3.8 - Media Protection

Control Satisfaction Matrix

Standard	Category	Controls Satisfied	800-53r4 Controls	ISO/SEC 27001	Audit Controls
NIST 800-171	Media Protection	3.8.1-3.8.3	MP-2, MP-4, MP-6	A.8.2.3, A.8.3.1, A.11.2.9, A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7	17.0, 22.0

Major Document History

Date	Comment	Who
5/13/2019	Initial Doc	Tharp
6/21/2019	CO's & Assertions updated with feedback from B&V CPA's	Tharp
6/28/2019	CO's & Assertions updated with feedback from Dave	Tharp
7/30/2019	Added 17.0, 22.0	Tharp
7/30/2019	Strike thru control Objectives	Tharp
8/12/2019	Formatting Updates	Tharp
8/29/2019	Copied Content For IS-1 SOC submission	Tharp
10/6/2021	Policy's Reviewed for Audit	Tharp

Purpose and Scope

The purpose of this policy is to address physical media and printed documents. Neither of which should exist outside of DLZP Group Headquarters.

Background

DLZP has adopted a 100% virtualized infrastructure for its business needs and the interactivity of its remote workers. All systems and documents should be stored in the cloud and not downloaded to a local machine.

Policy

3.8.1

DLZP Group shall protect and store physical media securely containing all DLZP and Customer Records. This control specifically focuses on Confidential Unclassified Information (CUI) but DLZP Policy treats all records and client information as if they met this classification. This includes both physical media and paper records.

3.8.2

All access to systems media shall be limited to authorized users.

3.8.3

Any physical media will be destroyed by appropriate means when no longer required.

Response Plan

17.0 Media Disposition Plan

17.1 Purpose

This document provides specific guidance on methods, processes and procedures to ensure no data remains on removable storage devices that are to be permanently removed from DLZP Group.

17.2 Methods for media sanitization and clearing

Overwriting is the process of replacing information (data) with meaningless data in such a way that meaningful information cannot be recovered from a device. The DLZP Group technician performing the overwriting will have suitable technical expertise and will be responsible for certifying that the process has been successfully completed.

Destruction of a device is the process of physically damaging a medium so that it is not usable in a computer and so that no known exploitation method can retrieve data from it.

Clearing data (deleting files) simply removes information from storage media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. However, because the clearing process does not prevent data from being recovered by technical means, it is not an acceptable method of sanitizing DLZP Group controlled storage media.

17.3 Disposition

Storage devices may be scheduled for reuse, repair, replacement, or removal from service for a variety of reasons and disposed of in various ways as described below.

22.0 Removeable Media Plan

22.1 Overview

Removable media can be classified as any portable device that can be used to store and/or move data. Media devices can come in various shapes and forms, including USB memory sticks, floppy disks, read/write compact disks and DVDs, PDA storage cards, magnetic tapes and cassettes – essentially anything that can be copied, saved, and/or written to which can then be taken away and restored on another computer.

By design, removable media create their own security vulnerabilities – they provide the means to conveniently transport up to several gigabytes of data from one computer or network to another. The most salient vulnerabilities being:

1) Most forms of removable media require no form of authentication, password protection, or configuration to install or use and they can make use of “plug and play” technologies and generally do not require any administrator privileges to install.

2) Unauthorized disclosure of sensitive data could occur if an item of removable media fell into the wrong hands.

3) In addition to their authorized data, users may also inadvertently transport (and therefore introduce) malicious software on to DLZP Group’s systems.

4) The nature and tangible size of removable media is such that they are also prone to accidental loss and/or theft.

22.2 Restrictions for the Management of Removable Media

1) Only DLZP Group owned and managed removable media should be used with DLZP Group systems.

2) It is not permissible to use DLZP Group owned media on personal computers or other devices that do not have an official connection to DLZP Group networks.

3) High sensitivity data must be protected to 256bit encryption levels when stored on removable media. If it is not possible to achieve this level of encryption, then its storage is prohibited.

4) Removable media should only be used to transport or store data when other more secure means (internal email or network shares) are not available.

5) If any item of removable media is no longer required by DLZP Group, it must be destroyed by approved secure means. This is only to be carried out by the Help Desk.

6) When transferring data from outside of DLZP Group, extreme caution must be taken, as the potential impact of a malicious software attack on DLZP Group’s systems could be severe.

7) Any loss or theft of any item of removable media must be reported immediately to the Help Desk so that the level of compromise can be assessed, and necessary efforts can be made for

recovery.

22.3 Enforcement

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