



A-LIGN



ITS Fiber, LLC
SOC 3
2019

ITSFiber®

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

January 1, 2019 To December 31, 2019

Table of Contents

SECTION 1 ASSERTION OF ITS FIBER, LLC MANAGEMENT	1
SECTION 2 INDEPENDENT SERVICE AUDITOR’S REPORT	3
SECTION 3 ITS FIBER, LLC’S DESCRIPTON OF ITS COLOCATION AND SUPPORT SERVICES SYSTEM THROUGHOUT THE PERIOD JANUARY 1, 2019 TO DECEMBER 31, 2019.....	7
OVERVIEW OF OPERATIONS.....	8
Company Background	8
Description of Services Provided	8
Principal Service Commitments and System Requirements.....	8
Components of the System.....	9
Boundaries of the System.....	10
Changes to the System Since the Last Review.....	10
Incident Since the Last Review.....	11
Criteria Not Applicable to the System	11
COMPLEMENTARY USER ENTITY CONTROLS.....	11

SECTION 1
ASSERTION OF ITS FIBER, LLC MANAGEMENT

ASSERTION OF ITS FIBER, LLC MANAGEMENT

February 18, 2020

We are responsible for designing, implementing, operating, and maintaining effective controls within ITS Fiber, LLC's ('ITS Fiber' or 'the Company') Colocation and Support Services System throughout the period January 1, 2019 To December 31, 2019, to provide reasonable assurance that ITS Fiber's service commitments and system requirements relevant to Security and Availability (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in "ITS Fiber, LLC's Description of Its Colocation and Support Services System Throughout the Period January 1, 2019 To December 31, 2019" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2019 To December 31, 2019, to provide reasonable assurance that ITS Fiber's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). ITS Fiber's objectives for the system in applying applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "ITS Fiber, LLC's Description of Its Colocation and Support Services System Throughout the Period January 1, 2019 To December 31, 2019".

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve ITS Fiber's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of ITS Fiber's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period January 1, 2019 to December 31, 2019 to provide reasonable assurance that ITS Fiber's service commitments and system requirements were achieved based on the applicable trust services criteria.



Bruce Russell
Chief Financial Officer
ITS Fiber, LLC

SECTION 2
INDEPENDENT SERVICE AUDITOR'S REPORT



INDEPENDENT SERVICE AUDITOR'S REPORT

To ITS Fiber, LLC:

Subject

We have examined ITS Fiber, LLC's ('ITS Fiber' or 'the Company') accompanying description of Colocation and Support Services System titled "ITS Fiber, LLC's Description of Its Colocation and Support Services System Throughout the Period January 1, 2019 To December 31, 2019" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2019 to December 31, 2019, to provide reasonable assurance that ITS Fiber's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at ITS Fiber, to achieve ITS Fiber's service commitments and system requirements based on the applicable trust services criteria. The description presents ITS Fiber's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of ITS Fiber's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

ITS Fiber is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that ITS Fiber's service commitments and system requirements were achieved. ITS Fiber has provided the accompanying assertion titled "Assertion of ITS Fiber, LLC Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. ITS Fiber is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within ITS Fiber's Colocation and Support Services System were suitably designed and operating effectively throughout the period January 1, 2019 to December 31, 2019, to provide reasonable assurance that ITS Fiber's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

The SOC logo for Service Organizations on ITS Fiber's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of ITS Fiber, user entities of ITS Fiber's Colocation and Support Services System during some or all of the period January 1, 2019 to December 31, 2019, business partners of ITS Fiber subject to risks arising from interactions with the Colocation and Support Services System, and those who have sufficient knowledge and understanding of the complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
February 18, 2020

SECTION 3

**ITS FIBER, LLC'S DESCRIPTION OF ITS COLOCATION AND SUPPORT SERVICES
SYSTEM THROUGHOUT THE PERIOD JANUARY 1, 2019
TO DECEMBER 31, 2019**

OVERVIEW OF OPERATIONS

Company Background

ITS Fiber began as a small rural telephone company in the early 1930's and was originally owned and operated by Indiantown Development Corporation. In the early 1950's, the Indiantown Development Corporation was purchased and the Indiantown Company, Inc. was formed, which included the telephone company, a water company, and plans to install a modern sewage system and treatment plant. In 1956, the telephone portion of Indiantown Company, Inc. was changed to Indiantown Telephone System, Inc. (ITS). In 1998, a corporate restructure of Indiantown Company, Inc. formed the current parent company, Postco, Inc. At the same time, the increased need for communications services prompted a name change from Indiantown Telephone Systems, Inc. to ITS Telecommunications Systems, Inc. Postco, Inc. continues to operate the water, and sanitation services companies in addition to ITS Fiber.

Today the company has 80 percent underground fiber-optic network in its regulated service territory activating approximately 2,000 customers onto ITS Fiber communication services. The company has implemented an extension of its fiber ring that is within close proximity of most of the major businesses in Martin and Southern St. Lucie Counties, which has positioned ITS for a period of rapid growth and expansion in the dynamic fiber services market place.

Description of Services Provided

ITS Fiber owns its entire information technology (IT) infrastructure and co-locates such systems in a world-class Data Center to provide advanced access services for its clients and their end users, regardless of their point-of-access.

The APC Hot Aisle Containment System (HACS) Data Center, where client servers are collocated, provides multiple layers of physical and network security. Physical security includes closed-circuit TV cameras both outside and inside the Data Center, key proximity door access, security systems with mantrap that produce an alarm when an external door is open. All cabinets and rack spaces are locked unless authorized personnel are performing maintenance work. The facility is monitored by the Network Operations Center (NOC) via closed-circuit digital cameras with 24-hour recording and 15-day digital video storage. The facility is also equipped with centralized security and 24x7x365 security personnel contracted by ITS.

All ITS Fiber servers sit behind Enterprise Class, redundant firewalls. Only required ports and services are exposed to the external Internet and continuous monitoring of the status, overall health, security of the systems, and network is performed by NOC personnel.

Principal Service Commitments and System Requirements

ITS Fiber designs its processes and procedures to meet its objectives for its business services. Those objectives are based on the service commitments that ITS Fiber makes to user entities, the laws and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that ITS Fiber has established for the services. The business services of ITS Fiber are subject to state privacy security laws and regulations in the jurisdictions in which ITS Fiber operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

Security principles within the fundamental designs of the business services that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.

Use of encryption technologies to protect customer data both at rest and in transit.

ITS Fiber establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in ITS Fiber's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the business services.

Components of the System

Infrastructure

Primary infrastructure used to provide ITS Fiber's Colocation and Support Services system includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
HVAC containment system	APC Hot Aisle Containment System	Combination of APC racks, enclosure, in row cooling units, and monitoring and management system. Maintains controlled environment for collocated equipment.
UPS	APC Galaxy MGE 5000	Provides uninterrupted power to equipment collocated in the data center.
Generator	Cummins	Generates power using locally stored fuel, in the event of utility provided power failure.
Video surveillance	Night Owl	Provides monitoring recording of facility.
Core network	Juniper	Combination of routers, switches, and firewalls provide network connectivity to equipment collocated in the data center.

Software

Primary software used to provide ITS Fiber's Colocation and Support Services system includes the following:

Primary Software		
Software	Operating System	Purpose
Access Control	BioStar	Provides management and control of multi-factor authenticated access.
Monitoring	Kaseya, OpenNMS, and Cacti	Used to monitor production environment and in the event fault thresholds are exceeded, alert responsible parties.
Backup	Veeam	Used for backup solution.
Virtual Environment	VMware	Virtual environment management and control.

People

ITS Fiber staff provides support for the above services in each of the following functional areas:

- Executive management - provides general oversight and strategic planning of operations
- Accounting - responsible for financial and regulatory aspects of the organization
- Business Development - ensures continued business opportunities for the company
- Customer Operations - serves customers by providing product and service information that includes resolving product and service issues
- Information Technology - responsible for effective operation and maintenance of systems hardware and software relevant to the services provided
- Outside Plant - responsible for effective provisioning and installation of serving devices at customer locations
- Marketing - ensures effective communication to customers, in respect to services provided

Data

Data is captured which is utilized by ITS Fiber in delivering its Colocation and Support Services System. Such data includes, but is not limited to, the following:

- Alert notifications and monitoring reports generated from the commercial monitoring applications
- Alert notifications received from automated backup systems
- Vulnerability or security alerts received from various sources including security subscriptions, scanning tools, IDS alerts, or automated patching systems
- Incident reports documented via the ticketing systems

Processes, Policies and Procedures

ITS Fiber data center operational policies and procedures are documented and made available to employees and customers. The responsibility and accountability for developing and maintaining these policies, and changes and updates to these policies, are assigned to appropriate data center employees. Additionally, a dedicated member of management or committee reviews the information in these policies on an annual basis. A dedicated NOC administration manual has been developed and is available to employees in case of an emergency.

The NOC utilizes its own intranet webpage dedicated to its policies and procedures. Content is updated in real time on the intranet webpage to ensure NOC employees are always aware of the newest policy or procedures. On an annual basis, NOC management performs a review of information on the NOC intranet webpage to ensure the information is up-to-date and accurate. The NOC utilizes a ticketing system to track all incidents and customer requests. On a monthly basis, ticket resolution metrics are prepared and presented to operations management for review.

Customers may contact ITS Fiber via a dedicated website and online customer portal. The website hosts a detailed description of the data center services and the portal contains customer specific information and enables customers to contact ITS Fiber directly through the system. This customer portal and communication methods are utilized to ensure transparent communication with customers.

Boundaries of the System

The scope of this report includes the Colocation and Support Services system performed in the Indiantown, Florida facilities.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization's last review.

Incident Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization's last review.

Criteria Not Applicable to the System

All Common and Availability criterion were applicable to the ITS Fiber Colocation and Support Services system.

COMPLEMENTARY USER ENTITY CONTROLS

ITS Fiber's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to ITS Fiber's services to be solely achieved by ITS Fiber control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of ITS Fiber's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to ITS Fiber.
2. User entities are responsible for notifying ITS Fiber of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of ITS Fiber services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize ITS Fiber services.
6. User entities are responsible for providing ITS Fiber with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying ITS Fiber of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.