1.0 PURPOSE AND SCOPE

This policy describes how the organization protects and secures media that may contain sensitive or confidential information (organization data). This includes protecting paper and digital system media, limiting access to information on system media to authorized users, and sanitizing or destroying system media before disposal or release for reuse. Media protections can restrict access and make media available to authorized personnel only, apply security labels to sensitive information, and provide instructions on how to remove information from media so that the information cannot be retrieved or reconstructed.

2.0 SCOPE

This policy applies to all electronic records in the organization's data storage systems and on physical paper that may contain sensitive or confidential information.

3.0 POLICY

3.1 Protect media containing organization data and limit access (3.8.1, 3.8.2, 3.8.8)

External media includes both digital and non-digital media. Digital media includes diskettes, magnetic tapes, external and removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes paper and microfilm. The organization must protect external media by keeping it in a secure area, such as a locked drawer, desk, or cabinet, or a secure office location. Sensitive data stored on external electronic media should be encrypted. If portable storage devices are used, they should have an identifiable owner. Devices without an identifiable owner or labelling that describes the contents should not be used.

3.2 Sanitize or destroy media before disposal (3.8.3)

All systems and media containing organization data are physically or logically wiped of all data prior to the system or media being disposed of, reused, or otherwise leaving the control of the organization. Systems that may contain organization data do not leave organization's premises without being encrypted.

Organization data on physical media (paper) is physically destroyed by shredding when no longer needed.

3.3 External media marking and control (3.8.4)

External media should be properly labeled and tracked. Examples include "confidential" or other markers in the footers of electronic and paper documents, and physical labels applied to external media

3.4 Media encryption (3.8.5, 3.8.6, 3.8.9)

Media and technology systems that may contain organization data are encrypted at rest. Organization data is encrypted in transit. Data backups are encrypted. Encryption mechanisms are FIPS-140-2 compliant.

3.5 Control the use of removable media on system components (3.8.7)

Users with access to organization data should be made aware, through training or other communication, that storage and transmission of organization data through the organization's Office 365 environment is preferred, and that external media should only be used when necessary, and that external media should be encrypted.

4.0 REVISION HISTORY

Date	Name	Changes Made	Revision #
10/9/2023	Frank Schipani	Initial draft created	0.9
12/30/2023	Audit Committee	Approved Policies	

5.0 RELEVANT NIST CONTROLS

Control	Control Description	Document Section
NIST 800-171 3.8	Media Protection	Entire Document