Corporate Zayo Group

Supplier Security Document - External

Code:	Z-SupplierSecurity
Version:	1.4
Date of Version:	2/9/2022
Created by:	Diane Chamberlin
Approved by:	Dale Drew, CSO

Preface **2**

1. Purpose, scope and users **2**

2. Supplier Security Requirements **3**

2.1. Overall Policy Issues 3

2.2 Logical Security Requirements 3

2.3. Physical Security Requirements 4

2.4 Data Handling Requirements 4

4. Acknowledgement **5**

5. Validity and document management **5**

Preface

This policy provides high-level security requirements associated with suppliers (including contractors, vendors, and partners, which will be referred to as Suppliers hereafter) who need to gain access to Zayo logical systems, physical Zayo facilities, and/or will have Zayo data.

The threats to information assets are continually changing, and readers are encouraged to contact Zayo's Security Department – security@zayo.com for any questions or clarification of the issues addressed herein.

1. Purpose, scope and users

The purpose of this policy is to communicate the minimal logical, physical, and data security requirements for Suppliers when connecting into Zayo internal systems, accessing physical facilities, and when collecting, managing, processing and/or storing Zayo data. Suppliers will be required to be compliant with these Security Requirements when providing services to Zayo. Zayo will reserve the right to audit and validate that the Security Requirements are being followed and are maintained as part of an implemented and consistent process.

This policy is intended for Zayo Suppliers who are providing services to Zayo and have the ability to influence confidentiality, integrity and availability of any assets that are part of the Information Security Management System (ISMS).

Suppliers with access to Zayo logical systems will refer to section 2.2 for requirements and acceptable usage. Suppliers with access to Zayo physical facilities will refer to section 2.3 for requirements and acceptable usage. Suppliers with access to Zayo data will refer to section 2.4 for requirements and acceptable usage.

Exceptions

In certain circumstances, exceptions to this policy may be allowed based on demonstrated business need, or to apply local relevant laws and regulations. Exceptions to this policy must be formally documented and approved by the Corporate Security team before the exception can be implemented. Policy exceptions will be reviewed on a yearly basis to ensure the exceptions are still relevant.

The Corporate Security team is the only team that can accept security risks for the Organization: Security@zayo.com

2. Supplier Security Requirements

2.1. Overall Policy Issues

- Suppliers must comply with applicable Zayo Logical, Physical, and Data Security Company policies, procedures and standards located herein, hereafter called “Security Policy”. Supplier will be provided access to updates of the Security Policy when a critical Security Policy is introduced, during the life of the contract.
- Zayo reserves the right to filter, restrict, block any traffic, user or service originating from the Supplier network to Zayo for any reason, at any time without prior notice.
- Should there be any transition of information (or termination of contract), both parties must ensure that the appropriate retention of data is adhered to and that there is no leaking of confidential or internal use data from Zayo.
- The Supplier must establish, implement and maintain reasonable policies and a program of organizational, operational, administrative, physical, and technical security measures to prevent any security breach or unauthorized disclosure of Zayo’s services, systems, infrastructure or confidential data. The Supplier must ensure that its information security staff has reasonable and necessary experience to administer its program. The Supplier must also ensure that the appropriate security awareness training is in place for this program.

2.2 Logical Security Requirements

Suppliers must only have access to logical systems that are necessary for their job function. Access permissions must be based on the principles of need-to-know and need-to-use as related to a specific job role. All activities will be monitored and access shall be strictly controlled.

The following are Zayo’s minimal logical requirements for reducing risks. These requirements must be agreed upon and documented before granting the Supplier access to Zayo logical systems.

- Supplier will access Zayo’s network, systems and associated data only via Zayo approved provided methods.
- Zayo reserves the right to implement and maintain security infrastructure that monitors users actions while utilizing the Zayo environment. Any unauthorized activity detected using these security controls will be reported to the Supplier Security POC.
- At no time will Supplier employees share Zayo supplied credentials, passwords or other uniquely identified resources when accessing Zayo systems.
- Supplier must not access Zayo systems or resources that they have not been explicitly provided permission to access.

2.3. Physical Security Requirements

Suppliers needing physical access to Zayo facilities are approved on an as needed basis depending on the need and scope of work.

The following are Zayo's minimal physical requirements for reducing organizational risk. These requirements must be agreed upon and documented before granting the Supplier access to Zayo physical facilities:

- Suppliers are required to comply with the Zayo Physical Security Policies and Procedures while working on a Zayo site.
- At no time will Supplier employees share physical access cards when accessing Zayo physical facilities.
- Suppliers performing work or maintenance at the site must return the temporary Supplier physical access cards upon completion of work.

2.4 Data Handling Requirements

Information that users at Zayo share with a Supplier must only be shared based on a need-to-know and need-to-use basis and this method of information sharing must be used by the Supplier in the case that the Supplier uses any other Suppliers for the services provided to Zayo.

The following are Zayo's minimal requirements for handling Zayo Data for mitigating risks. These requirements must be agreed upon and documented before giving the Supplier any Zayo data.

- Zayo confidential data will not be transmitted, processed, evaluated or stored outside the Zayo network environment unless specifically permitted.
- At no time will Supplier employees share Zayo data with unauthorized personnel.
- Zayo Confidential or Sensitive Data must not be sent to third party networks without pre-authorization from Zayo Security Compliance.
- Supplier will report any Zayo Confidential or Sensitive Data when discovered on unapproved Supplier systems and immediately remove it from unapproved Supplier systems.
- Any Zayo data must be transmitted securely and encrypted when stored utilizing approved Zayo encryption tools and methodology.
- Any Zayo Confidential or Sensitive Data authorized for storage on Supplier systems must be protected in accordance with Zayo Security Policy.
- Any Zayo Confidential or Sensitive Data authorized for storage on Supplier systems must be deleted, via a secure method approved by Zayo Security Compliance, after use or upon termination of Supplier Service; whichever occurs first.
- In the event there is any loss of Zayo Sensitive or Confidential Data, or any unauthorized or unlawful access to, use of, or disclosure of, or any other compromise of Zayo Sensitive or Confidential Data, Supplier must immediately notify Zayo in writing of the Security Incident. Supplier must (i) fully cooperate with Zayo to investigate and resolve the Security Incident,

including without limitation, agreeing to the content of any notifications of the Security Incident, (ii) be responsible for all costs related to any Security Incident, including without limitation, costs related to investigations, notifications, customer support and credit monitoring, and (iii) properly document responsive actions taken related to any Security Incident, including without limitation, post-incident review of events and actions taken, if any, to make changes in business practices related to the protection of Zayo Sensitive or Confidential Data, escalation procedures to senior managers, and any reporting to regulatory and law enforcement agencies.

4. Acknowledgement

Vendors must acknowledge compliance with this policy to security@zayo.com in order to complete the registration process. Failure to acknowledge compliance, will result in vendors not being approved to provide services to Zayo.

5. Validity and document management

This document is valid as of February 9, 2022.

The owner of this document is the Corporate Security team, who must check and, if necessary, update the document at least once a year.

Change History

Date	Version	Created by	Description of Change
12/3/19	1	Diane Chamberlin	Original Document
1/20/20	1.1	Diane Chamberlin	Document Review
2/3/20	1.2	Diane Chamberlin	Language tuned
9/23/20	1.3	Diane Chamberlin	Logo updated
2/9/22	1.4	Dale Drew	Simplified Version