3.1 Access Control Policy

Control Satisfaction Matrix

Framework Standard	Category	Controls Satisfied	800-53r4 Controls	ISO/SEC 27001	Audit Controls
NIST 800-171	Access Control	3.1 - 3.22	AC-2, AC-3, AC-4, AC-5, AC-6, AC-7, AC-8, AC-11,AC-12, AC-17, AC-18, AC-19, AC-20, AC-22	A.6.1.2, A.6.2.1, A.6.2.2, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.9.4.1, A.9.4.2, A.9.4.4, A.9.4.5, A.11.2.6, A.11.2.8, A.11.2.9, A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3, A.18.1.3	3.0, 28.0

Major Document History

Date	Comment	Who
5/6/2019	Initial Doc	Tharp
7/26/2019	Added Access Control Policy 3.0	Tharp
7/30/2019	Added 28.0	Tharp
8/12/2019	NIST Section 3.1, Format Updates	Tharp
8/15/2019	Updated Control Satisfaction Matrix	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 a repeatable set of access control guidelines to align with the NIST 800-171 Framework. Conforming to these controls establishes the minimum controls to secure all Controlled Unclassified Data at a Moderate Classification or lower in FIPS 199.

Background

Infrastructure Security and Cyber Security are crucial elements of any application or infrastructure hosting services. DLZP has made a commitment to design and build highly secure environments for our customers. But, attack strategies and vulnerabilities are consistently evolving so tight access control policy is necessary to prevent unauthorized usage.

Policy Requirements

3.1.1

Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

3.1.2

Limit system access to the types of transactions and functions that authorized users are permitted to execute.

3.1.3

Control the flow of CUI in accordance with approved authorizations.

3.1.4

Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

3.1.5

Employ the principle of least privilege, including for specific security functions and privileged accounts.

3.1.6

Use non-privileged accounts or roles when accessing nonsecurity functions.

3.1.7

Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

3.1.8

Limit unsuccessful logon attempts.

3.1.9

Provide privacy and security notices consistent with applicable CUI rules.

3.1.10

Use session lock with pattern- hiding displays to prevent access and viewing of data after a period of inactivity.

3.1.11

Terminate (automatically) a user session after a defined condition.

3.1.12

Monitor and control remote access sessions.

3.1.13

Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

3.1.14

Route remote access via managed access control points.

3.1.15

Authorize remote execution of privileged commands and remote access to security- relevant information.

3.1.16

Authorize wireless access prior to allowing such connections.

3.1.17

Protect wireless access using authentication and encryption.

3.1.18

Control connection of mobile devices.

3.1.19

Encrypt CUI on mobile devices and mobile computing platforms.

3.1.20

Verify and control/limit connections to and use of external systems.

3.1.21

Limit use of portable storage devices on external systems.

3.1.22

Control CUI posted or processed on publicly accessible systems.

Response Plans

3.0 Access Control Plan

- DLZP Group has established the following policy to define how access control to information systems and services cover all stages in the life cycle of user access: from registration of new users to de-registration of users who no longer need access. Where possible, user policies are enforced by the operating system or other software.
- DLZP Group data must have sufficient granularity to allow appropriate authorized access. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. DLZP Group recognizes this balance.
- Where possible and financially feasible, more than one person must have full rights to any DLZP Group owned server storing or transmitting highly sensitive data. DLZP Group has a standard policy that applies to user access rights.
- Access to DLZP Group’s network, servers and systems is achieved by individual and unique logins, and requires authentication. Authentication may include the use of passwords, smart cards, biometrics, and/or other recognized forms of authentication. Where possible a lockout policy will be enforced to disable login for 24 hours when 3 incorrect login attempts are made without success.
- As stated in DLZP Group’s policy on appropriate and acceptable use, users must not share usernames and passwords, nor should they be written down or recorded in unencrypted

electronic files or documents. All users must secure their username or account, password, and system access from unauthorized use.
- All users of DLZP Group systems that contain high risk or confidential data must have a strong password - the definition of which is established in DLZP Group's password policy. Empowered accounts, such as administrator, root or supervisor accounts, must be changed frequently, consistent with guidelines established in the password policy.
- Default passwords on all DLZP Group systems are changed after installation. All administrator or root accounts are given a password that conforms to the password selection criteria when a system is installed, rebuilt, or reconfigured.
- Logins and passwords are not coded into programs or queries unless they are encrypted or otherwise secure.
- Users are responsible for safe handling and storage of all DLZP Group authentication devices. If an authentication device is lost or stolen, the loss must be immediately reported to the appropriate individual in the issuing unit so that the device can be disabled.
- Terminated employee access is reviewed and adjusted as found necessary. Terminated employees have their accounts disabled upon transfer or termination. Since there could be delays in reporting changes in user responsibilities, periodic user access reviews are conducted by company leaders.
- Transferred employee access is reviewed and adjusted as found necessary.
- Physical access to DLZP Group is out of scope as all systems are virtual.
- Monitoring has been implemented on all DLZP Group systems including recording logon attempts and failures, successful logons and date and time of logon and logoff.
- Activities performed as administrator are logged where it is feasible to do so.
- Personnel who have administrative system access must use other less powerful accounts for performing non-administrative tasks.

28.0 Third Party Access Plan

28.1 Purpose

All consultants, contractors, vendors, and outside parties such as law firms, hereinafter referred to as "Third Party" or "Third Parties" who access data hosted by DLZP Group must comply with this policy. All DLZP Group Third Parties must secure against unauthorized network or physical access, damage or interference to DLZP Group's business operations assets, including but not limited to confidential client information and IT resources. DLZP Group Third Parties are subject to applicable requirements of this policy when they perform work for DLZP Group or its clients. DLZP Group Third Parties who violate this policy will be subject to termination of access and investigation and may result in breach of contract or other penalties.

28.2 Third Party Access General requirements

1. All Third Parties must sign a non-disclosure / confidentiality agreement.
2. Third Parties may only access network and system resources by approved methods.
3. Third Parties must ensure basic security methodologies are in place within their infrastructure (firewall, user access control, etc.).
4. Individuals working for Third Parties are not allowed to share accounts or passwords.

5. Third Parties must ensure that any device connecting to DLZP Group's infrastructure be secured with basic security tools (anti-malware/virus software, firewalls, etc.).
6. In the event of a security incident, DLZP Group reserves the right to request an audit of the third parties processes or methods leading to the incident.
7. Third party must report any known or suspected security-related incident to DLZP Group immediately.
