3.5 Identification & Authentication

Control Satisfaction Matrix

Standard	Category	Controls Satisfied	800-53r4 Controls	ISO/SEC 27001	A-lign Controls
NIST 800-171	Identification & Authentication	3.5.1 - 3.5.11	IA-2, IA-2(1), IA-2(2), IA-2(3), IA-2(8), IA-2(9), IA-3, IA-4, IA-5, IA-5(1), IA-6	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3, A.12.5.1, A.12.6.2	9.0, 10.0

Major Document History

Date	Comment	Who
7/29/2019	Initial Doc, 9.0, 10.0	Tharp
8/09/2019	Updated, 9.6, 10.5	Tharp
8/12/2019	Format	Tharp
8/29/2019	Database PW Plan Removed, 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 Identification & Authentication management practices to ensure we operate within a secure infrastructure, using methods that meet or exceed industry best practices as well any governing compliance frameworks necessary to support our customers.

Background

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

Policy

3.5.1

Identify system users, processes acting on behalf of users, and devices.

3.5.2

Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

3.5.3

Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

3.5.4

Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

3.5.5

Prevent reuse of identifiers for a defined period.

3.5.6

Disable identifiers after a defined period of inactivity.

3.5.7

Enforce a minimum password complexity and change of characters when new passwords are created.

3.5.8

Prohibit password reuse for a specified number of generations.

3.5.9

Allow temporary password use for system logons with an immediate change to a permanent password.

3.5.10

Store and transmit only cryptographically-protected passwords.

3.5.11

Obscure feedback of authentication information.

Response Plan

9.0 Password Plan (All Systems)

9.1 Overview

All DLZP Group employees (including contractors and vendors with access to DLZP Group systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

9.2 Purpose

The purpose of this Plan is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

9.3 Scope

The scope of this Plan includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any DLZP Group facility, has access to the DLZP Group network, or stores any non-public DLZP Group information.

9.4 Plan

9.4.1 General

- All system-level passwords (e.g., root, administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.
- User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

9.4.1.1 Password Protection Standards

Do not use the same password for DLZP Group accounts as for other non-DLZP Group access (e.g.,

personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various DLZP Group access needs.

Do not share DLZP Group passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential DLZP Group information.

Here is a list of “don’ts”:

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., “my family name”)
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call the DLZP Leadership.

Do not use the “Remember Password” feature of Windows or applications (e.g., Internet Explorer, Outlook, Netscape, etc.).

Again, do not write passwords down and store them anywhere in the office. Do not store passwords in a file on ANY computer system (including mobile or similar devices) without encryption.

If an account or password is suspected to have been compromised, report the incident and change all passwords.

Administrative password cracking or guessing may be performed on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it.

9.4.1.2 Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

9.4.1.3 Use of Passwords and Shared Keys for Remote Access Users

Access to the DLZP Group network via remote access (VPN) is to be controlled using either password authentication or a shared key system managed by a VPN client.

9.4.2 Active Directory

- Change passwords every 90 days (except system-level passwords which must be changed at

least quarterly).
- Users cannot reuse any of their last 24 passwords.
- Password must be a minimum of 14 characters; it must contain one capital letter or special character and at least one number.

9.4.3 Connections

- New users receive a temporary password that needs to be changed every 90 days
- Users cannot reuse their previous password when prompted to change it
- Passwords must be a minimum of 14 characters; passwords require at least one capital letter and one number and one special character
- Passwords are encrypted using a 256 bit RC4 stream cipher during transmission to the server and are stored in the database using a secure 160-bit SHA hash value. This secure hash means that although passwords may be reset by an administrator they can never be retrieved from the database.

9.5 Enforcement

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

9.6 Definitions

Term	Definition
Application Administration Account	Any account that is for the administration of an application (e.g., Oracle database administrator).
Min PW Requirements	Must be at least 10 characters long, Must include at least one uppercase letter, Must include at least one lowercase letter, Must include at least one number, Must include at least one special character
Computer language	A language used to generate programs.
Credentials	Something a user knows (e.g., a password or pass phrase), and/or something that identifies a user as being present for authentication (e.g., a user name, a fingerprint, voiceprint, retina print).
Entitlement	The level of privilege that has been authenticated and authorized. The privileges level at which to access resources.
Executing body	The series of computer instructions that the computer executes to run a program.
Hash	An algorithmically generated number that identifies a datum or its location.
LDAP	Lightweight Directory Access Protocol, a set of protocols for accessing information directories.
Module	A collection of computer language instructions grouped together either logically or physically. A module may also be called a package or a class, depending upon which computer language is used.
Name space	A logical area of code in which the declared symbolic names are known and outside of which these names are not visible.
Production	Software that is being used for a purpose other than when software is being implemented or tested.

Term	Definition
Min PW Requirements	Must be at least 14 characters long, Must include at least one uppercase letter, Must include at least one lowercase letter, Must include at least one number, Must include at least one non-alphanumeric character