Catholic Diocese of Columbus

Workstation Security Policy

Steve Nasdeo

Diocesan Director of Technical Services and Catholic Schools

September 2018

Table of Contents

Revision History

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

Workstation Security Policy

1. Overview

The Catholic Diocese of Columbus strives to maintain the most secure environment for our employees as well as protect the assets and information of the Catholic Diocese of Columbus. This task is not to encumber the user with a too restrictive policy but rather one that allows options for the protection of devices and the information they hold.

2. Purpose

The purpose of this policy is to provide guidance for workstation security for the Diocese workstations in order to ensure the security of information on the workstation and information the workstation may have access to.

3. Scope

This policy applies to all Diocesan employees, contractors, workforce members, vendors and agents with a Diocesan-owned or personal workstation connected to the Diocesan network.

4. Policy

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including personally identifiable information (PII) and that access to sensitive information is restricted to authorized users.

3.1 Workforce members using workstations shall consider the sensitivity of the information, including personally identifiable information (PII) that may be accessed and minimize the possibility of unauthorized access.

3.2 Appropriate measures include:

- Restricting physical access to workstations to only authorized personnel.
- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that are left unsecured will be protected. The password must comply with the Diocese *Password Policy*.
- Complying with all applicable password policies and procedures. See the Diocese *Password Policy*.
- Ensuring workstations are used for authorized business purposes only.
- Never installing unauthorized software on workstations.
- Storing all sensitive information, including personally identifiable information (PII) on authorized SharePoint sites or network servers
- Keeping food and drink away from workstations in order to avoid accidental spills.

- Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
- Complying with the *Portable Workstation Encryption Policy*
- Complying with the Baseline *Workstation Configuration Standard*
- Installing privacy screen filters or using other physical barriers to alleviate exposing data.
- Exit running applications and close open documents
- Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
- If wireless network access is used, ensure access is secure by following the *Wireless Communication policy*

5. Policy Compliance

5.1 Compliance Measurement

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

5.2 Exceptions

The Director of Technical Services or their delegate must approve any exception to this policy 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

- Password Policy
- Portable Workstation Encryption Policy
- Wireless Communication policy
- Workstation Configuration Standard