# Catholic Diocese of Columbus
# Clean Desk Policy

**Steve Nasdeo**

**Diocesan Director of Technical Services and Catholic Schools**

**September 2018**

# Table of Contents

Revision History ..... 2
Overview ..... 3
1. Purpose ..... 3
2. Scope ..... 3
3. Policy ..... 3
4. Policy Compliance ..... 4
4.2. Exceptions ..... 4
4.3. Non-Compliance ..... 4
5 Related Standards, Policies and Processes ..... 4
6 Definitions and Terms ..... 4

## Revision History

| Date of Change | Responsible for Change | Change Summary |
|---|---|---|
| 13 June 2017 | Steve Nasdeo | Initial Policy Document |
| 17 Sept 18 | Steve Nasdeo | Final policy wording |
| 20 Sept 18 | Steve Nasdeo | Policy Approved – marked FINAL |
| | | |
| | | |

## Overview

A clean desk policy can be an important 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.

## 1. 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, it is also part of standard basic privacy controls.

## 2. Scope

This policy applies to all Catholic Diocese of Columbus employees and affiliates.

## 3. Policy

3.1. 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 as well as when they are expected to be gone for an extended period.

3.2. Office doors should be closed and locked at the end of the day. If, due to cleaners the office is not locked, the door to the office should be closed at a minimum.

3.3. Computer workstations must be locked when workspace is unoccupied.

3.4. Computer workstations must be shut completely down at the end of the workday.

3.5. 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.

3.6. File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

3.7. Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

3.8. Laptops, if left at the office overnight, must be either locked with a locking cable or locked away in a drawer.

3.9. 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.

3.10. Printouts containing Restricted or Sensitive information should immediately be removed from the printer.

3.11. After restricted and/or sensitive documents have been addressed, they should be shredded in the official shredder bins or placed in the lock confidential disposal bins.

Catholic Diocese of Columbus 2018 – All Rights Reserved

3.12. Whiteboards containing Restricted and/or Sensitive information should be erased when no longer being used.
3.13. Lock away portable computing devices such as laptops and tablets.
3.14. Treat mass storage devices, if approved, such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer
3.15. All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

## 4. Policy Compliance

### 4.1. Compliance Measurement

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

### 4.2. Exceptions

The Chancellor or the Director of Technical Services or their delegates must approve any exception to this policy in advance.

### 4.3. Non-Compliance

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

## 5 Related Standards, Policies and Processes

None.

## 6 Definitions and Terms

None.