COMPUTER & INFORMATION TECHNOLOGY CENTER

Clear Desk and Clear Screen

Document Controls

This document is reviewed every six months

Document Reference	PAAET-PLCY-CLEAR DESK AND CLEAR SCREEN
Document Title	Clear Desk and Clear Screen Policy
Document Owner	Abdullah AlDousari
ISO 27001:2013 reference	A.11.2.9 - Clear Desk and Clear Screen Policy
Security Classification	Internal -Unrestricted
Stored	http://sp13.paaet.edu/sites/TecDep
Next Review Date	12th Dec, 2016
Document Status	Final

Document Review and Approval History

Date	Version	Amended by	Reviewer/Approver	Remarks	RFC#
5th April, 2016	Draft v1.0	Reena Varghese		Initial	
25th May, 2016	Draft v1.1	Abdullah AlDousari		Edited	
25th Dec, 2016	Draft v1.2	Rabie Al-Mejbas	Rabie Al-Mejbas	Final Review	

Document Distribution List

Sl.No.	Name and Department	Purpose
1	Dr. Jasem AlOstad, CIC Manager	For his information & feedback
2	Ali Hussain, Technical Support Supervisor	Distribution to concerned staff responsible for creating documents for Technical Support Supervision
3	Ibtisam Shaban, Development Supervisor	Distribution to concerned staff responsible for creating documents for Development Supervision
4	Ammal AlQattan, PC & Servers section Head.	For here information
5	ISO team : • Rabie Al-Mejbas • Rajiv Prakash • Nadia AL Saleh • Shaikha AL Barak • Mai AlAbdulqader • Abdullah Aldousari	Start implementing this policy on all documentations.
6	All PAAET and Contracted Staff at CIC	Ensure they start enforcing the policy.

CONTENTS

CONFIDENTIALITY STATEMENT

This document includes confidential information related to the Computer and Information Technology Center (**CIC**) at the Public Authority for Applied Education and Training (**PAAET**), shall not be distributed to any persons other than those mentioned in the distribution list herein, and shall be used solely for **CIC**'s internal purpose.

1.0 INTRODUCTION

In order to reduce the risk of security breaches in the workplace, CIC at PAAET have adopted a clear desk policy for papers and removable storage media, and clear screen policy for information processing facilities.

This can ensure that all sensitive/confidential materials are removed or inaccessible from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. Such a policy can also increase employee's awareness about protecting sensitive information.

This Policy is issued by CIC at PAAET. The owner of this document is responsible for maintenance of this Policy. The supervisor of the technical support is responsible for final approval.

2.0 OBJECTIVE

The purpose for the policy is to establish the minimum requirements for maintaining a "clear desk and clear screen" where sensitive/critical information about CIC and its employees and contracted employees , intellectual property, students and vendors is secure in locked areas and out of site.

3.0 SCOPE

This policy applies to all PAAET CIC employees, contractors, vendors and students operating on behalf of PAAET in building 5, building 10, and part of building 2.

4.0 POLICY

- Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day, and if they expect to be gone for an extended period.
- Computer workstations must be protected with a screen saver and locked with a password or logged off when unattended or when workspace is unoccupied.
    1. If the workstation is idle for more than 5 minutes, the screen shall be locked automatically. It shall have the feature of unlocking only by entering the password.
    2. If the server is idle for more than 5 minutes, the screen shall be locked automatically. It shall have the feature of unlocking only by entering the password.

- 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.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing Restricted or Confidential information should be immediately removed from the printer.
- Upon disposal, Restricted and/or Confidential documents should be shredded in the official shredder bins.
- Whiteboards containing Restricted and/or Sensitive information should be erased.
- Lock away portable computing devices such as laptops and tablets.
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer
- Incoming/outgoing mail points and unattended faxes shall be protected.

5.0 ENFORCEMENT

Compliance to this policy can be verified through various methods, including but not limited to, periodic walkthroughs, internal and external audits, and feedback to the policy owner.

An employee found to have violated this policy may be subject to disciplinary action.

6.0 DEFINITIONS

Names	Definitions
Security breaches	A security breach is any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms.
Workspace	A space used or required for one's work, as in an office or home.
Intellectual property	Intellectual property is a broad categorical description for the set of intangibles owned and legally protected by a company from outside use or implementation without consent example patents, trade secrets, copyrights and trademarks, or simply ideas.
Screen saver	A screensaver is a computer program that blanks the screen or fills it with moving images or patterns when the computer is not in use
Incoming/outgoing mail points	All processing points of mails when coming in and exiting an organization
Compliance	Conformity in fulfilling official requirements
Walkthrough	Step-by-step test of all aspects of an environment, plan, or process to verify it is ready for its intended purpose

7.0 REFERENCES

ISO/IEC 27001:2013 – A.11.2.9 - Clear Desk and Clear Screen Policy

8.0 ASSOCIATED DOCUMENTS

1) Information Security Policy