Clean Desk Policy

2020-04-21

Document Number:

QMZ-CDP-01.DOCX

Prepared by: Qmuzik Technologies (Pty) Ltd

Submitted to:

Contents

1. Overview 3
2. Purpose 3
3. Scope 3
4. Policy 3
5. Policy Compliance 4
6. Related Standards, Policies and Processes 4
7. Definitions and Terms 4
8. Revision and version control 4
9. Policy acceptance 5

1. Overview

A clean desk policy can be an import tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

2. Purpose

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of site. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

3. SCOPE

This policy applies to all Qmuzik Technologies employees and affiliates.

4. POLICY

4.1. 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 when they expect to be gone for an extended period.

4.2. Computer workstations must be locked when workspace is unoccupied. To ensure this, domain policy automatically locks all inactive computer sessions after 10 minutes.

4.3. Computer workstations must be shut down at the end of the work day.

4.4. Any restricted or sensitive information must be removed from the desk and locked in the drawers or cupboards when the desk is unoccupied and at the end of the day.

4.5. File cabinets containing restricted or sensitive information must be kept closed and locked when not in use or when not attended.

4.6. Office keys, including keys used to access restricted or sensitive information, must not be left at an unattended desk.

4.7. All laptops must be locked with a locking cable or locked away in a drawer/cupboard. All employees are provided with the standard Kensington locks or with the more recent Noble locks as required.

4.8. Passwords may not be left on sticky notes posted near, on or under a computer nor may they be written down in an accessible location.

4.9. Printouts containing restricted or sensitive information should immediately be removed from the printers.

4.10. Upon disposal, restricted or sensitive documents should be shredded in the official shredder bin.

4.11. Whiteboards containing restricted or sensitive information should be wiped down after use.

4.12. Portable computing such as laptops and tablets as well as mass storage devices such as CD-, DVD ROM, external harddrives and USB flash drives must be securely locked in the drawers or cupboards when not in use.

5. Policy Compliance

5.1 Compliance Measurement

The Qmuzik Technologies team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exception

Any exception to the policy must be approved by the Qmuzik Technologies Management team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

None

7. Definitions and Terms

None

8. Revision and version control

Version Number	Date	Description of Change	Changed By
1.0	2020/05/06	Creation	Tinus Kleingeld

9. Policy acceptance

The undersigned hereby agrees that this policy is valid and can be enforced.

Name	Role	Signature