



NIGERIA SECURITY PRINTING AND MINTING PLC

POLICY NAME: CLEAR DESK, CLEAR SCREEN



DOCUMENT OWNERSHIP AND CREATION RECORD

	DESIGNATION	NAME	SIGNATURE	DATE
Policy Owner(s)	NSPM Data Protection Officer (DPO)	Mrs. Chika Ikelionwu		14/03//2024
Developed & authorized by:	Head, Risk Management	Mr. Samuel Keffas		14/03//2024
Approved by:	Executive Committee	EXCO		

POLICY REVISION TIMETABLE

REVISION	DESCRIPTION	DATE
1	Date Created	June 2021
2	Version 1.0	October 2021
3	Version 2.0	March 2024



DISTRIBUTION CONTROL

The policy owner controls the distribution of this document. The policy document is published as a PDF file on the MintNET intranet site:

NOTICE AND WARNING

This document is the property of the Nigerian Security Printing and Minting (NSPM) Plc, its circulation is restricted to the NSPM, and where a business requirement exists, to its designated associates, contractors, and consultants. It must not be copied or used for any other purpose other than that for which it is supplied, without the express written authority of the NSPM.

Except where provided for purposes of contractual requirements, NSPM disclaims any responsibility or liability for any use or misuse of the document by any person and makes no warranty as to the accuracy or suitability of the information to any third party.

**POLICY METADATA**

Title	CLEAR DESK, CLEAR SCREEN POLICY
Policy Number	ISM-CDCS-001
Version	2.0
Issuing Department	Risk Management
Policy Status	Draft
Approving Authority	EXCO
Date Of Approval	
Date Last Amended	5 th October 2024
Next Review Date	2025
Effective Date	Date of Approval
Date Created	June 2021
Policy Reviewer	Head, Risk Management
Intended Audience	The policy is applicable in all Departments / Units and other locations of the NSPM. The policy also applies to all NSPM employees, contractors, and other agents of the company entrusted with its sensitive data.
Description	A clear desk, clear screen policy is a set of rules designed to enhance information security by encouraging users to ensure that documents or computer systems are not left unattended
Document Size	8 pages



CONTENTS

1.0 INTRODUCTION	6
2.0 POLICY STATEMENT	6
3.0 RATIONALE	6
4.0 SCOPE.....	6
5.0 PROCEDURE.....	7
6.0 AUTHORIZATION	8
7.0 OTHER RELATED DOCUMENTS.....	8



1.0 INTRODUCTION

Although Technical and Administrative controls that aim to safeguard information and how they are managed within NSPM operations exist to prevent unauthorized access to Confidential and Restricted information, employees have a significant role to play in strengthening the information security program of the company.

To provide accountability, prevent misuse and abuse of access to information, it is important that employees take ownership and responsibility in managing information at their disposal in carrying out their job functions. This information can be warehoused in IT hardware (Desktop, Laptops, PCs etc.) or physical internal and external memos. This makes employees the front-line defense for information security management.

This policy defines guidelines and procedures to enhance information security of the NSPM assigning roles and responsibilities to employees and other insiders regarding information security management.

2.0 POLICY STATEMENT

All information (either softcopy on IT systems or hardcopy documents) accessed during operations or authorized access shall be protected with confidentiality and accessibility considerations. Therefore, it is the policy of the NSPM that standard procedures and guidelines shall be defined and enforced to control access to information.

3.0 PURPOSE

The purpose of this document is to define rules to prevent unauthorized access to confidential and restricted information in NSPM, as well as to shared facilities and equipment.

4.0 SCOPE AND APPLICABILITY

This policy applies to Confidential and restricted information collected, processed or stored on paper or electronic (including removable) storage media by staff of, or contractors and consultants to NSPM.



PROCEDURE

- A clear desk policy for papers and removable storage media and a clear screen policy for NSPM information processing facilities and equipment shall be observed by all staff, contractors and consultants. It is important not to expose confidential information and staff should strictly comply with the provisions of NSPM information classifications.
- All sensitive or critical business information, for example: on paper or on electronic storage media, must be locked away in a safe or cabinet (or other forms of security furniture) when not required, or in use and especially when the office is vacated.
- Computers and terminals must be left logged off or protected with a password-controlled screensaver and keyboard locking mechanism; when unattended.
- Access to all incoming and outgoing physical mail storage points and fax machines shall be restricted.
- Photocopiers and other reproduction technology (for example, scanners, digital cameras) shall be protected from unauthorized access and use.
- Documents containing sensitive or classified information must be promptly removed from printers, scanners and other reproduction technology.

5.0 ROLES AND RESPONSIBILITIES

5.1 Responsibility of Information Communication Technology (ICT)

System Administrators shall ensure that all NSPM computers are enforced with an auto-lock policy that reduces the risk of open information on those IT systems.

5.2 Responsibility of Risk Management Unit (RMU)

Ensure the adequacy and relevance of this Policy. It may be reviewed annually or as the need may arise due to change in operations, external events, or regulatory requirements.

6.0 POLICY ON NON-COMPLIANCE

Failure to comply with the Clear Desk/Clear Screen Policy may, at full discretion of management, lead to disciplinary action in accordance with HR Policies and Procedures.



7.0 AUTHORIZATION

This policy is as approved by the EXCO, of the Nigerian Security Printing and Minting Plc.

7.0 OTHER RELATED DOCUMENTS

- Information Security Policy
- Information Classification Policy
- IT Security Policy
- Enterprise Risk Management Framework
- Use of IT Work tool or Network Resources Policy
- IT Standard Policy