DIGICALL

A11 - CLEAN DESK AND CLEAR SCREEN 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
1.3	01.09.2024	Donald Fraser	2024 Revision, template change

Table of Contents

1 Policy Scope

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

2 Policy Statement

To improve the security and confidentiality of information, the Digicall Group has adopted a Clean Desk and Clear Screen Policy for all devices and printers involved in the processing of customer data.

3 Purpose

This ensures that all sensitive and confidential information, whether it be on paper, a storage device, or a hardware device, is properly locked away or disposed of, when a workstation or device is not in use.

This policy will reduce the risk of unauthorized access, loss of, and damage to information during and outside of normal business hours or when workstations or devices are left unattended.

4 General

Whenever a desk is unoccupied for an extended period the following will apply:

1. All sensitive and confidential paperwork must be removed from the desk. This includes mass storage devices such as CDs, DVDs, and USB drives.
2. All wastepaper which contains sensitive or confidential information must be shredded and placed in the designated confidential waste bins.
3. Under no circumstances should sensitive or confidential information be placed in regular wastepaper bins.
4. Laptops should be locked and should comply with the encryption standards as indicated in the Data Encryption Policy.
5. Keys for accessing drawers or filing cabinets should not be left unattended at a desk.
6. Printers should be treated with the same care under this policy:
    a) Any print jobs containing sensitive and confidential paperwork should be retrieved immediately. When possible, the “Locked/Secure Print” functionality should be used.
    b) All paperwork left over at the end of the workday will be properly disposed of.

Whenever a device with a screen is unattended for any period, while on company premises (e.g., a computer screen, laptop, tablet, or mobile device), the device must be locked, and password protected.

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, 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.