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

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 r

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	Verc	.