<< Zscaler >>

Standard Operating Procedure

<<Insert Document Number>>

<<June 2024>>

1. 

Table of Contents

[Table of Contents i](#_Toc171946053)

[Table of Figures iii](#_Toc171946054)

[Table of Tables iii](#_Toc171946055)

[Revision History iv](#_Toc171946056)

[1 Introduction 1](#_Toc171946057)

[Purpose 1](#_Toc171946058)

[1.1 Intended Audience 2](#_Toc171946059)

[1.2 Roles and Responsibilities 2](#_Toc171946060)

[1.3 Primary Points of Contact 3](#_Toc171946061)

[1.4 Related Documents 3](#_Toc171946062)

[2 <<Insert Section Title>> 5](#_Toc171946063)

[3 Service CI 6](#_Toc171946064)

[4 Zscaler Client Connector 7](#_Toc171946065)

[4.1 Installation Packages 7](#_Toc171946066)

[4.2 Zscaler Client Connector Tray Icon Options 7](#_Toc171946067)

[5 Triage 10](#_Toc171946068)

[Blocked Web site 10](#_Toc171946069)

[Common support issues 10](#_Toc171946070)

[6 Responsible, Accountable, Supported, Consulted, Informed (RASCI) Matrix 15](#_Toc171946071)

[7 Related Controls 17](#_Toc171946072)

[7.1 Control Activity Summary 17](#_Toc171946073)

[7.2 Records Management 17](#_Toc171946074)

[8 Approvals 18](#_Toc171946075)

[Appendix A: Key Terms and Acronyms 19](#_Toc171946076)

[Appendix B: <<Insert Appendix Title>> 20](#_Toc171946077)

# Table of Figures

[Figure 1: <<Insert Figure Caption>> i](#_Toc514074195)

# Table of Tables

[Table 1: <<Insert Table Caption>> i](#_Toc514076461)

[Table 2: Roles and Responsibilities Summary 1](#_Toc514076462)

[Table 3: Document Points of Contact Summary 1](#_Toc514076463)

[Table 4: Related Documents Summary 1](#_Toc514076464)

[Table 5: Key Terms and Acronyms 1](#_Toc514076465)

<<Template Formatting Instructions – DELETE PRIOR TO PUBLICATION>>

There is no need to manually create these tables. For figures and tables, make sure to add a caption by going to the References tab on the MS Office ribbon and selecting “Insert Caption.” Alternatively, you can copy and paste the lines below as needed and then right-click on the relevant caption number and select “Update Field” to automatically apply the next number in the sequence. Once you have added new captions, right-click on the lists above and select to “Update Field” and then “Update Entire Table.”

Figure 1: <<Insert Figure Caption>>

Table 1: <<Insert Table Caption>>

Revision History

Table 2: Revision History

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

# Introduction

<<Template Formatting Instructions – DELETE PRIOR TO PUBLICATION>>

<<Every reference must begin with this introductory section and must include each of these specific subsections. If your reference would benefit from any additional introductory information, you may add new subsections after section 1.5 as needed. Helpful tips and expectations are provided for each section. Remember to delete these guidance placeholders before inserting your content.>>

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

<<Briefly state which Bureau audience(s) this document is most intended for (e.g., all Bureau employees and contractors, all T&I employees and contractors, a specific T&I team, etc.).>>

CFPB Service desk which includes, Service Desk (Tier I), Desktop Support (Tier II), AD Management, and Incident Management team.

## Roles and Responsibilities

<<Describe the organizational level roles and responsibilities for the topic addressed in this document. Include roles for individuals only if they have a unique approval responsibility (e.g., CIO approval step). Individuals should only be listed by the official role title, not a person’s name.>>

Table 3: Roles and Responsibilities Summary

|  |  |
| --- | --- |
| Role | Responsibility |
| Service Desk (Tier I) | First User contact, provide initial triage of incidents, or direct users to the correct Request Catalog. |
| Desktop Support (Tier II)  AD Management Team  Incident Management | Further troubleshooting and documenting issues, including capture screen shots and logs. |
| Network Management | Deep dive into Network related issues, including capturing screen shots and logs (if necessary; escalate to DOJ or resolve |
| Desktop Engineering | 3rd level support for the Zscaler Client for MACs and Windows |
| 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

<<List the Document Owner and any other key personnel who will have a role in maintaining this document or supporting its topic.>>

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

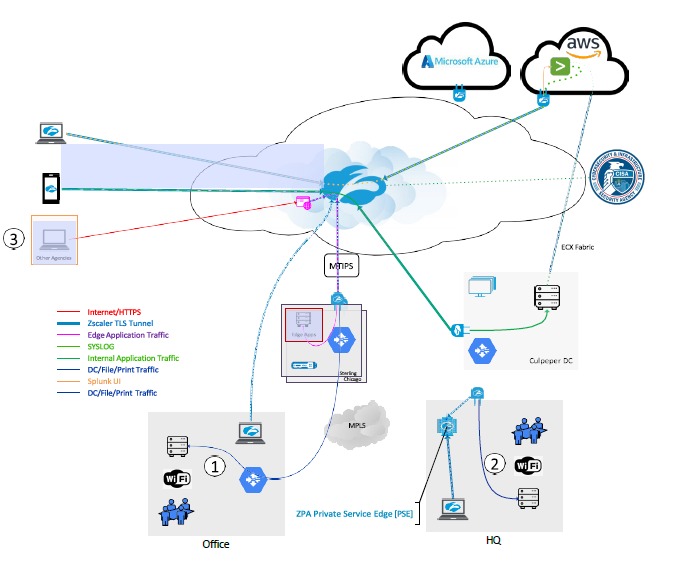
<<Include a list of key regulations, legal authorities, policies, and other Bureau guidance documents that are directly related to the topic of this official document to support users looking for additional information or the source of specific requirements.>>

Table 5: Related Documents Summary

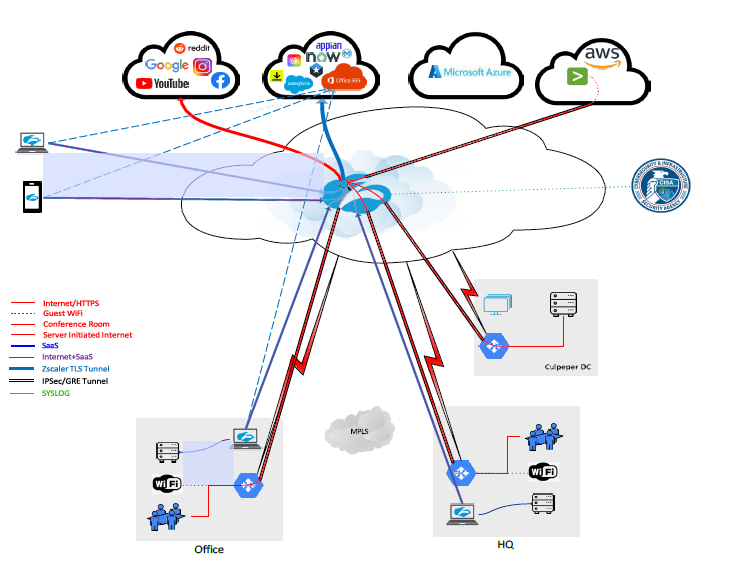
|  |  |  |
| --- | --- | --- |
| Document Name | Brief Description | Location or Link |
|  |  |  |
|  |  |  |

# <<Insert Section Title>>

**Detailed Design Diagram**



**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 installed on each type of end-user devices (IOS, Macs, and Windows)

Zscaler Client Connector is an application installed on your device to ensure that your internet

traffic and access to your organization's internal apps are secure and in compliance with your

organization’s policies, even when you're off your corporate 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 trusted network (for example, your corporate office network) and depending on your organization's configuration, can disable ZIA, ZPA, and ZDX services accordingly. It can also recognize 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.

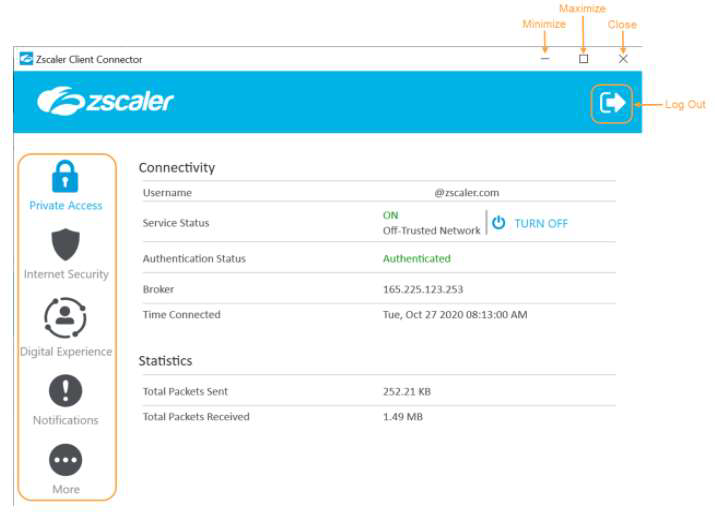
## Zscaler Client Connector Tray Icon Options

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



If **notifications** are enabled, you will see notifications in the tray icon, as shown below. To learn how to enable the system tray notifications.





You can click the following buttons:

* Click the log out button on the top right-hand corner to log out of Zscaler Client Connector. 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.
* Click the minimize button to minimize the window without closing it.
* Click the maximize button to maximize the window.
* Click the close button to close the window. This does not log you out of the app.

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

Blocked Web site - direct user to submit a [Web Content Filtering Exception](https://cfpbprod.servicenowservices.com/servicecenter?id=sc_cat_item&sys_id=c1be7d621b897510db1da82fe54bcb63) Request

If approve, CSIRT route request to DOJ to implement. DOJ Email address[DOJ.Service.Desk@usdoj.gov](mailto:DOJ.Service.Desk@usdoj.gov)and[DOJ.SharedServicesEngineering@usdoj.gov](mailto:DOJ.SharedServicesEngineering@usdoj.gov). DOJ provides a reference number (Ticket).

Common support issues for administrators and support staff

### 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

Determine the Cloud Path: Provide a screenshot of ip.zscaler.com from the affected machine.

a. Next, we will check the node health, datacenter throughput and provide an MTR back to your IP.

2. Run MTR Trace - with Zscaler Analyzer => z-traceroute found on the (ip.zscaler.com) page.

a. https://help.zscaler.com/zia/how-do-i-use-zscaler-analyzer

b. Collect at least 300 packets

c. If you are using IPsec or GRE tunnels this must show the route outside the tunnel.

d. This Zscaler Analyzer tool is present on (ip.zscaler.com) page, for download.

3. Run Specific URL baseline - Zscaler Analyzer => z-WebLoad tool with default settings.

Never test using google.com.

a. https://help.zscaler.com/zia/how-do-i-use-zscaler-analyzer

b. 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 base-lining and troubleshooting. Note, this

may require correct firewall ruleset and routing considerations.

### Application 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.

****

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.

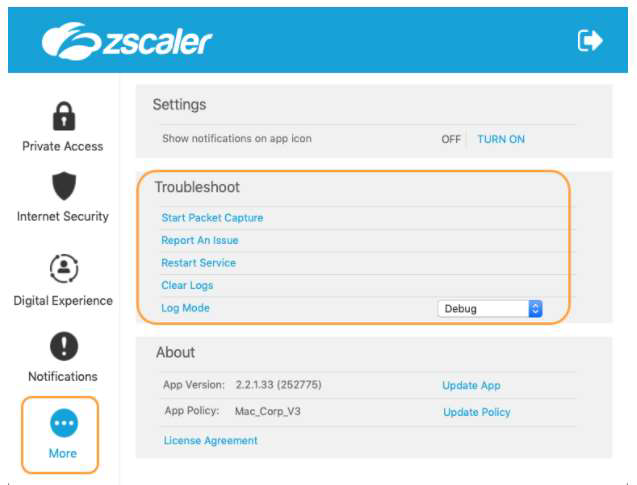
**Debug**: Logs all app activity that could assist Zscaler Support in debugging

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.



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.

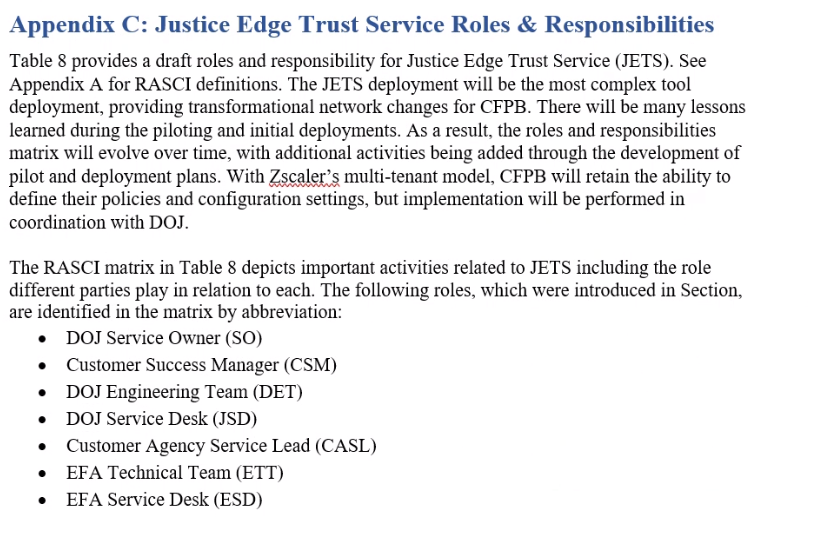
**Debug**: Logs all app activity that could assist Zscaler Support in debugging

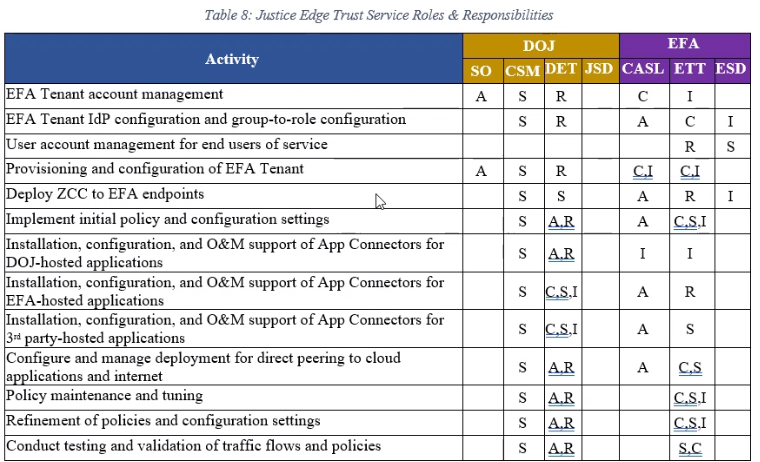
issues, or logs when conditions for the Info log mode are met.

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





# Related Controls

<<Template Formatting Instructions – DELETE PRIOR TO PUBLICATION>>

<<This section is required for most SOPs. Identify any necessary controls, such as checklists, supervisory reviews, etc. that must be completed as part of this process. Include who is responsible for the control activity and any required timelines for completion (e.g., monthly, quarterly). If you feel that your topic t truly does not have any related controls, consult with T&I Policy to confirm whether this section can be omitted. >>

## Control Activity Summary

<<List any control activities that are described in the content sections above or otherwise related to the topic of this SOP.>>

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

<<List any official Bureau records that are created as a result of this SOP process/topic. You may also include other key outputs that are not official records, but that Bureau users may need assistance in locating.>>

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

<<Template Formatting Instructions – DELETE PRIOR TO PUBLICATION>>

<<Additional T&I Team Lead signature lines may be inserted in this page if needed for SOPs with dual ownership or cross-team impacts. >>

1. Key Terms and Acronyms

Table 8: Key Terms and Acronyms

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

<<Template Formatting Instructions – DELETE PRIOR TO PUBLICATION>>

<<This appendix must be included in every official document as Appendix A. Define key terms and acronyms that may be unfamiliar or misinterpreted by readers. Insert any additional appendices needed for your document as Appendix B and forward.>>

1. <<Insert Appendix Title>>

<<Insert appendices as needed or delete placeholder section.>>