<< Zscaler >>

Standard Operating Procedure

<<Insert Document Number>>

<<June 2024>>

1. 

Table of Contents

[Table of Contents i](#_Toc172552447)

[Table of Figures iii](#_Toc172552448)

[Table of Tables iii](#_Toc172552449)

[Revision History iv](#_Toc172552450)

[1 Introduction 1](#_Toc172552451)

[Purpose 2](#_Toc172552452)

[1.1 Intended Audience 2](#_Toc172552453)

[1.2 Roles and Responsibilities 2](#_Toc172552454)

[1.3 Primary Points of Contact 2](#_Toc172552455)

[1.4 Related Documents 2](#_Toc172552456)

[2 <<Insert Section Title>> 1](#_Toc172552457)

[3 Service CI 1](#_Toc172552458)

[4 Zscaler Client Connector 1](#_Toc172552459)

[4.1 Installation Packages 2](#_Toc172552460)

[4.2 Zscaler Client Connector Tray Icon Options 2](#_Toc172552461)

[5 Triage 1](#_Toc172552462)

[5.1 Common Support Issues 2](#_Toc172552463)

[5.1.1 Blocked Website 2](#_Toc172552464)

[6 Responsible, Accountable, Supported, Consulted, Informed (RASCI) Matrix 1](#_Toc172552465)

[7 Related Controls 4](#_Toc172552466)

[7.1 Control Activity Summary 4](#_Toc172552467)

[7.2 Records Management 4](#_Toc172552468)

[8 Approvals 5](#_Toc172552469)

[9 Appendices 6](#_Toc172552470)

[Appendix A: Key Terms and Acronyms 6](#_Toc172552471)

[Appendix B: <<Insert Appendix Title>> 7](#_Toc172552472)

# Table of Figures

[Figure 1: Detailed Design Diagram 4](#_Toc172552480)

[Figure 2: Flow Diagram 5](#_Toc172552481)

[Figure 3: Zscaler Client Connector icon 8](#_Toc172552482)

[Figure 4: Zscaler Client Connector Notifications 8](#_Toc172552483)

[Figure 5: Zscaler Client Connector 9](#_Toc172552484)

[Figure 6: Zscaler Troubleshoot menu (Windows) 12](#_Toc172552485)

[Figure 7: Zscaler Troubleshoot menu (macOS) 14](#_Toc172552486)

# Table of Tables

[Table 2: Revision History iv](#_Toc172552473)

[Table 3: Roles and Responsibilities Summary 2](#_Toc172552474)

[Table 4: Document Points of Contact Summary 2](#_Toc172552475)

[Table 5: Related Documents Summary 2](#_Toc172552476)

[Table 6: Control Activities Summary 4](#_Toc172552477)

[Table 7: Records Management Summary 4](#_Toc172552478)

[Table 8: Key Terms and Acronyms 6](#_Toc172552479)

Revision History

Table 2: Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Effective | Version | Change Summary | Point of Contact |
| <<June 2024>> | 1.0 | Initial Release | <<Insert POC Name>> |

# Introduction

This document defines the scope and roles and responsibilities for the Cybersecurity Services that the Consumer Financial Protection Bureau (“CFPB” or the “Bureau”) has provisioned from the Department of Justice (DOJ) and Zscaler. As an outcome of the Discovery Project that CFPB and DOJ completed, DOJ will provide recommendations for the deployment of its Justice Edge Trust Service (JETS) tailored to CFPB technical and operating environment. JETS is built on top of a secure and scalable infrastructure that provides end to end encryption and strong authentication to ensure the confidentiality and privacy of transmitted data. Based on the information gathered during the Discovery project, CFPB selected capabilities will be listed on scope of work and defined.

To successfully integrate cloud computing and Software-as-a-Service (SaaS) for almost all its requirements, the CFPB is implementing a Zero Trust Architecture (ZTA). The general ZTA plan is to outsource market-supported commodity work and shift practically all current computing and data workloads to AWS. Legacy applications will also be replaced with comparable SaaS services. This will eventually enable the Bureau to lessen and scale back its reliance on the Local Area Network (LAN) and conventional network security models in order to access vital technological services and instead adopt key Zero Trust principles such as never trust and always verify based on identity with multi-factor authentication, device trust, and important security attributes like location, micro segmentation, and least privilege.

The Bureau will utilize DOJ JETS for the administration of CFPB's Zscaler tenants. DOJ will have the responsibility to make all configuration and policy changes that have been approved and requested by CFPB.

## Purpose

The purpose of this standard Operating Procedures (SOP) is to provide overview and instruction how to triage and escalate requests and incidents.

## Intended Audience

The CFPB Service Desk which includes, Service Desk (Tier I), Desktop Support (Tier II), Active Directory (AD) Management, and Incident Management teams.

## Roles and Responsibilities

Table 3: Roles and Responsibilities Summary

|  |  |
| --- | --- |
| Role | Responsibility |
| **Service Desk (Tier I)** | * First User contact * Provide initial triage of incidents * Assist users to the correct Request Catalog |
| **Deskside Support (Tier II)**  **AD Management Team**  **Incident Management** | Further troubleshooting and documenting issues, including capture screen shots and logs. |
| **Desktop Engineering** | 3rd level support for the Zscaler Client for MACs and Windows |
| **Network Management** | Deep dive into Network related issues, including capturing screen shots and logs (if necessary; escalate to DOJ or resolve |
| **ETS Mobility** | * 3rd Tier Support for Zscaler client issues on IOS and Android devices. * Android devices – Desktop Audiocode phones located in limited (Director’s office and SCC). |

## Primary Points of Contact

Table 4: Document Points of Contact Summary

|  |  |  |
| --- | --- | --- |
| Role | Point of Contact | Contact Topics |
| **System Owner**  \*This role must always be a Lead or higher | Name: Ali Sadeghi  Title: Senior Infrastructure Engineer  T&I Office: Infrastructure | * Providing oversight and system owner function for the solution. |
| **Network Management** | Name: Walter Riddle Title: Network Engineer | * Network Engineering SME |
| **Desktop Engineering** | Name: Cesar Carvajal  Title: Infrastructure End-User Strategy Lead | * Desktop Engineering SME |
| **Service Desk** | Name: Cathy Hurkamp  Title Sr Service Desk Specialist | * Tier I/II support |

## Related Documents

Table 5: Related Documents Summary

|  |  |  |
| --- | --- | --- |
| Document Name | Brief Description | Location or Link |
| KB0014228 Reconnect to Always On VPN Zscaler on Windows | The **Zscaler Test – AnyConnect Profile** – Switcher utility was created to allow Windows laptops to disconnect from the VPNs while maintaining internet connectivity in support of Zscaler Pilot Phase. The utility has been made available to your Microsoft Windows laptop for install via SCCM. | https://cfpbprod.servicenowservices.com/kb\_view.do?sysparm\_article=KB0014228 |
| KB0014229 Connect to Zscaler VPN for Macs | The **Zscaler Test – AnyConnect Profile** – Switcher utility was created to allow Mac laptops to disconnect from the VPNs while maintaining internet connectivity in support of Zscaler Pilot Phase. The utility has been made available to your Mac laptop for install via Self Service. | https://cfpbprod.servicenowservices.com/kb\_view.do?sysparm\_article=KB0014229 |

# <<Insert Section Title>>

Figure : **Detailed Design Diagram**

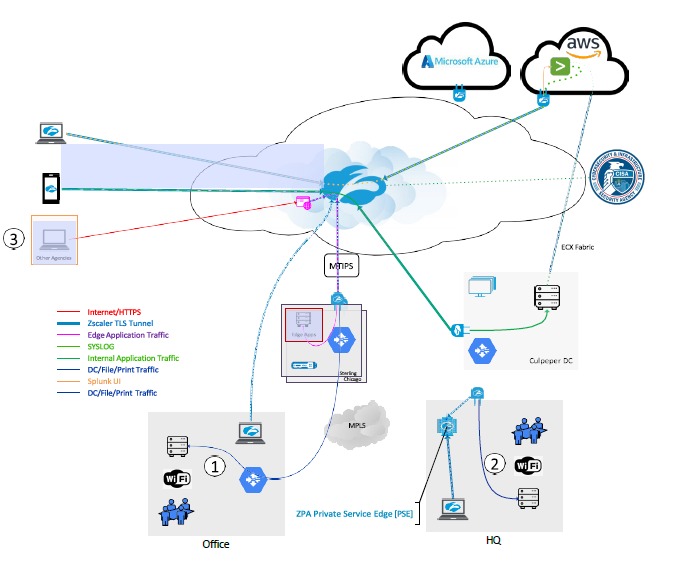
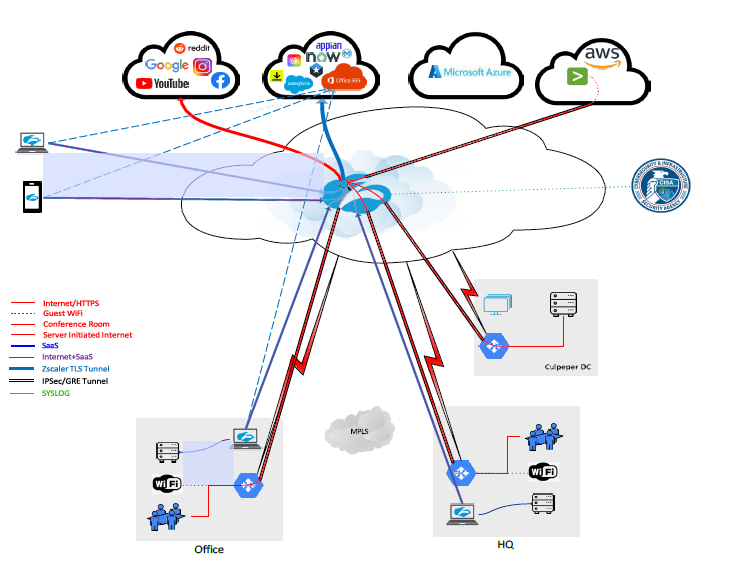


Figure : **Flow Diagram**



# Service CI

**Service CI -** [Zscaler JETS Prod](https://cfpbprod.servicenowservices.com/cmdb_ci_service.do?sys_id=0cecd4cd1b75691044f587fbe54bcbca&sysparm_record_target=cmdb_ci_service&sysparm_record_row=1&sysparm_record_rows=1&sysparm_record_list=nameCONTAINSzscaler%5EORDERBYname)

# Zscaler Client Connector

Zscaler Client Connector is an application installed on all CFPB end-user device(s) (iPhone, Macs, and Dell laptops) to ensure internet traffic and access to Bureau internal apps is secure and in compliance with CFPB policies, even when you're off a CFPB network. No matter where you're accessing the web, Zscaler Client Connector ensures that your traffic is forwarded to and protected by the Zscaler Internet Access (ZIA) service. Additionally, with Zscaler Private Access (ZPA) enabled, you can also securely access your organization's internal resources from any location. Finally, with the Zscaler Digital Experience (ZDX) service enabled, Zscaler Client Connector performs synthetic probing to a desired Software-as-a-Service (SaaS) application or internet-based service (e.g., OneDrive, Gmail, etc.) to triage and pinpoint the source of performance issues.

Zscaler Client Connector is designed to provide a seamless user experience. It automatically recognizes when you are connected to a CFPB-trusted network and when you connect to Wi-Fi hotspots (for example, at airports, hotels, and cafés) where you must pay or accept a use policy before connecting. The app disables its services for temporarily and re-enables itself after you've had a chance to complete the steps necessary to connect.

## Installation Packages

* **Windows** - UDA - ZScaler (AOVPN Cutover) is located in SCCM.
* MACs - Installation Package for Macs – Need the name (?), located in JAMF.

## Zscaler Client Connector Tray Icon Options

The Zscaler Client Connector displays an icon in the system tray, as shown below:

Figure : Zscaler Client Connector icon



If **notifications** are enabled, you will see notifications in the tray icon, as shown below.

Figure : Zscaler Client Connector Notifications



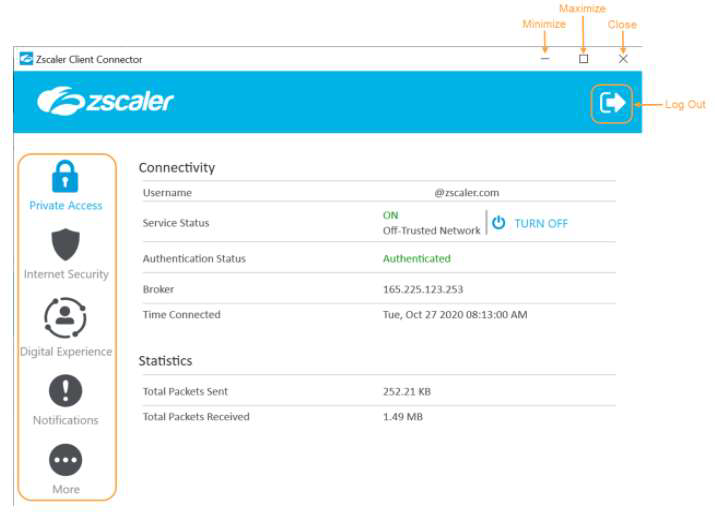
To learn how to enable the system tray notifications, click the following:

1. Click the log out button on the top right-hand corner to log out of Zscaler Client Connector.

**Note:** You might be required to enter a password your organization's admin has set for the app. If you log out of the app, you must complete enrollment again when you log back in.

1. Click the minimize button to minimize the window without closing it.
2. Click the maximize button to maximize the window.
3. Click the close button to close the window. This does not log you out of the app.

Figure : Zscaler Client Connector



The app features Zscaler Client Connector's services in the menu on the left. The example above shows the menu options for an organization that has subscribed to the ZIA, ZPA, and ZDX services. If your organization is not subscribed to one of these services, you will not see that option in the left menu.

# Triage

## Common Support Issues

### Blocked Website(s)

### Service Desk Technician will direct the user(s) to submit a [Web Content Filtering Exception](https://cfpbprod.servicenowservices.com/servicecenter?id=sc_cat_item&sys_id=c1be7d621b897510db1da82fe54bcb63) Request.

### If approved, CSIRT will route request to DOJ to implement. Create email to:

### DOJ: [DOJ.Service.Desk@usdoj.gov](mailto:DOJ.Service.Desk@usdoj.gov)and[DOJ.SharedServicesEngineering@usdoj.gov](mailto:DOJ.SharedServicesEngineering@usdoj.gov), **DOJ Customer Success Manager (CSM)**

### DOJ provides a reference number (Ticket) to CSIRT.

### CSIRT will update the CFPB ServiceNow ticketing system.

### Whitelisted will allow access to the website(s).Blacklisted will not allow access to the website(s).

### Slowness with Zscaler Service

Slow browsing or download issues can come from multiple source issues including DNS resolution delay, packet retransmission issues, or even third-party software components.

To find what is causing the slowness and get to the root cause as fast as possible, we want to collect a bit more information.

**Questions to Answer**

* When did the slowness start?
* Does this impact a single user, single site, or multiple sites?
* Is this for all websites or a specific website/web application? Provide a list
* Which method(s) are you using to route traffic? (i.e., Explicit proxy, PAC, GRE, VPN)

**Gather the Following Information**

1. Determine the Cloud Path: Provide a screenshot of ip.zscaler.com from the affected machine.
2. Next, we will check the node health, datacenter throughput and provide an MTR back to your IP.
3. Run MTR Trace - with Zscaler Analyzer => z-traceroute found on the (ip.zscaler.com) page.
4. https://help.zscaler.com/zia/how-do-i-use-zscaler-analyzer
5. Collect at least 300 packets
6. If you are using IPsec or GRE tunnels this must show the route outside the tunnel.
7. This Zscaler Analyzer tool is present on (ip.zscaler.com) page, for download.
8. Run Specific URL baseline - Zscaler Analyzer => z-WebLoad tool with default settings.
9. Never test using google.com.
10. https://help.zscaler.com/zia/how-do-i-use-zscaler-analyzer

**Note 1:** Please be prepared to install Wireshark or Windows NetMon, for a WebEx with our engineers. We may need captures from your client and on our nodes, so we can analyze the traffic flow between yourselves and our nodes.

**Note 2:** We strongly recommend setting up Zscaler Analyzer on monitoring stations in various regions for long-term regional baselining and troubleshooting. Note, this may require correct firewall ruleset and routing considerations.

### Application(s) unable to connect to the internet

Applications that are unable to connect to the internet are sometimes caused when SSL decryption using Zscaler breaks the application due to certificate pinning.

**Escalation**: **Escalate incident to Network Management**

**Troubleshooting Data Collection:**

* When did the slowness start?
* Does this impact a single user, single site, or multiple sites?
* Is this for all websites or a specific website/web application? Provide a list
* Zscaler Application Logs in Debug Mode.
* Screenshot of the error seen.
* Also collect HTTP header capture and Wireshark capture, this will provide additional insights (optional).

**Troubleshooting Zscaler App (Windows)**

Following are further details about the Troubleshoot menu features of the Windows version of the Zscaler App.

Figure : Zscaler Troubleshoot menu (Windows)

****

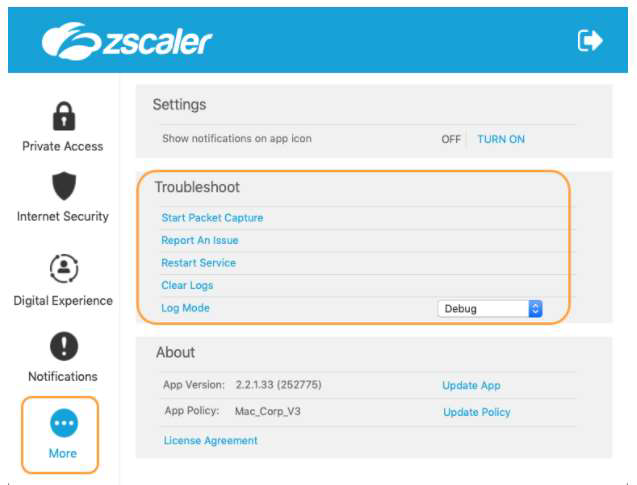
* **Start Packet Capture:** If your organization's admin enabled packet captures, you can use this feature when reproducing an issue. To learn more, see Using the Start Packet Capture Option.
* **Report an Issue:** If your organization's admin enabled in-app support access, you can use this feature to report an issue. When you submit the form, depending on your organization's set up, Zscaler Client Connector can send an email to your organization's support admin or submit a ticket directly to Zscaler Support (your support admin will receive a copy of this ticket as well). After you submit the form, you will receive an email acknowledging the support request. For instructions on completing the form, see Reporting an Issue with Zscaler Client Connector for Windows.
* **Restart Service:** You can click to restart the app. Restarting does not impact security enforcement.
* **Repair App:** If you select this option, the app will attempt to repair itself by reinstalling app drivers and services. Zscaler recommends trying this option before reporting an issue.
* **Clear Logs**: You can clear stored logs.
* **Log Mode:** You can change the mode in which Zscaler Client Connector generates logs, but the change is effective for that connection session only. At the start of the next connection session, the app returns to the default log mode set by your organization. Below is a description of each log mode.
  + - **Error:** Logs only when the app encounters an error and functionality is affected.
    - **Warn:** Logs when the app is functioning but is encountering potential issues, or logs when conditions for the Error log mode are met.
    - **Info:** Logs general app activity, or logs when conditions for the Warn log mode are met.
    - **Debug**: Logs all app activity that could assist Zscaler Support in debugging issues, or logs when conditions for the Info log mode are met.

**Troubleshooting Zscaler App (macOS)**

Following are further details about the Troubleshoot menu features of the macOS version of the

Zscaler App.

Figure : Zscaler Troubleshoot menu (macOS)



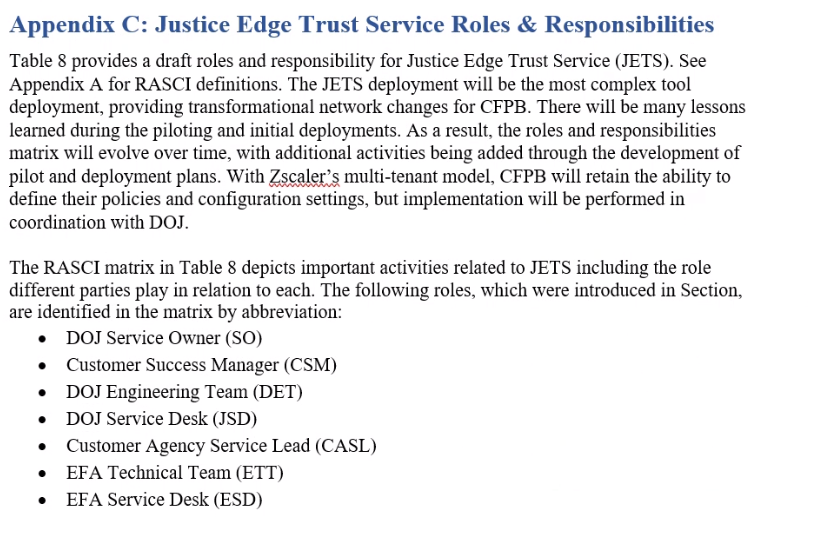
* **Start Packet Capture:** If your organization's admin enabled packet captures, you can use this feature when reproducing an issue. To learn more, see Using the Start Packet Capture Option.
* **Report an Issue:** If your organization's admin enabled in-app support access, you can use this feature to report an issue. When you submit the form, depending on your organization's set up, Zscaler Client Connector can send an email to your organization's support admin or submit a ticket directly to Zscaler Support (your support admin will receive a copy of this ticket as well). After you submit the form, you will receive an email acknowledging the support request. For instructions on completing the form, see Reporting an Issue with Zscaler Client Connector for Windows.
* **Restart Service:** You can click to restart the app. Restarting does not impact security enforcement.
* **Repair App:** If you select this option, the app will attempt to repair itself by reinstalling app drivers and services. Zscaler recommends trying this option before reporting an issue.
* **Clear Logs**: You can clear stored logs.
* **Log Mode:** You can change the mode in which Zscaler Client Connector generates logs, but the change is effective for that connection session only. At the start of the next connection session, the app returns to the default log mode set by your organization. Below is a description of each log mode.
  + - **Error:** Logs only when the app encounters an error and functionality is affected.
    - **Warn:** Logs when the app is functioning but is encountering potential issues, or logs when conditions for the Error log mode are met.
    - **Info:** Logs general app activity, or logs when conditions for the Warn log mode are met.

**Debug**: Logs all app activity that could assist Zscaler Support in debugging issues, or logs when conditions for the Info log mode are met.

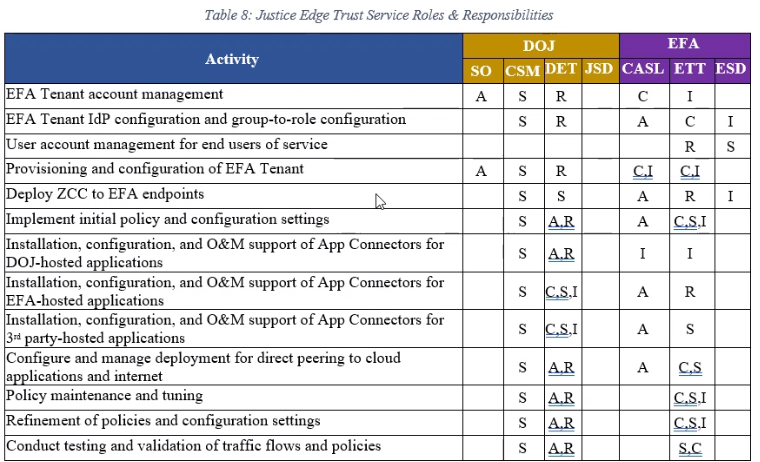
**Troubleshooting Zscaler App (iOS)**

Following are the Troubleshoot menu features of the iOS version of the Zscaler Client Connector:

# Responsible, Accountable, Supported, Consulted, Informed (RASCI) Matrix



|  |  |
| --- | --- |
| Role | Responsibility |
| **DOJ Service Owner (SO)** |  |
| **DOJ Customer Success Manager (CSM)** |  |
| **DOJ Engineering Team (DET)** |  |
| **DOJ Service Desk (JSD)** |  |
| **Customer Agency Service Lead (CASL)** |  |
| **EFA Technical Team (ETT)** |  |
| **EFA Service Desk (ESD)** |  |
| **Service Desk (Tier I)** | * First User contact * Provide initial triage of incidents * Assist users to the correct Request Catalog |
| **Deskside Support (Tier II)**  **AD Management Team**  **Incident Management** | Further troubleshooting and documenting issues, including capture screen shots and logs. |
| **Desktop Engineering** | 3rd level support for the Zscaler Client for MACs and Windows |
| **Network Management** | Deep dive into Network related issues, including capturing screen shots and logs (if necessary; escalate to DOJ or resolve |
| **ETS Mobility** | * 3rd Tier Support for Zscaler client issues on IOS and Android devices. * Android devices – Desktop Audiocode phones located in limited (Director’s office and SCC). |



# Related Controls

## Control Activity Summary

Table 6: Control Activities Summary

|  |  |  |  |
| --- | --- | --- | --- |
| Control Activity | Responsibility | Timing | Key Output(s) |
| **<<Name of control activity>>** | <<Position titles of those responsible for the activity>> | <<Required timing of the activity (e.g., weekly, monthly, quarterly)>> | <<Key documents or other outputs created as a result of the activity>> |
|  |  |  |  |

## Records Management

Table 7: Records Management Summary

|  |  |  |
| --- | --- | --- |
| Record/Document Type | Retention Requirement | Storage Location |
|  |  |  |
|  |  |  |
|  |  |  |

# Approvals

Document Owner Date

T&I Team Lead Date

CIO (or Delegate) Date

# Appendices

1. Key Terms and Acronyms

Table 8: Key Terms and Acronyms

|  |  |
| --- | --- |
| Term/Acronym | Definition |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. <<Insert Appendix Title>>