3.13 SYSTEM AND COMMUNICATIONS PROTECTION

Control Satisfaction Matrix

Standard	Category	Controls Satisfied	800-53r4 Controls	ISO/SEC 27001	A-lign Controls
NIST 800-171	Systems & Communications Protection	3.13.1 - 3.13.16	SC-4, SC-7, SC-7(5), SC-7(7), SA-8SC-2, SC-8, SC-8(1), SC-10, SC-12, SC-13, SC-15, SC-18, SC-19, SC-23, SC-28	A.8.2.3, A.10.1.1, A.10.1.2, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3, A.14.2.5, A.18.1.5	13.0, 18.0, 20.0, 21.0, 27.0

Major Document History

Date	Comment	Who
7/29/2019	Initial Doc, 13.0	Tharp
7/30/2019	Added 18.0, 20.0, 21.0	Tharp
7/30/2019	Strike thru control Objectives	Tharp
8/09/2019	Updated 13.5, Replaced terms with DLZP Group	Tharp
8/12/2019	Formatting Updates, Added 27.0	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 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

3.13.1

Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

3.13.2

Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

3.13.3

Separate user functionality from system management functionality.

3.13.4

Prevent unauthorized and unintended information transfer via shared system resources.

3.13.5

Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

3.13.6

Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

3.13.7

Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

3.13.8

Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

3.13.9

Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

3.13.10

Establish and manage cryptographic keys for cryptography employed in organizational systems.

3.13.11

Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

3.13.12

Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

3.13.13

Control and monitor the use of mobile code.

3.13.14

Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

3.13.15

Protect the authenticity of communications sessions.

3.13.16

Protect the confidentiality of CUI at rest.

Response Plan

13.0 Extranet Plan

13.1 Purpose

This document describes the Plan under which third party organizations connect to DLZP Group networks for the purpose of transacting business related to DLZP Group.

13.2 Scope

Connections between third parties that require access to non-public DLZP Group resources fall under this Plan, regardless of the technology used for the connection. Connectivity to third parties such as the Internet Service Providers (ISPs) that provide Internet access for DLZP Group or to the Public Switched Telephone Network does NOT fall under this Plan.

13.3 Plan

13.3.1 Pre-Requisites

13.3.1.1 Security Review

All new extranet connectivity will go through a security review by DLZP leadership. The reviews are to ensure that all access matches the business requirements in the best possible way, and that the principle of least required access is followed.

13.3.1.2 Third Party Connection Agreement

All new connection requests between third parties and DLZP Group require that the third party and DLZP Group representatives agree to and sign an Agreement. This agreement must be signed by the DLZP Group executive management as well as a representative from the third party who is legally empowered to sign on behalf of the third party. The signed document is to be kept on file with the relevant extranet group.

13.3.1.3 Business Case

All production extranet connections must be accompanied by a valid business justification, in writing, that is approved by DLZP leadership. Typically this function is handled as part of the Third Party Agreement.

13.3.1.4 Point of Contact

The Sponsoring Organization must designate a person to be the Point of Contact (POC) for the

Extranet connection. The POC acts on behalf of the Sponsoring Organization, and is responsible for those portions of this Plan and the Third Party Agreement that pertain to it. In the event that the POC changes, the relevant extranet organization must be informed promptly.

13.3.2 Establishing Connectivity

Sponsoring Organizations within DLZP Group that wish to establish connectivity to a third party are to file a new site request with the proper extranet group. The extranet group will engage IT management to address security issues inherent in the project.

All connectivity established must be based on the least-privalaged access principle, in accordance with the approved business requirements and the security review. In no case will DLZP Group rely upon the third party to protect DLZP Group’s resources.

13.3.3 Modifying or Changing Connectivity and Access

All changes in access must be accompanied by a valid business justification, and are subject to security review. Changes are to be implemented via corporate change management process. The Sponsoring Organization is responsible for notifying IT management when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

13.3.4 Terminating Access

When access is no longer required, the Sponsoring Organization within DLZP Group must notify the extranet team responsible for that connectivity, which will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate. The extranet and lab security teams must conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections that are found to be depreciated, and/or are no longer being used to conduct DLZP Group business, will be terminated immediately. Should a security incident or a finding that a circuit has been deprecated and is no longer being used to conduct DLZP Group business necessitate a modification of existing permissions, or termination of connectivity, IT management will notify the POC or the Sponsoring Organization of the change prior to taking any action.

13.4 Enforcement

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

13.5 Definitions

Term	Definition
Circuit	For the purposes of this Plan, circuit refers to the method of network access.
Sponsoring Organization	The DLZP Group organization who requested that the third party have access into DLZP Group.

Term	Definition
Third Party	A business that is not a formal or subsidiary part of DLZP Group.

18.0 Network Documentation Plan

18.1 Overview

This network documentation Plan is an internal DLZP Group Plan and defines the requirements for network documentation. It defines who will have access to read network documentation and who will have access to change it. It also defines who will be notified when changes are made to the network.

18.2 Purpose

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

18.3 Documentation

DLZP Group maintains all of its infrastructure in AWS cloud and may support other cloud environments in the future. The following virtual equivalents of these legacy services will be documented based on actual cloud services usage.

The network structure and configuration shall be documented and provide the following information:

1. IP addresses of all devices on the network with static IP addresses.
2. Server documentation on all servers as outlined in the “Server Documentation” document.

Network drawings showing:

1. The locations and IP addresses of all hubs, switches, routers, and firewalls on the network.
2. The various security zones on the network and devices that control access between them.
3. The interrelationship between all network devices showing lines running between the network devices.
4. All subnets on the network and their relationships including the range of IP addresses on all subnets and subnet mask information.
5. All wide area network (WAN) or metropolitan area network (MAN) information including network devices connecting them and IP addresses of connecting devices.

4. ItemConfiguration information on all network devices including:

    1. Switches

2. Routers
3. Firewalls

5. Configuration includes but is not limited to:

    1. IP Address
    2. Subnet mask
    3. Default gateway
    4. DNS server IP addresses for primary and secondary DNS servers.

6. Network connection information including:

    1. Type of connection to the internet or other WAN/MAN including cable, T1, or fiber.
    2. Provider of internet/WAN/MAN connection and contact information for sales and support.
    3. Configuration information including subnet mask, network ID, and gateway.
    4. Physical location of where the cabling enters the building and circuit number.

7. DHCP server settings showing:

    1. Range of IP addresses assigned by all DHCP servers on all subnets.
    2. Subnet mask, default gateway and DNS server settings assigned by all DHCP servers on all subnets.
    3. Lease duration time.

18.4 Access

IT Department Management have full access to all network documentation. IT Department Management shall have the ability to read and modify network documentation. Designated enterprise security staff shall have access to read and change network documentation but those not designated with change access cannot change it.

18.5 Change Notification

Appropriate groups of people shall be notified through email when network changes are made including:

1. Reboot of a network device including switches, routers, and firewalls.
2. Upgrades to any software on any network device.
3. Additions of any software on any network device.
4. Changes to any servers which perform significant network functions whether configuration or upgrade changes are made. These servers include:

    1. DHCP
    2. DNS
    3. Domain controllers

18.6 Documentation Review

The Network Administrator shall ensure that network documentation is kept current by performing a quarterly review of documentation or designating a staff member to perform a review. The Test Track requests within the last quarter should be reviewed to help determine whether any network changes were made. Also any current or completed projects affecting network settings are reviewed to determine whether there were any network changes made to support the project.

18.7 Storage Locations

Network documentation is kept in electronic form in a minimum of two places.

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

20.0 Remote Access Plan

20.1 Purpose

The purpose of this Plan is to define standards for connecting to DLZP Group’s network from any host. These standards are designed to minimize the potential exposure to DLZP Group from damages that may result from unauthorized use of DLZP Group’s resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical DLZP Group’s internal systems, etc.

20.2 Scope

This Plan applies to all DLZP Group employees, contractors, vendors and agents with a DLZP Group-owned or personally-owned computer or workstation used to connect to the DLZP Group network. This Plan applies to remote access connections used to do work on behalf of DLZP Group, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this Plan include, but are not limited to, cable modems, DSL, VPN (using an encrypted VPN client), etc.

20.3 Plan

20.3.1 General

1. It is the responsibility of DLZP Group’s employees, contractors, vendors and agents with remote access privileges to DLZP Group’s corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to DLZP Group’s

network.

2. General access to the Internet for recreational use by immediate household members through the DLZP Group network on personal computers is not permitted for employees. The DLZP Group employee bears responsibility for the consequences should the access be misused.

3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of DLZP Group's network:

1. Acceptable Encryption Plan
2. Virtual Private Network (VPN) Plan
3. Wireless Communications Plan
4. Acceptable Use Plan

4. For additional information regarding DLZP Group's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., contact the DLZP Leadership.

20.3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via password authentication or shared keys. For information on creating a strong password see the Password Plan.

2. At no time should any DLZP Group employee provide their login or email password to anyone, not even family members.

3. DLZP Group employees and contractors with remote access privileges must ensure that their DLZP Group-owned or personal computer or workstation, which is remotely connected to DLZP Group's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

4. DLZP Group employees and contractors with remote access privileges to DLZP Group's corporate network must not use non-DLZP Group email accounts (i.e., Hotmail, Yahoo, AOL, GMail), or other external resources to conduct DLZP Group business, thereby ensuring that official business is never confused with personal business.

5. Reconfiguration of a home user's equipment for the purpose of split-tunneling is not permitted at any time.

6. Non-standard hardware configurations must be approved by System Administrator, and must use approved security configurations for access to hardware.

6. All hosts that are connected to DLZP Group internal networks via remote access technologies must use the most up-to-date anti-virus software and definitions, and this includes personal computers. Third party connections must comply with requirements as stated in the Third Party Agreement.

8. Personal equipment that is used to connect to DLZP Group's networks must meet the requirements of DLZP Group-owned equipment for remote access.

9. Organizations or individuals who wish to implement non-standard Remote Access solutions to

the DLZP Group production network must obtain prior approval from DLZP leadership.

20.4 Enforcement

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

20.5 Definitions

Term	Definition
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 5 Mbps.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a DLZP Group-provided Remote Access home network, and connecting to another network, such as a spouse's remote access.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Remote Access	Any access to DLZP Group’s corporate network through a non-DLZP Group controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-DLZP Group network (such as the Internet, or a home network) from a remote device (PC, PDA, etc.) while connected into DLZP Group’s corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via “tunneling” through the Internet.

21.0 VPN Plan

21.1 Purpose

The purpose of this Plan is to provide guidelines for Remote Access Virtual Private Network (VPN) connections to the DLZP Group corporate network.

21.2 Scope

This Plan applies to all DLZP Group employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing a VPN to access the DLZP Group network.

21.3 Plan

Approved DLZP Group employees and authorized third parties (customers, vendors, etc.) may utilize

the benefits of a VPN, which is a “user managed” service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, and paying any associated fees. Further details may be found in the Remote Access Plan. Additionally,

1) It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to DLZP Group internal networks.

2) VPN use is to be controlled using strong password authentication and shared key.

3) When actively connected to the corporate network, the VPN will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.

4) Dual (split) tunneling is NOT permitted; only one network connection is allowed at a time.

5) VPN gateways (through SonicWALL) will be set up and managed by the System Administrator.

6) All computers connected to DLZP Group internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard TrendMicro; this includes personal computers.

7) Users of computers that are not DLZP Group-owned equipment must configure the equipment to comply with DLZP Group’s VPN and Network policies.

8) Only the authorized encrypted VPN client may be used for VPN access.

9) By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of DLZP Group’s network, and as such are subject to the same rules and regulations that apply to DLZP Group-owned equipment, i.e., their machines must be configured to comply with DLZP Group’s Security Policies.

21.4 Enforcement

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

21.5 Definitions

Term	Definition
Dual (split tunneling)	The practice of connecting to DLZP Group network resources via VPN while simultaneously connecting to a second tunnel (i.e. the internet).

27.0 Wireless Communication Plan

27.1 Purpose

This Plan prohibits access to DLZP Group networks via unsecured wireless communication mechanisms.

27.2 Scope

This Plan covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of DLZP Group's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to DLZP Group's networks do not fall under the purview of this Plan.

27.3 Plan

27.3.1 Register Access Points and Cards All wireless Access Points / Base Stations connected to the corporate network must be registered and approved by DLZP Group's Network Administrator. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in corporate laptop or desktop computers must be registered with DLZP Group.

27.3.2 Approved Technology All wireless LAN access must use corporate-approved vendor products and security configurations.

27.3.3 VPN Encryption and Authentication All computers with wireless LAN devices must utilize a corporate-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. To comply with this Plan, wireless implementations must maintain point to point hardware encryption of at least 256 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must support and employ strong user authentication.

27.4 Enforcement

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