3.6 - Incident Response

Control Satisfaction Matrix

Standard	Category	Controls Satisfied	800-53r4 Controls	ISO/SEC 27001	Audit Controls
NIST 800-171	Incident Response	3.6.1-3.6.3	IR-2, IR-4, IR-5, IR-6, IR-7, IR-3	A.7.2.2, A.16.1.4, A.16.1.5, A.16.1.6, A.6.1.3, A.16.1.2	14.0, 15.0

Major Document History

Date	Comment	Who
5/13/2019	Initial Doc	Tharp
5/29/2019	Added Control Objectives, Assertions, Tests, Action Items	Tharp
6/21/2019	CO's & Assertions updated with feedback from B&V CPA's	Tharp
7/29/2019.	Added 14.0, 15.0	Tharp
7/30/2019	Strike thru control Objectives	Tharp
8/09/2019	Updated 14.4	Tharp
8/12/2019	Formatting	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 incident systems and methods that are well reflected in operational methods and processes to support our clients business and technology needs.

Background

Clients depend on our prompt response to their problem escalations as well as a clear understanding of problem resolution. Well documented problem tickets are also important to communicate internally within our technical and functional teams for prompt problem resolution should escalation and help is sought from another internal resource.

Policy

3.6.1

DLZP Group provides each client established incident response and escalation processes Example Here. Each client Operation's Runbook includes at minimum: escalation process, contacts, primary support hours, agreed upon service levels, and client contacts and order of escalation. Incidents may

be raised by clients or DLZP functional or technical staff as well as monitoring infrastructure configure per the clients hosting Statement of Work.

3.6.2

Every incident will be tracked via an Issue Ticket in the clients discreet Project Management Project.

3.6.3

From time to time DLZP Executives may declare a client related incident to examine, response time and escalation efficacy.

Standard Support

For standard support, requests are submitted to the DLZP Support Site or via one of the methods in the Raise Ticket swim lane in **Figure 1**. You will be provided access to the DLZP Support Site upon engagement, and you contact your account representative or Project Manager to report issues. Support during non-business hours may be communicated via support email or the DLZP Group support phone number. DLZP will respond to all client-raised incidents and resolve them based on the Issue Severity that is declared by the client in **Table 1**. DLZP Support Site Documentation and Project User Guide, will be provided to new clients.

Figure 1

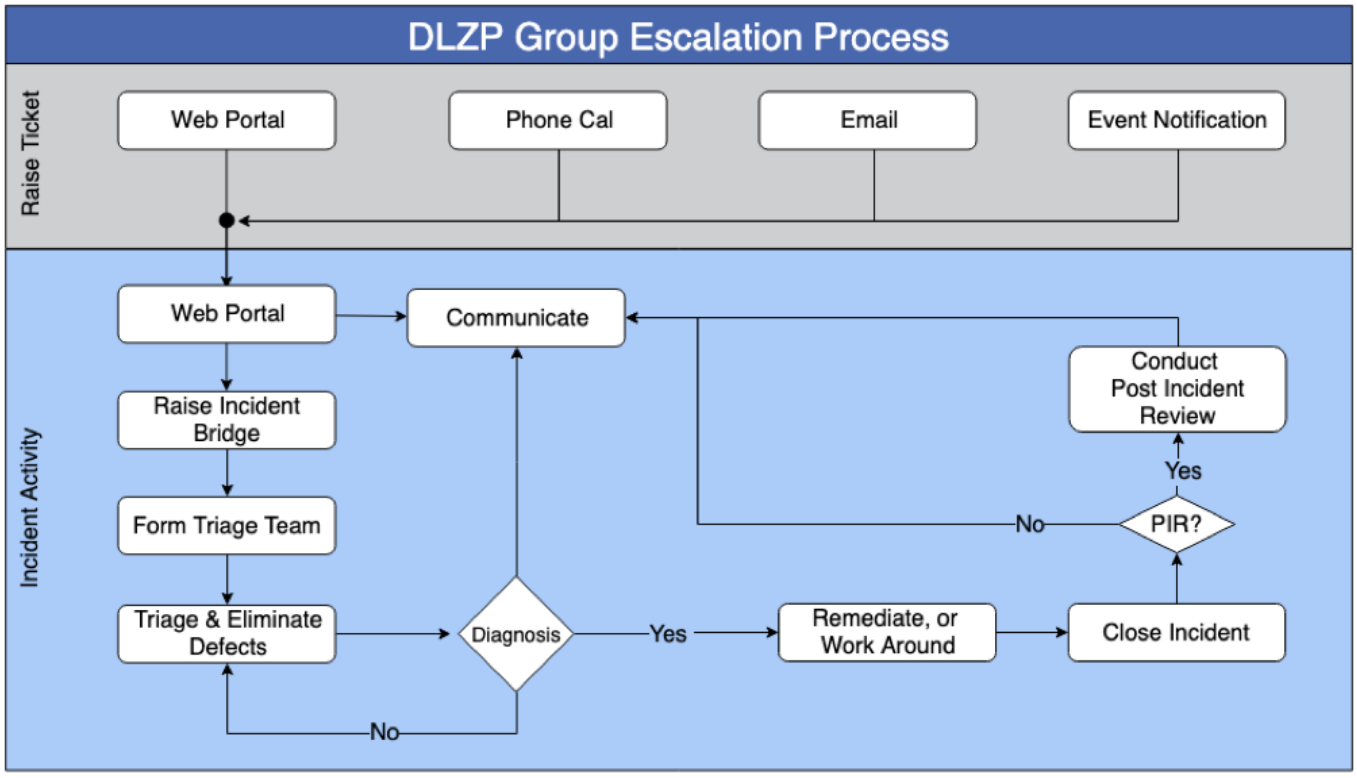

Table 1

Issue Severity	Response Time Within:	Resolution Targets
Critical: Critical business services are not operational Production systems are unavailable Data integrity is at risk No workaround is available	1 Hour	DLZP will work to resolve or provide a work around within 2 hours of customer request. Subject to fulfillment vendor support policies.
High: A core application component is impacted System is operational but in a restricted capacity, and productivity is adversely affected Data has been lost A temporary work around is available	4 Hours	DLZP will work to resolve or provide a work around within 8 hours of customer request. Subject to fulfillment vendor support policies.
Medium: Application or system is still functioning with non-critical loss of functionality Issue can be circumvented No risk to data	24 Hours	DLZP will work to resolve or provide a work around within 48 hours of customer request. Subject to fulfillment vendor support policies.
Low: Cosmetic issues, or requested changes to functionality Non-critical issues Enhancement request not requiring development activity	48 Hours	DLZP will work to resolve or provide a work around within 96 hours of customer request. Subject to fulfillment vendor support policies.

Response Plan

14.0 Incident Handling Policy

14.1 Overview

DLZP Group is increasingly dependent on data and network resources. Proper detection and response to incidents that may impact the integrity, confidentiality or availability of these resources is critical to the operation of the company. Such incidents include, but are not limited to: virus outbreaks, remote security breaches, denial-of service attacks, and other exploited vulnerabilities.

The following standards were developed by DLZP Group to prepare those employed by or affiliated with the company to properly detect and respond to incidents of any kind. Individuals are encouraged to implement any additional plans they deem necessary. These recommendations should not be used to reduce the level of preparedness that may already exist.

These minimum standards apply to all DLZP Group departments and affiliates, as well as contractors and vendors handling DLZP Group’s systems or data. They represent the recommended minimum planning and cooperative efforts necessary to ensure the best incident detection and response possible.

14.2 Security Incident Detection

DLZP Group users and administrators should be alert for symptoms that indicate and intrusion into

their systems. The following points are helpful in detecting intrusions:

Be suspicious of unusual activity – unusual computer or network activity can be an indicator of a virus, attack, or intrusion. Activities and symptoms to look for include:

- Excessive virus warnings or personal firewall pop-up messages
- Unexpected system reboots and/or sudden degradation of system performance
- Unauthorized new user accounts or altered passwords
- New directories or files, often with unusual names such as "…" or " .."
- Modification or defacement of web sites
- New open network ports on a system
- Unexpectedly full disk drives

Listen to complaints received from others – comments or emails claiming suspicious activity from a computer may indicate the machine is infected or has been compromised and may actively be attacking other computers.

DLZP Group regularly reviews server logs through – log files are invaluable in detecting and tracking attempted intrusions and other suspicious activity. To maximize the value of logs, the DLZP Group System Administrator:

- Ensures that a very high level of logging is enabled
- Checks logs regularly for suspicious activities and entries
- Monitors email alerts for suspicious activities
- Looks for missing time spans in logs
- Checks for repeated login failures or account lockouts
- Investigates unexpected system reboots
- Scans corporate antivirus logs for alerts and threat warnings

14.3 Incident Response

All DLZP Group system users should immediately report suspicious activity to DLZP leadership. Administrators will refer to DLZP Group's Incident Response Guidelines for technical assistance in investigating the incident.

This policy is applicable to any incident that occurs at DLZP Group, including but not limited to security incidents, theft, property damage, denial of service, threats, harassment and/or other criminal offenses involving individual user accounts, forgery and/or misrepresentation.

14.4 Definitions

Term	Definition
Incident	Any adverse event which compromises some aspect of DLZP Group computer or network functionality/security, or business operations.
Vulnerability	A characteristic piece of technology which can be exploited to perpetrate a security incident.

15.0 Incident Response Guidelines

15.1 Overview

DLZP Group computer users must be prepared to respond properly when a security incident occurs. DLZP takes a proactive approach to incident handling. A solid plan of attack for different types of security incidents is crucial to the continuance and/or restoration of normal operations at DLZP.

15.2 Purpose

The purpose of this document is to provide security personnel and administrators with guidelines for incident handling at DLZP.

15.3 Scope

These minimum standards apply to all DLZP departments and affiliates, including contractors and vendors handling DLZP systems or data.

15.4 Guidelines

Responses to specific incidents may include:

15.4.1 Incident Evaluation and response

- Check all systems for new or modified accounts
- Review log files for abnormal entries or missing time spans
- Look for modifications made to system software and/or configuration files
- Scan system for new binaries (including user directories)
- Check other local systems and related remote systems
- Change system password(s)
- Clean and/or reformat the system as appropriate

15.4.2

- Fill out a Test Track form in accordance with 8.7 Submission of a Change Request
- Contact the Internal Help Desk immediately to discuss the nature of the incident