assets include software assets, hardware assets and licences, as well as the information and data stored on these assets.

1.2 Expected Objectives/Outcome

This policy establishes the requirements for assigning ownership and tracking for all Digicall's IT assets and provides the control requirements for Digicall to validate the IT assets deployed throughout the business.

1.3 Definitions

Term	Definition
Information Asset	Means all data owned by or entrusted to Digicall, including, but not limited to: ● Data stored on computers, disks, and in storage. ● Data transmitted across the networks. ● Information printed or written on paper. Spoken in conversations, in person, or over the telephone
IT Assets	Including, but not limited to information, software, desktop computers, laptops, mobile devices, network equipment and servers.
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.

'Need to Know' Principle	The principle means giving a user account only those privileges which are essential to perform its intended function.
Information Classification	The process of assigning an appropriate level of classification to an information asset to ensure it receives an adequate level of protection.
Removable Media	Any type of storage device that can be removed from a computer while the system is running. Examples of removable media include CDs, DVDs and Blu-Ray disks, as well as diskettes, USB drives, external hard drives, and memory cards. Removable media makes it easy for a user to move data from one computer to another.
Sensitive Information	Information which is classified as 'Internal', 'Client Confidential' or 'Confidential'

2 Principles

2.1 Responsibility for Assets

2.1.1 Inventory of Assets

An inventory of IT assets should be maintained and reviewed every twelve (12) months to confirm completeness. The inventory must include hardware, software, and information assets.

2.1.2 Ownership of Assets

i. Owners and custodians must be assigned to all important assets identified and recorded in the asset register.
ii. Asset owners should determine appropriate classification levels for their information assets and make decisions about who will be permitted to access and use the information.
iii. Asset owners are responsible for maintaining the classification labelling.
iv. The 'need to know' principle should be applied to all assets.
v. Asset Custodians are responsible for defining specific security control procedures, implementation and maintenance measures for the controls, and recovery capabilities consistent with the instructions of the asset owner.

2.1.3 Acceptable Use of Assets

All users are required to maintain their use in alignment with the Acceptable Use Policy.

This policy outlines the level of use considered approved by Digicall management and includes the use of any electronic system and information.

2.1.4 Return of Asset

Any IT assets owned by Digicall that is assigned to a user (an employee or contractor) must be returned upon the termination of user's employment to their Line Manager. It is the Line Manager's responsibility to ensure all assets are returned on the last day of a user's employment.

2.1.5 Asset Lifecycle

Assets are reviewed on an ongoing basis. Due to the economic environment, it is not possible to refresh assets according to a set schedule and therefore assets are replaced on an as and when needed basis. Assets are also to be reviewed on a departmental and hierarchical level.

2.2 Information Classification

2.2.1 Classification of Information

i. All information assets (both physical and electronic formats) should be classified as per the Information Classification Matrix and Handling Guide.
ii. The authority to reclassify information assets belongs to the Information Owner.
iii. Parties who may encounter Digicall information are expected to familiarise themselves with the Information Classification Matrix and Handling Guide, and to consistently use it in their business activities.

2.2.2 Labelling of Information

Information must be labelled in a consistent manner to facilitate the identification of the information classification.

2.2.3 Handling of Assets

i. It is important that information is handled appropriately when it is distributed, transmitted, stored, or disposed of securely, as per the Information Classification Matrix and Handling Guide.
ii. Information that has not been assessed, and for which the classification cannot be readily determined, should be classified as Confidential until otherwise assessed.
iii. Physical confidential information should reside in an access controlled or lockable storage room.
iv. Confidential information must not be sent externally or removed from Digicall premises, without the prior authorisation of Information Owner.
v. The loss, or potential loss, of any Confidential information externally, must be reported to the IT Security and Compliance Manager immediately so that appropriate action can be taken to protect Digicall at the earliest opportunity.

2.3 Media Handling

2.3.1 Management of Removable Media

i. Authorisation must be required for all media removed from the organisation and a record of all such removals must be kept.
ii. All media must be stored in a safe and secure environment in accordance with the classification of the data stored on the media.
iii. Remote users who do not have access to the Digicall network or systems must ensure that data which is backed-up to removable media must be encrypted and stored in a secure manner, in accordance with the classification of the data stored on the media. This should be determined with Information Owner.

2.3.2 Disposal of Media

i. Media must be disposed of securely and safely when no longer required.
ii. The destruction of sensitive information must be carried out by authorised Digicall personnel or a suitable destruction contractor. Disposal of sensitive information must be logged to maintain an audit trail.
iii. Physical media that is no longer required must be either physically destroyed, degaussed, or the data must be rendered irretrievable using sanitisation software. For hard-copy materials, acceptable methods include but are not limited to cross-cut shredding, incineration, and pulping.
iv. Outsourced destruction of tape media containing confidential or sensitive information must use a bonded Disposal Vendor that provides a “Certificate of Destruction.”

2.3.3 Physical Media Transfer

i. Reliable transport or couriers must be used for the transfer of physical media.
ii. A list of authorised couriers should be created and agreed with Management.
iii. Prior to handing over media to couriers their identity needs to be verified.
iv. Media must be adequately packaged to protect from any physical damage during transit.
v. Logs which stipulate the content of the media, the protection applied, and time of transit and receipt must be maintained.

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 Officer.

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.