2022

ZIMWORX

REMOVABLE MEDIA 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

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations.

2. Purpose

The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by ZimWorX and to reduce the risk of acquiring malware infections on computers operated by ZimWorX.

3. Scope

This policy covers all computers and servers operating in ZimWorX.

4. Policy

4.1 Access to removable mass storage devices is prohibited on all ZimWorX computers.
4.2 When information is transferred on to removable media, it must be encrypted in accordance with the ZimWorX Acceptable Encryption Policy.

4.3 Smart mobile devices such as phones, tablets, iPod etc. are considered as removable media and are therefore prohibited to connect to ZimWorX computers.

4.4 Connecting and recharging of smart devices using ZimWorX computers is also prohibited. Users should charge smart devices or phones on power sockets.

Exceptions to this policy may be requested on a case-by-case basis by ZimWorX-exception procedures.

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-thrus, 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 Encryption Policy

7 Definitions and Terms

- Encryption - **encryption** is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext.
- Malware - **Malware** (a portmanteau for **malicious software**) is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive users access to information or which unknowingly interferes with the user's computer security and privacy.
- Removable Media - Expandable storage is a form of computer storage that is designed to be inserted and removed from a system.
- Sensitive Information - is the control of access to information or knowledge that might result in loss of an advantage or level of security if disclosed to others.

8 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

9. Revision History

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

EMPLOYEE

Authorised Signature

Print Name & Title

/ /

Date

COMPANY

Authorised Signature

Print Name & Title

/ /

Date