BEDC Electricity PLC
5, Akpakpava Street, Benin City, Edo State, Nigeria

Policy Area	IT		
Title of Policy	**CLEAN DESK POLICY**		
Reference No.			
Version	1.0		
Policy Owners	All Staff of BEDC		
No. of Revision	0		
Date of Draft	1st July 2022		
Effective Date			
Approve By	*Role*	*Name*	*Signature/Date*
	MD/CEO	**Dr. Henry Ajagbawa**	
	Board of Directors		

INTRODUCTION

BEDC has implemented a Clean Desk Policy for workspaces to improve data security and confidentiality. When items are not in use or an employee leaves his or her workstation, a clean desk policy is an important tool for ensuring that all sensitive/confidential materials and data are removed from an end user's workspace and locked away.

This policy mitigates the risk of unauthorized access, loss, and damage to information during and after normal business hours, as well as when workstations are left unattended. The policy also helps to raise employee awareness of the importance of protecting sensitive information.

PURPOSE

The goal of this policy is to establish the minimum requirements for maintaining a "clean desk," which means keeping sensitive/critical information about our employees, financial records, customers, and vendors secure and out of sight in locked areas. A clean desk policy is not only ISO 27001/17799 compliant, but it also falls under basic privacy controls.

SCOPE

This policy applies to all BEDC employees, including those on secondment from other organizations.

POLICY PROCEDURES

a) Employees must ensure that all sensitive/confidential information, whether hardcopy or electronic, is secure in their work area at the end of the day and when they are expected to be absent for an extended period of time.

b) When not in use, computer workstations must be locked.

c) At the end of the workday, computer workstations must be completely shut down.

d) Any restricted or sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.

e) When not in use, file cabinets containing restricted use or confidential information must be kept closed and locked.

a) Employees must ensure that all sensitive/confidential information, whether hardcopy or electronic, is secure in their work area at the end of the day and when they are expected to be absent for an extended period of time.

b) When not in use, computer workstations must be locked.

c) At the end of the workday, computer workstations must be completely shut down.

d) Any restricted or sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.

e) When not in use, file cabinets containing restricted use or confidential information must be kept closed and locked.

f) Keys used to gain access to restricted or confidential information should never be left unattended at a desk or workstation.

g) Laptops must be locked with a locking cable (if available) or stored in a drawer/file cabinet at the end of the day.

h) Passwords must not be left on sticky notes posted on or under a computer or laptop, nor should they be written down in an easily accessible location in the workstation.

i) Printouts containing restricted use or confidential information should be removed from the printer as soon as possible.

j) Restricted use and/or confidential documents should be shredded in the official shredder bins before disposal.

k) Whiteboards with restricted access and/or confidential information should be erased.

l) Laptops and tablets should be kept in a secure location.

m) All printers, scanners, and photocopiers should be cleared of papers as soon as they are printed/scanned; this prevents sensitive documents from being left in printer trays for an unauthorized person to pick up.

n) Liquids, food, and snacks should be kept away from computer systems/laptops. Spilled liquids can damage or short circuit internal components and corrupt restricted use/ confidential data, whereas crumbs from food and snacks can damage the keys (preventing them from fully depressing), invite insects, and damage circuitry.

POLICY COMPLIANCE

Compliance Measurement

Internal audit and **information technology departments** will use a variety of methods to ensure policy compliance, including but not limited to periodic walk-through and clean desk audits.

Non-Compliance

An employee who violates this policy is considered to have committed gross misconduct and will face appropriate disciplinary action, up to and including termination of employment.