2022

ZIMWORX

# WORKSTATION SECURITY (FOR HIPAA) POLICY

SupportDDS

SupportRealty

SUPPORT CPA OUTSOURCING ACCOUNTING PROFESSIONALS

SupportDrs OUTSOURCED SUPPORT FOR MEDICAL DOCTORS

WeSupportMinistries Spend Less Reach More

**Usage Disclaimer:** This policy was created by or for ZimWorX employees, contractors, consultants, temporary, and other workers. If you would like to contribute a new policy or updated version of this policy, please send email to **itsupport@zimworx.com.**

**Last Update Status:** Updated November 2021

## 1. Overview

See Purpose.

## 2. Purpose

The purpose of this policy is to provide guidance for workstation security for ZimWorX workstations to ensure the security of information on the workstation and information the workstation may have access to. Additionally, the policy provides guidance to ensure the requirements of the HIPAA Security Rule "Workstation Security" Standard 164.310(c) are met.

## 3. Scope

This policy applies to all ZimWorX's employees, contractors, workforce members, vendors, andagents with a ZimWorX's -owned or personal-workstation connected to the ZimWorX's network.

## 4. Policy

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

4.1 Workforce members using workstations shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimize the possibility of unauthorized access.

4.2 ZimWorX's will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

4.3 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 were left unsecured will be protected. The password must comply with ZimWorX's ***Password Policy***.

- Complying with all applicable password policies and procedures. See ZimWorX's Password Policy.
- Ensuring workstations are used for authorized business purposes only.
- Never installing unauthorized software on workstations.
- Storing all sensitive information, including protected health information (PHI) on 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.
- Installing privacy screen filters or using other physical barriers to alleviate exposing data.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates.
- 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 and personal mobile device connect only to guest wireless networks.

## 5. Policy Compliance

5.1 Compliance Measurement

The IT 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 Exceptions

Any exception to the policy must be approved by the IT 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

- Acceptable Use Policy
- Internet Usage Policy
- Email Policy
- Workstation Security (for HIPAA) Policy
- Removable Media Policy
- Bring Your Own Device (BYOD) Policy
- Password Policy
- Remote Work Policy
- Virtual Private Network (VPN) Policy

- Wireless Communication Policy
- Encryption Policy

HIPPA 164.210
http://www.hipaasurvivalguide.com/hipaa-regulations/164-310.php

## 7 Policy Governance

The following table identifies who within ZimWorX is accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply;

- Responsible – the person(s) responsible for developing and implementing the policy.
- Accountable - the person who has ultimate accountability and authority for the policy.
- Consulted – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- Informed – the person(s) or groups to be informed after policy implementation or amendment.

| | |
|---|---|
| **Responsible** | IT Department |
| **Accountable** | COO |
| **Consulted** | Human Resources, EOS Heads |
| **Informed** | All Employees |

## 8 Definitions and Terms

None.

## 9. Revision History

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| December 2021 | IT Department | Updated and converted to new format |

I understand and agree to the above as part of my terms of employment with ZimWorX.

**EMPLOYEE**

Authorised Signature

Print Name & Title

/ /

Date

**COMPANY**

Authorised Signature

Print Name & Title

/ /

Date