3.14 SYSTEM AND INFORMATION INTEGRITY

Control Satisfaction Matrix

Standard	Category	Controls Satisfied	800-53r4 Controls	ISO/SEC 27001	A-lign Controls
NIST 800-171	Systems & Information Integrity	3.14.1 - 3.14.3	SI-2, SI-3, SI-5	A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3, A.12.2.1, A.6.1.4	5.0, 7.0

Major Document History

Date	Comment	Who
7/26/2019	Initial Doc, Anti-Virus Policy	Tharp
8/09/2019	Updated 7.4	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 establish the organizational requirements for Systems Integration and Integrity monitoring and logging to ensure we operate within a secure infrastructure, using methods that meet or exceed industry best practice as well any governing compliance frameworks necessary to support our customers.

Background

Provide guidance to operation methods and processes that must be maintained to conform with these policies.

Policy

3.14.1

Identify, report, and correct system flaws in a timely manner.

3.14.2

Provide protection from malicious code at designated locations within organizational systems.

3.14.3

Monitor system security alerts and advisories and take action in response.

3.14.4

Update malicious code protection mechanisms when new releases are available.

3.14.5

Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

3.14.6

Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

3.14.7

Identify unauthorized use of organizational systems.

Response Plan

5.0 Anti-Virus Software Plan

- All workstations and servers owned and operated by DLZP Group are required to run TrendMicro Antivirus software.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then “double delete” them by emptying the computer’s Recycle Bin.
- Delete spam, chain, and other junk email without forwarding, as per DLZP Group’s Acceptable Use Plan.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan removable disks from an unknown source for viruses before using them.
- If testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the test. After the test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

- New viruses are discovered almost every day. Virus definitions are automatically updated by TrendMicro.

7.0 Backup / Restore Plan

7.1 Overview

This Plan defines the backup Plan for computers within DLZP Group which have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers backed up include file, mail, database, application, and web.

7.2 Purpose

This Plan is designed to protect data within DLZP Group to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

7.3 Scope

This Plan applies to all equipment and data owned and operated by DLZP Group, Inc.

7.4 Definitions

Term	Definition
Backup	The saving of files onto mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
Archive	The saving of old or unused files on offline low-cost mass storage media for the purpose of reducing storage costs.
Restore	The process of bringing backup data back from mass storage media and putting it on an online storage system such for systems or data recovery.

7.5 Timing

Backups are performed per the clients Contract or Statement of Work.

Full data replication of scanned files and reports, and scanned billing documentation and invoices is done real time using AWS data replication technology. DLZP Group also utilizes other AWS services to replicate production data to alternate site and/or disaster recovery standby databases. As data is changed on the production systems, that data is replicated to standby databases. This is done realtime. In case of primary database failure, the standby database can configured as the primary database with minimal configuration changes.
