DIGICALL

A11 - PHYSICAL AND ENVIRONMENTAL SECURITY POLICY V1.7

DOCUMENT CLASSIFICATION	Internal Use Only
VERSION	1.7
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	28.01.2019	Justus Boyens	Document Creation
0.9	29.01.2019	Justus Boyens	Final Draft
1.0	05.02.2019	Justus Boyens	Version 1.0
1.1	04.02.2020	Ameet Ranchod	Annual Review
1.2	17.03.2020	Ameet Ranchod	Changes to responsibilities
1.3	19.03.2020	Ameet Ranchod	Amendments to Review, Added Policy Compliance Monitoring and Policy Governance
1.4	16.10.2020	Ameet Ranchod	Corrections to surveillance recordings to be in line with current business process and updated template
1.5	31.05.2022	Ameet Ranchod	Annual Review
1.6	01.07.2023	Donald Fraser	Updated personnel & roles
1.7	01.09.2024	Donald Fraser	2024 Revision, template change

Table of Contents

1 Policy Scope 5
2 Policy Statement 5
3 Purpose 5
4 General 5
4.1 Secure Areas 5
4.2 Physical Security Perimeter 5
4.3 Secure Area Controls 6
4.4 Secure Offices, Rooms and Facilities 6
4.5 Access to Restricted Facilities 7
4.6 Requests for Access 7
4.7 Approved Access Control Systems 7
4.8 Access Control Process 7
4.9 Key Access and Card Systems 7
4.10 Visitor and Guest Access 8
4.11 Confidential Area Access 8
4.12 Digicall Group security staff shall: 9
4.13 Physical Site Access 9
4.14 Contractor Requirements 9
4.15 Audit Controls and Management 10
4.16 Security of Equipment Off-Premises 10
4.17 Secure Disposal or Re-use of Equipment 10
4.18 Cabling Security 10
4.19 Equipment Siting and Protection 11
4.20 Supporting Utilities 11
4.21 Protecting against External and Environmental Threats 11
4.22 Delivery & Loading Areas 12
5 Responsibilities 12
6 Policy Compliance Monitoring 12
6.1 Compliance 12
6.2 Exceptions 12
6.3 Non-compliance 12
6.4 Remediation of Non-compliance 13

7 Policy Governance 13
8 Audit and Review Process.....13
9 Appendices.....14

1 Policy Scope

This policy applies to all employees and contractors during the performance of company related business and duties.

2 Policy Statement

Management, technical support staff, system administrators, and security personnel are responsible for facility access requirements. The management and monitoring of physical access to facilities is extremely important to Digicall Group security and helps maintain information as well as employee safety.

3 Purpose

This policy establishes rules for management, control, monitoring, and removal of physical access to Digicall Group facilities.

4 General

4.1 Secure Areas

For all Digicall facilities, the subdivision of the facility that houses sensitive information assets must be defined as a Secure Area. Based on the classification as a Secure Area, additional physical security measures for example barriers such as walls, card-controlled entry gates, keyed doors or staffed reception desks must be implemented to provide adequate protection for specific types of confidential information housed there.

4.2 Physical Security Perimeter

Security perimeters should be used to protect areas that contain information and information processing facilities -- using walls, controlled entry doors/gates, staffed reception desks and other measures. Control includes:

a. Perimeter siting and strength determined by risk assessment.
b. Clearly defined and marked perimeters, except in situations where hidden/disguised perimeters would enhance security.
c. Use of physically sound walls, windows, and doors, protected with bars, locks, alarms as appropriate.
d. Use of additional physical barriers, where appropriate to prevent unauthorized access or physical contamination.
e. Provision of appropriate protection against fire, water, or other anticipated environmental threats.
f. Use of appropriate intrusion detection systems, such as motion and perimeter alarms, audio, and video surveillance.

g. Use of staffed reception areas or appropriate lock/ID systems to control passage into the restricted area.
h. Measures designed with sufficient redundancy such that a single point of failure does not compromise security; and
i. Regular maintenance to and review of the adequacy of the components of these physical protections.

4.3 Secure Area Controls

a. All Secure Areas must be protected with appropriate entry controls, such as keys and/or card readers, to ensure that only authorised users are granted physical access.
b. To limit access to authorised users only, entrance controls appropriate to specific types of sensitive information must be implemented.
c. Physical protection and guidelines for working in secure areas should be designed and implemented. Control includes:
    - Limiting personnel's awareness of, and activities within, a secure location on a need-to-know basis.
    - Limiting or prohibiting unsupervised/unmonitored work in secure areas, both for safety reasons and to avoid opportunities for malfeasance.
    - Keeping vacant secure areas locked, subject to periodic inspection, and/or monitored remotely as appropriate by video or other technologies.
    - Limiting video, audio, or other recording equipment, including cameras in portable devices, in secure areas.

4.4 Secure Offices, Rooms, and Facilities

Physical security for offices, rooms and facilities should be designed and implemented. Control includes:

a. Use of measures that are commensurate to the identified risks and the value of the assets at risk in each setting.
b. Use of measures that balance relevant health, safety and related regulations and standards.
c. Use of highly visible controls, where appropriate as a deterrent.
d. Use of unobtrusive or hidden controls/facilities, where appropriate for sensitive assets; and
e. Restrictions on information about facilities, including directory and location information.

4.5 Access to Restricted Facilities

a. Physical access to all restricted facilities shall be documented and managed. All facilities must be physically protected relative to the criticality or importance of the function or purpose of the area managed.

4.6 Requests for Access

a. Requests for access shall come from the applicable manager in the area where the data/system resides. Access to facilities will be granted only to personnel whose job responsibilities require access.

4.7 Approved Access Control Systems

a. Electronic access control systems shall be used to manage access to controlled spaces and facilities.

4.8 Access Control Process

a. The process for granting biometric, card and/or key access resides with the Digicall Group Human Resources Department. They shall regularly review biometric, card and/or key access rights and remove access for individuals that no longer require access or persons who leave the Digicall Group. Access rights shall be based on an employee's (staff, visitor, contractor, etc.) role or function in the organization.

4.9 Key Access and Card Systems

a. Employee biometric access, access cards and/or keys must not be shared or loaned to others.
b. Access cards/keys shall not have identifiable information other than a return mail address and all cards/keys that are no longer required must be returned to Digicall Group Human Resources or Facilities Departments.
c. Lost or stolen cards/or keys must be reported immediately.
d. Digicall Group Human Resources Department shall remove biometric, card and/or key access rights of individuals that change roles or are separated from their relationship with Digicall Group.
e. The Digicall Group Human Resources Department or their designee regularly reviews access records and visitor logs for facilities and is responsible for investigating any unusual events or incidents related to physical facility access.

4.10 Visitor and Guest Access

a. Any Digicall Group facility that allows access to visitors shall track visitor access with a sign in/out log.
b. A visitor log shall be used to maintain a physical audit trail of visitor activity to facilities as well as computer rooms and data centres where sensitive information is stored or transmitted.
c. The visitor log shall document the date, time, visitor's name, purpose, the firm represented, and the on-site personnel authorizing physical access on the log.
d. The visitor log shall be retained for a minimum of three months, unless otherwise restricted by rule, regulation, statute, or Digicall Group audit control.
e. Visitors shall be identified and given a badge or other identification that expires and that visibly distinguishes the visitors from on-site personnel.
f. Visitors shall surrender the badge or identification before leaving the facility or at the date of expiration.
g. Visitors shall be authorized before entering, and always escorted within areas where sensitive information is processed or maintained.
h. Visitors must be escorted in card access-controlled areas of facilities.

4.11 Confidential Area Access

a. All areas containing sensitive information shall be physically restricted.
b. All individuals in these areas must wear an identification badge on their person so that both the picture and information on the badge are clearly visible to Digicall Group personnel.
c. Restricted IT areas such as data centres, computer rooms, telephone closets, network router and hub rooms, voicemail system rooms, and similar areas containing IT resources shall be restricted based upon functional business need.
d. Physical access to records containing sensitive information, and storage of such records and data in locked facilities, storage areas, or containers shall be restricted.
e. Sensitive IT resources located in unsecured areas shall be secured to prevent physical tampering, damage, theft, or unauthorized physical access to sensitive information.
f. Appropriate facility entry controls shall limit and monitor physical access to information systems.
g. Video cameras and/or access control mechanisms shall monitor individual physical access to sensitive areas and this data shall be stored for at least one month (30 days), unless otherwise restricted by rule, regulation, statute, or law.

4.12 Digicall Group security staff shall:

a. Implement physical and/or logical controls to restrict access to publicly accessible data jacks (for example, data jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized).
b. Ensure visitors are always escorted in areas with sensitive information.
c. Areas accessible to visitors should not have enabled data jacks unless network access is provided to a secure guest network only.
d. Restrict physical access to wireless access points, gateways, handheld devices, networking, communications hardware, and telecommunications lines.
e. Control physical and logical access to diagnostic and configuration ports.
f. Receive prior authorization before disposing, relocating, or transferring hardware, software, or data to any offsite premises.

4.13 Physical Site Access

On-site physical access to sensitive or confidential areas for shall be controlled though a combination of the following mechanisms:

a. Security based on individual job function.
b. Revocation of all facility access immediately upon termination and collection of keys, biometric access, access/smart cards, and/or any other asset used to enter Digicall Group facilities.
c. Policies and procedures shall be established to ensure the secure use, asset management, and secure repurposing and disposal of equipment maintained and used outside the organization's premises.

4.14 Contractor Requirements

a. External contractors shall comply with applicable laws and regulations regarding security and background checks when working in Digicall Group facilities. For unclassified personnel, an appropriately cleared and technically knowledgeable staff member shall escort the individual to the area where facility maintenance is being performed and ensure that appropriate security procedures are followed.
b. Any system access, initiation or termination shall be performed by the escort.
c. Keystroke monitoring shall be performed during access to the system.
d. Prior to maintenance, the information system is completely cleared, and all non-volatile data storage media shall be removed or physically disconnected and secured.
e. Maintenance personnel must not have visual or electronic access to any sensitive or confidential information contained on the system they are servicing.
f. Devices that display or output sensitive information in human-readable form shall be positioned to prevent unauthorized individuals from reading the information.

g. All personnel granted unescorted access to the physical area containing the information system shall have an appropriate security clearance.

4.15 Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of normal Digicall Group operations. Examples of acceptable controls and procedures include:

a. Visitor logs.
b. Access control procedures and processes.
c. Operational key-card access and premise control systems.
d. Operational video surveillance systems and demonstrated archival retrieval of data.

4.16 Security of Equipment Off-Premises

a. Security procedures and controls must be used to secure equipment outside of Digicall premises.
b. Management must authorise the use of Digicall equipment outside of the company premises.

4.17 Secure Disposal or Re-use of Equipment

a. Sensitive information must be securely removed from any information systems equipment that has been used for Digicall business before disposal, donation, or re-use. This sanitisation process must take place before releasing such equipment to a third party.
b. Before equipment of any type is sold, disposed of, recycled, donated, or otherwise conveyed to a third party, approval must first be obtained.

4.18 Cabling Security

a. In line with industry electrical / cabling standards precautions must be taken to mitigate the risk of unauthorised / malicious data interception and accidental / malicious damage to ICT installations.
b. Electric cabling is physically separated from data cabling to prevent interference and reduce risk of injury and damage to equipment.
c. All power and telecommunications lines into information processing facilities are underground, or subject to adequate alternative protection.
d. All cabling and networking equipment is clearly labelled using a documented convention to minimise handling errors.

e. Any communications or networking equipment (routers, switches, hubs, and patch panels) is protected against unauthorised physical access by either placing it within a secured data centre or a locked cabinet or room.

4.19 Equipment Siting and Protection

Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and to reduce the opportunities for unauthorized access by human threats. Control includes:

a. Siting to minimize unnecessary risks to the equipment, and to reduce the need for unauthorized access to sensitive areas; Siting to isolate items requiring special protection, to minimize the general level of protection required.
b. Use of particularized controls as appropriate to minimize physical threats -- e.g., theft or damage from vandalism, fire, water, dust, smoke, vibration, electrical supply variance, or electromagnetic radiation; and
c. Guidelines for eating, drinking, smoking, or other activities in the vicinity of equipment.

4.20 Supporting Utilities

Equipment should be protected from power failures, telecommunications failures, and other disruptions caused by failures in supporting utilities such as HVAC, water supply and sewage. Control includes:

a. Assuring that the supporting utilities are adequate to support the equipment under normal operating conditions; and
b. Making reasonable provision for backups (e.g., a ups) in the event of supporting utility failure.

4.21 Protecting against External and Environmental Threats

Physical protection against damage from fire, flood, wind, earthquake, explosion, civil unrest, and other forms of natural and manufactured risk should be designed and implemented. Control includes:

a. Consideration of probabilities of various categories of risks and value of assets protected against those risks.
b. Consideration of security threats posed by neighbouring facilities and structures.
c. Appropriate fire-fighting equipment and other countermeasures provided and suitably located on site; and
d. Appropriate siting of backup facilities and data copies in a suitable location off-site.

4.22 Delivery & Loading Areas

a. Delivery and loading of hardware, software, or data should only be performed in the reception area.
b. Only IT staff are allowed to sign for the delivery of hardware, software or data being delivered or collected from Digicall Assist premises.
c. Once delivery is accepted and signed for, items are to be moved to the designated secure areas for safe keeping until they are needed.

5 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 personally responsible for implementing the policy and ensuring staff compliance.

Compliance with this Information Security and all subsequent policies is mandatory.

6 Policy Compliance Monitoring

6.1 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).

6.2 Exceptions

Any exception to this policy must be approved by the Group Chief Information Officer in advance.

6.3 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.

6.4 Remediation of Non-compliance

Where non-compliance has been identified, dependent on the severity and 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.

7 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

8 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.

9 Appendices

None included with this policy.