3.4 Configuration Management

Control Satisfaction Matrix

Standard	Category	Controls Satisfied	800-53r4 Controls	ISO/SEC 27001	A-lign Controls
NIST 800-171	Configuration Management	3.4.1 - 3.4.9	CM-2, CM-6, CM-8, CM-8(1), CM-3, CM-4, CM-5, CM-7, CM-7(1), CM-7(2), CM-7(4), CM-7(5), CM-11	A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3, A.12.2.1, A.6.1.4	8.0, 12.0, 24.0, 25.0, 26.0

Major Document History

Date	Comment	Who
7/26/2019	Initial Doc, Operational and Software Development Change Management Policy - 8.0	Tharp
7/29/2019	Added Encryption Policy 12.0	Tharp
7/30/2019	Added 24.0, 25.0, 26.0	Tharp
8/09/2019	Updated 8.4, 12.5	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 configuration 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

3.4.1

Establish and maintain baseline configurations and inventories of organizational systems (including

hardware, software, firmware, and documentation) throughout the respective system development life cycles.

3.4.2

Establish and enforce security configuration settings for information technology products employed in organizational systems.

3.4.3

Track, review, approve or disapprove, and log changes to organizational systems.

3.4.4

Analyze the security impact of changes prior to implementation.

3.4.5

Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

3.4.6

Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

3.4.7

Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

3.4.8

Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by- exception (whitelisting) policy to allow the execution of authorized software.

3.4.9

Control and monitor user- installed software.

Response Plan

8.0 Operational and Software Development Change Management Policy

8.1 Policy

This policy describes the responsibilities, policies, and procedures to be followed when making changes or recording events to the DLZP Group IT infrastructure and applications.

8.2 Mission Statement

The System Administrators, and Applications teams are tasked with providing a stable and reliable IT infrastructure and applications for DLZP Group. The purpose of this Change Management process is to minimize service disruptions to our computing environment and promote system availability.

8.3 Policy/Procedure Maintenance Responsibility

The System Administrators, and Applications teams are responsible for maintaining and updating this Change Management Policy/Procedure.

8.4 Definitions

Term	Definition
Change	To transform, alter, or modify the operating environment or standard operating procedures; any modification that could have a potential and/or significant impact on the stability and reliability of the infrastructure and impacts conducting normal business operation; any interruption in building environments (i.e., electrical outages) that may cause disruption to the IT infrastructure.
Event	Any activity outside of the normal operating procedures that could have a potential and/or significant impact on the stability and reliability of the infrastructure, i.e. a request to keep a system up during a normal shutdown period. Change and Event will be used interchangeably throughout this document.
Change Request	The official notification of the change/event submitted using Test Track.

8.5 Purpose

The Change Management Process is designed to provide an orderly method in which changes to the IT environment are requested and approved prior to the installation or implementation. The purpose is not to question the rationale of a change, but to ensure that all elements are in place, all parties are notified in advance, and the schedule for implementation is coordinated with all other activities within

the organization.

8.6 Scope

Change Management provides a process to apply changes, upgrades, or modifications to the IT environment. This covers any and all changes to the hardware, software or applications. This process also includes modifications, additions or changes to the, Network or Server virtual infrastructure and software. The process is for any change that might affect one or all of the environments DLZP Group relies on to conduct normal business operations. It also includes any event that may alter the normal operating procedures.

Changes to the IT environment arise from many circumstances, such as:

- Periodic maintenance
- User requests
- Machine and/or software upgrades
- Instantiation of new machines and/or software
- Changes or modifications to the infrastructure
- Environmental changes
- Operations schedule changes
- Changes in hours of availability
- Unforeseen events

The above list is not all-inclusive. If you are unsure if a change needs to be submitted through the Change Management process, you should contact DLZP Group leaders.

8.7 Submission of a Change Request

The requester must submit a change request. All change requests shall be submitted using Zoho. The change request must include enough detail so that all areas know the relative impact of the change and how it may affect other areas. The Zoho change form shall be submitted directly through the web interface. If you do not know how to complete a Zoho request form or you do not know how to access the website, you may contact DLZP leadership. If a change is submitted and is in conflict with a previous change request, the change will not be posted and the responsible project manager will notify the parties of the conflict. The first requested change will remain posted until the parties notify the DLZP Leadership of the resolution, preferably by email. If the parties cannot reach an agreement, the issue shall be elevated to the VP of R & D for resolution, and again the resolution is to be submitted to the DLZP Leadership team.

8.8 Updating, Correcting, or Withdrawing a Change Request

Once a Change Request has been submitted and a situation arises that the request must be updated, corrected, or withdrawn, an email is to be sent to DLZP leadership ASAP requesting the change submission be deleted. A new Zoho change request form must be submitted to the Zoho for updates or corrections. An exception to this requirement may be a minor correction in the content of the previously submitted request. If there is a question as to whether or not a new form should be submitted, please contact DLZP Leadership.

8.9 Emergencies

Emergencies exist only as a result of:

- a user’s computer is completely out of service
- there is a severe degradation of service needing immediate action
- there is an outage in communication with customers or vendors
- a system/application/component is inoperable and the failure causes a negative impact
- a response to a natural disaster
- a response to an emergency business need

All emergencies are handled on an as-required basis with the approval of the System Administrator & DLZP leadership and must follow the guidelines below: Send an email or otherwise call a member of the DLZP Leadership team either before or immediately after the change/event occurs.

The emergency email should include at a minimum the following information:

- what additional users have been affected and who needs to be notified
- external user names and or phone number, when applicable
- if there is a possible work around until the problem is resolved
- approximate time event or change occurred
- the approximate length of the outage
- notification of resolution, if any
- any error messages or alerts if applicable

Emergencies after normal business hours, on the weekend or holidays, will be resolved immediately and reported to the Project Manager. A completed Zoho change incident request form must be submitted through the regular reporting process immediately following when the change was made or the event occurred.

The Project Manager will review all emergency submissions to ensure the change met the criteria for an “emergency change” and to prevent the process from becoming normal practice to circumvent the Change Management Process.

8.10 Responsibilities

8.10.1 System Administrator & Internal Help Desk

The System Administrator & Internal Help Desk will direct the Change Management Process.

The System Administrator & Internal Help Desk responsibilities include the following tasks:

- Analyze and evaluate a Test Track change request as it relates to the impact on the DLZP Group infrastructure.
- Approve or deny the change schedule in accordance with the DLZP Group Change Management Policy, and report any deviations.
- Coordinate the changes/events.
- Notify parties of conflicts needing resolution.
- Send out notifications of any emergency changes or events.

8.10.2 Change Requester

It is the primary responsibility of the individual submitting a request to evaluate the change prior to submission.

The Change Requester's responsibilities include the following tasks:

- Evaluate the impact to the client, customer or vendor
- Document any error messages or alerts
- Document any important contact information (user/customer or vendors name, telephone number, extension or email address)
- Submit a complete, concise, and descriptive Test Track change request form.

Change Request Forms not completed properly will be rejected and returned to the Requester with an explanation for denial.

Once the request is approved the Project Manager will perform the following tasks:

- Ensure that clients are aware of any possible impact.
- Coordinate proper on-site or on-call support as needed to resolve any problems or answer any questions that may occur during installation, or immediately subsequent to installation.
- Contact names and numbers should be available to support staff to obtain additional or outside support.
- Report unplanned outages or problems immediately.
- Provide a status update in the "Notes" section of the Zoho change request form upon completion of the requested change. The completed form must provide an update on the success or failure of the change in detail.

8.11 Unplanned Outages

All unplanned outages shall be reported to the Project Manager immediately. For any major outages, an outage notification report will be available within 24 hours of the resolved outage. The outage notification report will include such information as the type of outage, down time, clients affected, and resolution. All DLZP Group employees are encouraged to provide accurate details of the problem and resolution. Cooperation and participation is required from all levels of management and staff to facilitate generating this report.

8.12 Zoho Prioritization

Following are examples of priorities for Change Management. This list is not all-inclusive. If you have doubts on whether your change should be requested through the Change Management process, contact DLZP leadership.

8.12.1 Severity

8.12.1.1 Cosmetic

Issues regarding the appearance or minor functionality glitches of the application that have little impact to the users being able to perform their jobs.

8.12.1.2 Workaround

Issues where users are still able to perform an activity via other means, but are not able use an application as it was intended.

8.12.1.3 No Workaround

Issues where users are not able to perform an activity by any means.

8.12.1.4 Causes Crash

Issue causes a crash for an application, server or system.

8.12.2 Priority

8.12.2.1 Urgent/Emergency

The problem requires immediate attention where either system failure or mission essential requirements are not available and no work around exists. This problem can apply to the system as a whole or to a user if system access is lost. The corrective action is implemented as soon as the fix is available regardless of change management schedule.

8.12.2.2 High

The problem is of high importance and can justify an out-of-cycle change. This priority is used for problems that meet Urgent requirements, except that a work around exists, or performance degradation for which no temporary work-around is available however delay would not cause adverse mission impact beyond that of inconvenience. These changes must still be controlled, tested and approved prior to implementation on a production system.

8.12.2.3 Medium

Routine Change Requests are judged less operationally important than High Priority and is not critical for implementation. This priority may be used for important software/hardware/network maintenance issues such as version upgrades, utility software, etc. This priority may be used to improve very difficult or awkward implementations for heavily used subsystems on a selective basis. This priority

may be used for development activity or new requirements providing that the activity cannot be accomplished with the lower priority. These problems are resolved and implemented in the next scheduled change cycle.

8.12.2.4 Low

This priority is intended primarily for fixing capabilities that are currently operational but are difficult or awkward to use. It applies also to non-standard implementations, and other assorted irritants.

8.12.2.5 Future Release

This priority is intended primarily for gathering new requirements regarding unscheduled projects.

8.13 Types of Changes

Following are examples of candidates for Change Management. This list is not all-inclusive. If you have doubts on whether your change should be requested through the Change Management process, contact the Internal Help Desk.

8.13.1 Applications and Information Systems

Implementation of new applications, volume changes, new systems, new releases, or modifications. Migration from test to production of source code.

8.13.2 Backups and restores

Restoring data from backups, or performing special backups. If it is a restore, the reason for the restore must be provided, i.e. what happened to the original data.

8.13.3 Computing Systems Machines

Hardware changes, additions, deletions, re-configurations, re-locations, preventive, or emergency maintenance.

8.13.4 Computing Systems Software

Program or OS hotfixes, product releases, versions, I/O and Network Control Programs (NCP), table changes, tuning, alterations to libraries, catalogs, monitors, traps, or changes to priority mechanisms, job classes, print classes.

8.13.5 Environmental

Power, UPS systems, generators, electrical work, facility maintenance, security systems, fire control systems.

8.13.6 Network Systems

Additions, modifications, deletions to configurations. Software components either distributed or centralized, router software, printing routines, servers.

8.13.7 Operating procedures

Changes in systems downtime schedules, planned system outages, changes in delivering services, or changes to service levels.

8.13.8 Web Applications

Requests for new functionality, maintenance, and bug fixes. This also includes requests to fix system crashes, unplanned downtimes, and sluggish performance. Requests for new functionality must also go through the IT Intake and Development Process as documented in the Intake and Development Procedure.

12.0 Encryption Policy

12.1 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

12.2 Scope

This policy applies to all DLZP Group employees and affiliates.

12.3 Policy

Proven, standard algorithms such as 3DES, RSA, and RC5 should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, PGP Corporation’s Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-

Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 256 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. DLZP Group's key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question. Be aware that the U.S. Government restricts the export of encryption technologies. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

12.4 Enforcement

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

12.5 Definitions

Term	Definition
Proprietary Encryption	An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.
Symmetric Cryptosystem	A method of encryption in which the same key is used for both encryption and decryption of the data.
Asymmetric Cryptosystem	A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

—-

24.0 Server Documentation Policy

24.1 Overview

This policy is an internal DLZP Group policy and defines the requirements for server documentation. This policy defines the level of server documentation required such as configuration information and services that are running. It defines who will have access to read server documentation and who will have access to change it. It also defines who will be notified when changes are made to the servers.

24.2 Purpose

This policy is designed to provide for systems stability by ensuring that systems documentation is complete and current. This policy should complement disaster management and recovery by ensuring that documentation is available in the event that systems should need to be rebuilt. This policy will help reduce troubleshooting time by ensuring that appropriate personnel are notified when changes are made to any servers.

24.3 Documentation

For every server on a secure network, there is a list of items that must be documented and reviewed on a regular basis to keep a private network secure. This list of information about every server should be created as servers are added to the network and updated regularly.

1. Server name
2. Server location
3. The function or purpose of the server.
4. Components of the system including the type of each system.
5. List of essential software running on the server including operating system, programs, and services running on the server.
6. Configuration information about how the server is configured including:
    1. Event logging settings
    2. Configuration of any security lockdown tool or setting
    3. Account settings
    4. Configuration and settings of software running on the server.
7. Types of data stored on the server.
8. The sensitivity of data stored on the server.
9. Data on the server that should be backed up along with its location.
10. Users or groups with access to data stored on the server.
11. Administrators on the server with a list of rights of each administrator.
12. The authentication process and protocols used for authentication for administrators on the server.
13. Latest patch to operating system.
14. Disaster recovery plan and location of backup data.

24.4 Access Control

The DLZP Group Administrator and Project Managers have full read and change access to server documentation for the server or servers they are tasked with administering.

24.5 Change Notification

The administration staff, application developer staff, and executive management shall be notified when changes are made to servers. Notification shall be through email to designated groups of people.

24.6 Documentation Review

DLZP Group's Administrator ensures that server documentation is kept current by performing a quarterly review of documentation or designating a staff member to perform a review. The Zoho requests within the last quarter should be reviewed to help determine whether any server changes were made. Also any current or completed projects affecting server settings should be reviewed to determine whether there were any server changes made to support the project.

24.7 Storage Locations

DLZP Group's server documentation is kept either in electronic form in a Dropbox in the respective project folder.

25.0 Server Security Policy

25.1 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by DLZP Group. Effective implementation of this policy will minimize unauthorized access to DLZP Group proprietary information and technology.

25.2 Scope

This policy applies to server equipment owned and/or operated by DLZP Group, and to servers registered under any DLZP Group-owned internal network domain.

This policy is specifically for equipment on the internal DLZP Group network.

25.3 Policy

25.3.1 Ownership and Responsibilities All internal servers deployed at DLZP Group must be operated by the Systems Administrator. Approved server configuration guides must are established and maintained by DLZP Leadership, based on business needs. The Systems Administrator should monitor configuration compliance and implement an exception policy tailored to the server's environment. The Server Administrator must establish a process for changing the

configuration guides, which includes review and approval by DLZP Group.

- Servers must be documented according the Server Documentation Policy.
- Configuration changes for production servers must follow the appropriate change management procedures.

25.3.2 General Configuration Guidelines

- Operating System configuration should be in accordance with approved DLZP Group guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least privileged access to perform a function.
- Do not use the administrator account when a non-privileged account will do.
- If a methodology for a secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSL or IPSec).

25.3.3 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved to the Syslog servers.
- Security-related events will be reported to the Systems Administrator, who will review logs and report incidents. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

25.3.4 Compliance

- Audits will be performed on a regular basis by DLZP Group.
- Audits will be managed by the DLZP leadership. Systems Administrators will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

25.4 Enforcement

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

25.5 Definitions

Term	Definition
DMZ	Demilitarized Zone. A network segment external to the corporate production network.
Server	For purposes of this policy, a Server is defined as an internal DLZP Group Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.
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
Account Lockout Policy	Where possible a lockout policy will be enforced to disable login for 24 hours when 3 incorrect login attempts are made without success.

26.0 Source Code Control Policy

26.1 Revision Control

Source code revision control is accomplished utilizing a git repo whose data is kept on a S3 storage system. Git is an open-source revision control solution. Access to the code repository is limited using folder-level permissions which are customized for each authorized user.

A separate release branch is maintained in the repository which allows revisions to be selectively released as they are deemed stable after being fully tested and accepted by all affected users. The production package is built from this release branch, which only the change manager has write access to, so developers have no way of directly releasing their own code. The software manager will merge changes from the main code trunk to the release branch only after the Business Analysis and Quality Assurance teams advise him that the change is authorized to be deployed.

Revisions are not released individually; all revisions for a given project will be released at the same time. Projects are tracked using the Zoho issue management. Each project is given a unique identifier in Zoho which is used to track the project from inception to completion. All code committed to the repository requires an associated issue. T

TT##### - Description of changes made goes here

When a given project is authorized for release, the change manager will merge all of the revisions associated with that project from the code trunk to the release branch in a single atomic action. This allows the change to easily be removed from the production build in the unlikely event that any unforeseen complications arise.

26.2 Source Control Life Cycle

The life-cycle of a single issue is as follows:

1. Zoho issue is created after Business Analysis team verifies business needs of project and Software Development team verifies changes are required
2. Issue is assigned to a developer who creates a development branch that starts as a copy of the

code trunk and tracks all changes the developer makes for the issue
3. Developer completes development of project, merges changes from their development branch into the code trunk and assigns the issue to the release manager
4. Release manager creates a test build from the code trunk, releases the test build to the testing site and assigns the issue to the Quality Assurance team
5. After Quality Assurance team verifies changes are working as intended the issue is assigned to the Business Analysis team and users are chosen for acceptance testing
6. Once all testing and acceptance is completed, project is assigned back to the release manager and is added to a scheduled release
7. All affected parties are notified of the release date which is to be no later than 30 days from completion of all testing
8. When the scheduled release date arrives the projects slated for release are merged into the release branch by the release manager who then builds the new version of the application
9. During scheduled downtime the night of the release the new version of the application is deployed to the production servers by the change manager and the Zoho issue is closed