Proprietary & Confidential

everstream™

FASTER FIBER. BETTER BUSINESS.

Grand Rapids Data Center System

SOC 2

Report on Everstream Solutions, LLC's System and Organization Controls Relevant to Security and Availability

JUNE 1, 2020 TO MAY 31, 2021

Moss Adams LLP
999 Third Avenue, Suite 2800
Seattle, WA 98104
(206) 302-6500

MOSSADAMS

Table of Contents

I. Independent Service Auditor's Report

Everstream Solutions, LLC
1228 Euclid Ave., Suite 250
Cleveland, OH 44115

To the Management of Everstream Solutions, LLC:

Scope

We have examined Everstream Solutions, LLC's accompanying description of its Grand Rapids Data Center System in Section III titled "Everstream Solutions, LLC's Description of Its Grand Rapids Data Center System" throughout the period June 1, 2020 to May 31, 2021 (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 June 1, 2020 to May 31, 2021, to provide reasonable assurance that Everstream Solutions, LLC'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 Everstream Solutions, LLC, to achieve Everstream Solutions, LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents Everstream Solutions, LLC's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Everstream Solutions, LLC'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

Everstream Solutions, LLC 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 Everstream Solutions, LLC's service commitments and system requirements were achieved. Everstream Solutions, LLC has provided the accompanying assertion in Section II titled "Everstream Solutions, LLC's Assertion" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Everstream Solutions, LLC 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 the design and operating effectiveness of the 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 report 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.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of our tests are listed in Section IV of this report titled "Trust Services Category, Criteria, Related Controls, and Tests of Controls."

Opinion

In our opinion, in all material respects:

- the description presents Everstream Solutions, LLC's Grand Rapids Data Center System that was designed and implemented throughout the period June 1, 2020 to May 31, 2021, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period June 1, 2020 to May 31, 2021 to provide reasonable assurance that Everstream Solutions, LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout that period, and if the user entities applied the complementary controls assumed in the design of Everstream Solutions, LLC's controls throughout that period.
- the controls stated in the description operated effectively throughout the period June 1, 2020 to May 31, 2021 to provide reasonable assurance that Everstream Solutions, LLC's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary user entity controls assumed in the design of Everstream Solutions, LLC's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Everstream Solutions, LLC, user entities of Everstream Solutions, LLC's Grand Rapids Data Center System during some or all of the period June 1, 2020 to May 31, 2021, business partners of Everstream Solutions, LLC subject to risks arising from interactions with the Grand Rapids Data Center System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and how those controls interact with the controls at the service organization(s) to achieve the service organization(s)'s service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the of the service organization's service commitments and system requirements and how controls address those risks

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

Moss Adams LLP

Seattle, Washington
August 25, 2021

II. Everstream Solutions, LLC's Assertion

We have prepared the accompanying description of Everstream Solutions, LLC's Grand Rapids Data Center System in Section III titled "Everstream Solutions, LLC's Description of Its Grand Rapids Data Center System" throughout the period June 1, 2020 to May 31, 2021 (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). The description is intended to provide report users with information about the Grand Rapids Data Center System that may be useful when assessing the risks arising from interactions with Everstream Solutions, LLC's Grand Rapids Data Center System, particularly information about system controls that Everstream Solutions, LLC has designed, implemented, and operated to provide reasonable assurance that its 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 Everstream Solutions, LLC, to achieve Everstream Solutions, LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents Everstream Solutions, LLC's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Everstream Solutions, LLC's controls.

We confirm, to the best of our knowledge and belief, that:

- the description presents Everstream Solutions, LLC's Grand Rapids Data Center System that was designed and implemented throughout the period June 1, 2020 to May 31, 2021, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period June 1, 2020 to May 31, 2021 to provide reasonable assurance that the Everstream Solutions, LLC service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout the period, and if the user entities applied the complementary controls assumed in the design of Everstream Solutions, LLC's controls throughout that period.
- the controls stated in the description operated effectively throughout the period June 1, 2020 to May 31, 2021 to provide reasonable assurance that Everstream Solutions, LLC's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary user entity controls assumed in the design of Everstream Solutions, LLC's controls operated effectively throughout that period.

III. Everstream Solutions, LLC's Description of Its Grand Rapids Data Center System

A. Services Provided

Everstream Solutions, LLC (Everstream or the Company) is a superregional network service provider bringing fiber-based ethernet, internet, and data center solutions to businesses throughout the Midwest. Everstream focuses on delivering best-in-class network solutions while providing a commitment to customer service. With more than 9,500 miles of fiber across five states and comprehensive data center connectivity at 100 Gigabit speed, Everstream provides the fastest network in its service areas. Everstream's network allows businesses to operate a converged IP network capable of delivering robust voice, video, and data services at speeds from 10 megabits per second (Mbps) to 100 gigabits per second (Gbps).

This report covers Everstream's data center located in Grand Rapids, Michigan.

B. Principal Service Commitments and System Requirements

Everstream is dedicated to making sure that the Company meets the necessary requirements in order to provide independent services that are compliant with applicable laws and regulations, all while meeting clients' obligations.

In order to meet client obligations, as well as applicable laws and regulations for its services, Everstream is responsible for ensuring that the system is available to meet those requirements. With a commitment to availability in mind, the company maintains documented processes and employs redundancies as necessary to ensure that it meets its service level uptime for its system. Everstream identifies the potential threats to the accessibility of the Company system and follows industry best practices to reduce the amount of downtime that would affect this availability.

The Company follows the principle of security to safeguard all protected information, which includes both Personally Identifiable Information (PII) and Protected Health Information (PHI), as well as the Grand Rapid Data Centers system. Everstream is committed to preventing unauthorized access and the potential abuse of information in order to meet client contractual agreements, as well as statutory requirements. Logical and physical access to all protected information is limited based on roles and permissions. The Company identifies the necessary roles and permissions needed to perform its services and ensures that permissions for protected information are assigned when the relevant need arises.

C. Components of the System Used to Provide the Services

1. Infrastructure

Everstream's data center located at 3950 Sparks Drive SE, Grand Rapids, Michigan is a Tier 3 facility that ensures 24x7x365 "always-on" status with dual emergency generators; technically advanced, redundant, flywheel-based uninterruptible power supplies; and power and environmental monitoring all the way to the cabinet level. This data center primarily serves cloud and colocation customers.

Everstream's cloud solution is designed using a VMware vSphere Metro Storage Cluster (vMSC) configuration. This configuration is a VMware vSphere® 5 certified solution that combines synchronous replication with array-based clustering. These solutions are typically deployed in environments where the distance between data centers is limited, often metropolitan or campus environments. VMware vMSC infrastructures are implemented with the goal of reaping the same benefits that high-availability clusters provide to a local site, but in a geographically dispersed model with two data centers in different locations. At its core, a VMware vMSC infrastructure is a stretched cluster. The architecture is built on the idea of extending what is defined as "local" in terms of network and storage. This enables these subsystems to span geographies, presenting a single and common base infrastructure set of resources to the vSphere cluster at both sites. In essence, it stretches network and storage between sites.

2. Software

Everstream is centered on a combination of the Company's own platforms and third party hosting systems. Everstream houses its own website hosting services, cloud services, and operations support systems (OSS) for billing, but relies on Salesforce.com for trouble ticket management, change management, and customer relationship management. The Marketing team uses Constant Contact for marketing campaigns.

When developing internal systems used by Everstream, Everstream has standardized on the PHP development language following the Zen Framework used with PostgreSQL and MySQL as the backend database. Drupal is also used as a content management platform with some customized modules developed. Everstream maintains separate environments for their development activities. Development is conducted in development systems and there are separate environments for test/quality assurance (QA), staging, and production.

3. People

Everstream's organizational structure is made up of distinct business units and departments to define reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. Everstream is led by the Chief Executive Officer (CEO), who has the Chief Financial Officer (CFO), Chief Technology Officer (CTO), Chief Revenue Officer (CRO), and Chief Marketing Officer (CMO) reporting directly to him. The CTO has a number of teams reporting to him that manage the data center operations, including the IT/Cloud Computing Services, Network Operations Center, Core Routing, and Network Engineering teams. The corporate organizational chart is maintained by the Manager, Office Administration and is available for viewing on the Company's shared drive.

4. Data

Data is logically partitioned such that employee or customer accounts can never see the data for any other user. Everstream does not have access to any user entity data. Everstream provides services such as physical security controls to ensure that unauthorized personnel cannot access user entity devices that are stored within the Everstream Grand Rapids data center.

5. Processes and Procedures

Everstream's data center operations business process/procedures include:

- 24x7 Network Operations Center (NOC) monitoring for health and performance
- Physical and logical access control
- Visitor management process
- Customer on-boarding/off-boarding
- Employee on-boarding/off-boarding
- Preventative maintenance on data center infrastructure
- Change management process
- IT security and availability policies
- Employee Handbook policies
- Hiring and termination policies

D. Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

1. Control Environment

Everstream strives to achieve the highest level of integrity and ethical values. With these objectives in mind, the management team has developed a distinct set of policies and procedures to help guide employee actions when accessing client systems and making changes to the infrastructure. Security and availability policies and procedures are accessible by employees and updated as needed by management. In addition to policies and procedures, Everstream has developed comprehensive job descriptions for each position that detail the responsibilities and areas of coverage for each position in the Company.

RECRUITING AND HIRING

When there is a need to fill an open job position, a job description is provided to Human Resources (HR). HR develops a posting narrative.

Prior to hiring a new employee, a copy of their resume is obtained and a background check is performed. The background check includes a criminal history, education, and experience check.

Interviews with the hiring manager and select staff are conducted once the resumes have been narrowed down to a pool of candidates. Management evaluates the potential candidates and prepares a formal offer letter along with job description for the one selected.

PERFORMANCE REVIEWS

New employees are granted a minimum 90-day probationary period from their first day on the job. After 90 days, the new employee's performance is evaluated.

Performance reviews are conducted at least annually between the employee and their manager. The reviews occur in January after the fiscal year ends or the employee's anniversary date and mid-year. Performance reviews consist of the employee highlighting their accomplishments during the prior year with their manager. The accomplishments are evaluated against goals that were set at the beginning of the performance period and their job description.

If needed, performance improvement plans (PIP) are developed by the employee's managers and Directors to provide specific development guidance. The employee is required to sign the performance review form after the meeting with their supervisor and manager. A copy of the performance review is retained by the CEO and kept in the employee folder.

SEPARATIONS

When an employee separates from Everstream, a service ticket is created to ensure network and physical access are disabled. The checklist is completed by HR to ensure that all access to any equipment and applications is removed. HR works directly with IT security, NOC, Accounting, Developers, and management teams.

The IT security team requests advance notice of up to 24 hours so that the Active Directory Account can be disabled as scheduled. The Active Directory controls network access, Outlook, shared documents, Terminal Access Controller Access-Control System (TACACS) System, Employee portals, and remote access via VPN. Off-boarding requests are submitted via email notification or help desk ticket to have remote VPN and network access disabled, system login terminated, and email access disabled. The Compliance and HR Director schedules and completes an exit interview with the off-boarded employee, who is provided a list of equipment to return, including laptops. In the event that operations staff with access to client servers and network equipment is terminated, Everstream removes access through Active Directory which is integrated with the Terminal Access Controller Access-Control System (TACACS) server. If the terminated employee is not tied to TACACS, Developers, NOC, or IT will change all of the passwords to the systems and devices once notified of the termination.

BUILDING SECURITY

The Grand Rapids data center is located in the basement of a corporate office complex. Surveillance cameras dot the exterior of the building and are also strategically pointed toward the main office. Surveillance cameras are positioned near doorway entrances throughout the Grand Rapids office area and the data center. Two large monitors are monitored in the NOC that display the footage from the surveillance cameras.

All entrances to the Grand Rapids data center facility remain locked with the exception of the main office entry. A badge reader is positioned at all entrance points into the building and throughout the data center space. The badge reader system at the Grand Rapids data center is configured to trigger an alarm if any of the monitored doors are open for an extended period of time.

Only authorized customers, Everstream employees, and subcontractors are provided the badge-reader-controlled access to the data center.

DATA CENTER ACCESSIBILITY

At the Grand Rapids data center facility, in order to descend the elevator to the lower data center floor, a configured badge swipe is required. Once a collocated customer is at the basement lower level, they are required to swipe their badge and enter the PIN at the entrance to the customer work area, which sits between the elevator lobby and the data center floor. Collocated customers need to swipe their badge and enter the PIN again at the badge reader at the top of the ramp leading up to the data center floor entrance from the customer work area.

The badge reader system captures and records all badge swipes throughout the facility. The badge reader system records the badge number, name of the Everstream or customer staff, date, time, and door accessed. The NOC continually monitors all badge reader access live on a screen in the NOC work area. The monitor shows the person's name, picture of person, facility, and time.

Access for new employees or changes in position is granted or updated based on authorization documented in a service ticket.

PHYSICAL NETWORK SECURITY

There are multiple access levels to restrict access throughout the Grand Rapids facility, including an access level for customers whose access will be limited to just the data center entrances.

At the Grand Rapids data center, customer systems are physically protected from tampering, damage, and theft as they sit in single-tenant, dual-door, lockable, and fully sealed server cabinets. The customer is provided a three-digit combination code to unlock their cabinet.

CHANGE MANAGEMENT

Everstream has a written change management policy to guide the change management process. All changes are documented in the ticketing system and include details of the change, what systems are affected, rollback procedures, and expected impacts. Data center changes are reviewed and approved by the CAB.

Most of the servers at Everstream are custom, in-house-built units. Server hardware has been standardized using a number of different OEM vendors depending on the component. Everstream uses standard hardware and equipment for core processors, RAM memory, hard disks, disk controller cards, and motherboards. In addition, a single vendor is used as the network interface card supplier while onboard video cards are used for video output.

Configuration and implementation changes are managed through the Change Advisory Board (CAB) process.

REDUNDANCY

Redundancy is built into customer requirements. RAID 1 (disk mirroring) is utilized as a minimum level of redundancy for disk storage. Dual power supplies and network interface cards (NICs) are installed as needed depending on customer requests and agreed-upon service level agreements. Systems that are critical to the infrastructure have dual power supplies and NICs.

A spare network switch is kept on hand, should a production switch fail. In the event of a failure, operations staff would replace the switch and install a backup configuration of the production switch onto the spare.

Redundant connectivity to the internet is enabled with the use of redundant routers and different transit providers, which include Cogent, nLayer, Verizon Business, NTT, and Level 3.

At the data center, each server cabinet's environmental health is monitored through temperature and humidity sensors that provide data via simple network management protocol (SNMP) The Grand Rapids data center has implemented a number of redundant environmental controls to provide high availability to customer systems. Electrical power to each server cabinet is provided via two power-distribution units configured for A/B circuits. Power to the data center floor is ensured with dual redundant 600kVA active flywheel enterprise-class UPS units and two 800kVA diesel generators. For air cooling, three Emerson Liebert 22-ton air conditioning units are configured to all run in either a reduced capacity, or N+1 configuration with the third unit on active standby.

PERFORMANCE MONITORING

Everstream uses a variety of monitoring tools in the NOC. Opsview is the main tool used for enterprise network and cloud monitoring, and other tools like Nagios, Cacti, RTG, SolarWinds NPM and NTM, and vendor-specific tools provide additional monitor and alerting functionality. Network and cloud monitoring is performed and logged in historical charts. The charts show performance metrics tracked over a set time period. These metrics include packets per second, packet loss, and downtime.

Everstream monitors the two core routers and six transit uplinks for issues such as latency, jitter, and packet loss. Critical infrastructure components, including switching, process utilization, memory utilization, temperature, and power utilization are monitored. Network performance is monitored based on preconfigured thresholds. NOC staff is alerted if thresholds are exceeded. Alerts can be in the form of email, visual alerts on the NOC monitors, or both. At the data center, each server cabinet's environmental health is monitored through temperature and humidity sensors that provide data via simple network management protocol (SNMP).

PREVENTATIVE MAINTENANCE

Generator preventative maintenance occurs on a semiannual basis (every six months), with one of the visits involving a full load test.

Equipment at the Grand Rapids data center undergoes periodic and scheduled preventative maintenance checks by local service providers. Air conditioning units and the fire suppression system undergo a semiannual preventative maintenance check, and the UPS system is maintained on a four-year cyclical basis.

ENVIRONMENTAL CONTROLS

The data center in Grand Rapids is equipped with various environmental controls. Dual, redundant 600kVA active flywheel Uninterruptible Power Supply (UPS) units provide backup power to the data center floor in the event of a sudden outage. There are two diesel 800kw generators secured in a bunker area that take the single electrical power feed from the local utility to power the data center floor. To ensure that the generators can start up with no issues, an Active Power GenStart unit provides A/C power from the enterprise class UPS for initial startup. Air cooling is handled by three 22-ton air conditioning units that run simultaneously in the data center.

Fire suppression at the data center comes from an FM200 system that is supplemented by a very early smoke detection apparatus (VESDA) system. In addition, multiple ceiling-mounted smoke detectors dot the ceiling of the data center. Handheld fire extinguishers are also available in the data center.

BACKUP

Everstream offers limited backup management services to some customers. The service provides the use of backup management software and disk-to-disk backup. The configuration of the backup process, including backup job type, schedule, and frequency is administered by the customer.

2. Risk Assessment Process

In a constantly changing business context, risk assessment and security monitoring is a continuous process from the perspective of the efficacy of the tools deployed and from a regulatory perspective as amendments and updates are released by the regulatory bodies. Everstream has established a process to review and maintain reasonable and appropriate security measures to comply with regulations. Initially the evaluation must be based on best practice security standards that help to comply with government and industry regulations. Subsequent evaluations must be performed in response to environmental or operational changes that affect the security and potentially introduce risk to the environment. Everstream conducts ongoing evaluations on a scheduled basis, annually. The evaluation includes reviews of the technical and nontechnical aspects of the security program to minimize risk to proprietary and customer systems.

3. Information and Communication Systems

The controls outlined in this report are supported through executive meetings to the staff as a whole. Everstream management believes that open lines of communication are the best way to enhance its ability to serve its customers.

Employees are encouraged to engage their peers and managers to improve the quality and productivity of their services. This encouragement comes from executive level staff meetings and from their direct reports within departments. Periodic departmental meetings create an atmosphere to allow staff to outline concerns and find solutions. Special teams are formed as needed to address specific issues which warrant further investigation or more focused level of resolution.

4. Monitoring Controls

As part of the Company's performance monitoring efforts, the Everstream management team has weekly continuous improvement meetings to ensure that the Company is meeting its obligations to its customers and stakeholders. The meeting topics include such topics as maintenance processes, visitor management, research and development, sales efforts, employee training, among others. The meeting is also used to monitor progress on current initiatives and improvement efforts.

E. Trust Services Criteria and Related Controls

Although the applicable trust services criteria, related controls, and management responses to deviations, if any, are presented in Section IV of this report titled "Trust Services Category, Criteria, Related Controls, and Tests of Controls", they are an integral part of Everstream's system description throughout the period June 1, 2020 to May 31, 2021.

F. Complementary User Entity Controls

Everstream's Grand Rapids Data Center System was designed under the assumption that certain controls would be implemented by the user entities for whom it provides its Grand Rapids Data Center System. In these situations, the application of specific controls at these customer organizations is necessary to achieve certain control objectives included in this report.

This section describes additional controls that should be in operation at the customer organizations to complement the controls at Everstream. User auditors should consider whether the following controls have been placed in operation by the customers.

Each customer must evaluate its own internal control structure to determine if the identified customer controls are in place. Users are responsible for:

Complementary User Entity Controls	
1	Implementing sound and consistent internal controls regarding general IT system access, and system usage appropriateness for all internal user entity components associated with Everstream.
2	Updating the initial password provided by Everstream upon login.
3	Timely removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with Everstream's data center products and services.
4	Ensuring transactions for user entities relating to Everstream's data center products and services are appropriately authorized, and transactions are secure, timely, and complete.
5	For user entities sending data to Everstream, data must be protected by appropriate methods for ensuring confidentiality, privacy, integrity, availability, and non-repudiation.
6	Reporting to Everstream in a timely manner any material changes to their overall control environment that may adversely affect services being performed by Everstream.

Complementary User Entity Controls	
7	Notifying Everstream in a timely manner of any changes to personnel directly involved with services performed by Everstream. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by Everstream.
8	Adhering to the terms and conditions stated within their contracts with Everstream.
9	Alerting Everstream about any regulatory changes within their industry that might affect their services.
10	Notifying Everstream of any accompanying vendors or contractors that are not on the authorization list that will be escorted by authorized company personnel.
11	Developing and, if necessary, implementing a business continuity and disaster recovery plan that will aid in the continuation of services provided by Everstream.
12	Maintaining appropriate disaster recovery processes and procedures, including backups of data.

IV. Trust Services Category, Criteria, Related Controls, and Tests of Controls

This SOC 2 Type 2 Report was prepared in accordance with the AICPA attestation standards, and has been performed to examine the suitability of the design and operating effectiveness of controls to meet the criteria for the Security and Availability categories set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) throughout the period June 1, 2020 through May 31, 2021.

The trust services categories for the Security and Availability criteria and related controls specified by Everstream are presented in Section IV of this report.

Test procedures performed in connection with determining the operating effectiveness of controls detailed here in Section IV are described below:

Test Procedure	Description
Inquiries	Inquiry of appropriate personnel and corroboration with management.
Observation	Observation of the application, performance or existence of the control.
Inspection	Inspection of documents and reports indicating performance of the control.
Reperformance	Reperformance of the control.

APPLICABLE TRUST SERVICES CRITERIA RELEVANT TO SECURITY AND AVAILABILITY

CC 1.0 Control Environment				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 1.1	The entity demonstrates a commitment to integrity and ethical values.	Security and availability policies and procedures are accessible by employees and updated as needed by management.	Inquired of the VP of Human Resources about security and availability policies noting that security and availability policies and procedures were accessible by employees and updated as needed by management. Inspected security and availability policies and procedures and company intranet noting that security and availability policies and procedures were accessible by employees and updated as needed by management.	No exceptions noted. No exceptions noted.
		Upon hire, employees acknowledge receipt of the employee handbook which covers security and confidentiality of information, and workforce conduct standards.	Inquired of the VP of Human Resources about new employee documentation noting that new employees were provided the employee handbook, which covered security and confidentiality of information and workforce conduct standards. Also noted that employees were required to acknowledge receipt of the employee handbook. Inspected the employee handbook noting that the employee handbook covered security and confidentiality of information, and workforce conduct standards. Inspected signed employee handbook acknowledgements for randomly selected new hires during the examination period noting that each new hire had signed an employee handbook acknowledgement.	No exceptions noted. No exceptions noted. No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The Board of Directors is governed by a set of bylaws that outlines the Board of Directors' responsibility for governance and oversight.	Inquired of VP, Service Delivery about the bylaws of the Board of Directors noting that the Board of Directors was governed by a set of bylaws that outlined the Board of Directors' responsibility for governance and oversight. Inspected the Everstream Operating Agreement, dated May 12, 2014, noting that the Board of Directors was governed by a set of bylaws that outlined the Board of Directors' responsibility for governance and oversight.	No exceptions noted. No exceptions noted.
		The Board of Directors meets once a quarter to review the financial position of the company, as well as strategic and operational initiatives and deficiencies. This includes any reported security events or instances of fraud.	Inquired of the VP, Service Delivery about Board Meetings noting that the Board of Directors met once a quarter to review the financial position of the company, as well as strategic and operational initiatives and deficiencies. Also noted that this included any reported security events or instances of fraud. Inspected board meeting summaries for randomly selected quarters during the examination period noting that the Board of Directors met once a quarter to review the financial position of the company, as well as strategic and operational initiatives and deficiencies. Also noted that this included any reported security events or instances of fraud.	No exceptions noted. No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The Board of Directors meets once a quarter to review the financial position of the company, as well as strategic and operational initiatives and deficiencies. This includes any reported security events or instances of fraud.	Inquired of the VP, Service Delivery about Board Meetings noting that the Board of Directors met once a quarter to review the financial position of the company, as well as strategic and operational initiatives and deficiencies. Also noted that this included any reported security events or instances of fraud. Inspected board meeting summaries for randomly selected quarters during the examination period noting that the Board of Directors met once a quarter to review the financial position of the company, as well as strategic and operational initiatives and deficiencies. Also noted that this included any reported security events or instances of fraud.	No exceptions noted. No exceptions noted.
		Everstream's organizational structure is made up of distinct business units and departments that define reporting lines, authorities, as well as responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	Inquired of the VP of Human Resources and Human Resources Manager about company organization noting that the organizational chart was made up of distinct business units and departments that defined reporting lines, authorities, as well as responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. Inspected Everstream's organization chart noting that the organizational chart was made up of distinct business units and departments that defined reporting lines, authorities, as well as responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted. No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		The responsibility and accountability for the security and availability of the data center system is assigned to the Chief Technology Officer (CTO).	Inquired of the VP of Human Resources about responsibility and accountability for the data center system noting that the responsibility and accountability for the security and availability of the data center system was assigned to the CTO. Inspected job description of the CTO noting that the responsibility and accountability for the security and availability of the data center system was assigned to the CTO.	No exceptions noted. No exceptions noted.
		Job descriptions are available for each position that define roles and responsibilities.	Inquired of the VP of Human Resources about job descriptions noting that job descriptions were available for each position that defined roles and responsibilities. Inspected job descriptions for randomly selected current employees during the examination period noting that job descriptions were available that defined roles and responsibilities.	No exceptions noted. No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Prior to hiring a new employee, a copy of their resume is obtained and a background check is performed. The background check includes a criminal history, education, and experience check.	Inquired of the VP of Human Resources about the hiring process noting that Everstream obtained a resume for each new hire. Also noted that a background check was completed that included a criminal history, education, and experience check. Inspected resumes and background checks for randomly selected new hires during the examination period noting that a resume was obtained and a background check was performed. Also noted that the background check included criminal history, education, and experience check.	No exceptions noted. No exceptions noted.
		Upon hire, employees acknowledge receipt of the employee handbook which covers security and confidentiality of information, and workforce conduct standards.	Inquired of the VP of Human Resources about new employee documentation noting that new employees were provided the employee handbook, which covered security and confidentiality of information and workforce conduct standards. Also noted that employees were required to acknowledge receipt of the employee handbook. Inspected the employee handbook noting that the employee handbook covered security and confidentiality of information, and workforce conduct standards. Inspected signed employee handbook acknowledgements for randomly selected new hires during the examination period noting that each new hire had signed an employee handbook acknowledgement.	No exceptions noted. No exceptions noted. No exceptions noted.
		Security and availability policies and procedures are accessible by employees and updated as needed by management.	Inquired of the VP of Human Resources about security and availability policies noting that security and availability policies and procedures were accessible by employees and updated as needed by management. Inspected security and availability policies and procedures and company intranet noting that security and availability policies and procedures were accessible by employees and updated as needed by management.	No exceptions noted. No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Performance reviews are conducted at least annually between the employee and their manager.	Inquired of the VP of Human Resources about performance evaluations noting that performance reviews were conducted at least annually between employees and managers. Inspected performance evaluations for randomly selected employees during the examination period noting that each employee had an annual performance review conducted between the employee and their manager.	No exceptions noted. No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Security and availability policies and procedures are accessible by employees and updated as needed by management.	Inquired of the VP of Human Resources about security and availability policies noting that security and availability policies and procedures were accessible by employees and updated as needed by management. Inspected security and availability policies and procedures and company intranet noting that security and availability policies and procedures were accessible by employees and updated as needed by management.	No exceptions noted. No exceptions noted.
		The responsibility and accountability for the security and availability of the data center system is assigned to the Chief Technology Officer (CTO).	Inquired of the VP of Human Resources about responsibility and accountability for the data center system noting that the responsibility and accountability for the security and availability of the data center system was assigned to the CTO. Inspected job description of the CTO noting that the responsibility and accountability for the security and availability of the data center system was assigned to the CTO.	No exceptions noted. No exceptions noted.
		Job descriptions are available for each position that define roles and responsibilities.	Inquired of the VP of Human Resources about job descriptions noting that job descriptions were available for each position that defined roles and responsibilities. Inspected job descriptions for randomly selected current employees during the examination period noting that job descriptions were available that defined roles and responsibilities.	No exceptions noted. No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Upon hire, employees acknowledge receipt of the employee handbook which covers security and confidentiality of information, and workforce conduct standards.	Inquired of the VP of Human Resources about new employee documentation noting that new employees were provided the employee handbook, which covered security and confidentiality of information and workforce conduct standards. Also noted that employees were required to acknowledge receipt of the employee handbook.	No exceptions noted.
			Inspected the employee handbook noting that the employee handbook covered security and confidentiality of information, and workforce conduct standards.	No exceptions noted.
			Inspected signed employee handbook acknowledgements for randomly selected new hires during the examination period noting that each new hire had signed an employee handbook acknowledgement.	No exceptions noted.
		Performance reviews are conducted at least annually between the employee and their manager.	Inquired of the VP of Human Resources about performance evaluations noting that performance reviews were conducted at least annually between employees and managers.	No exceptions noted.
			Inspected performance evaluations for randomly selected employees during the examination period noting that each employee had an annual performance review conducted between the employee and their manager.	No exceptions noted.

CC 2.0 Communication and Information				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The Board of Directors meets once a quarter to review the financial position of the company, as well as strategic and operational initiatives and deficiencies. This includes any reported security events or instances of fraud.	Inquired of the VP, Service Delivery about Board Meetings noting that the Board of Directors met once a quarter to review the financial position of the company, as well as strategic and operational initiatives and deficiencies. Also noted that this included any reported security events or instances of fraud. Inspected board meeting summaries for randomly selected quarters during the examination period noting that the Board of Directors met once a quarter to review the financial position of the company, as well as strategic and operational initiatives and deficiencies. Also noted that this included any reported security events or instances of fraud.	No exceptions noted. No exceptions noted.
		Everstream conducts an annual risk assessment to (1) identify potential threats that would impair system security and availability commitments and requirements, (2) analyze the significance of risks associated with the identified threats, and (3) determine mitigation strategies for those risks.	Inquired of the Chief Technology Officer about the risk assessment process noting that Everstream conducted an annual risk assessment to (1) identify potential threats that could impair system security and availability commitments and requirements, (2) analyze the significance of risks associated with the identified threats, and (3) determine mitigation strategies for those risks. Inspected the Risk Assessment Report and Risk Mitigation Process noting that Everstream conducted an annual risk assessment to (1) identify potential threats that would impair system security and availability commitments and requirements, (2) analyze the significance of risks associated with the identified threats, and (3) determine mitigation strategies for those risks.	No exceptions noted. No exceptions noted.

CC 2.0 Communication and Information				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Security and availability policies and procedures are accessible by employees and updated as needed by management.	Inquired of the VP of Human Resources about security and availability policies noting that security and availability policies and procedures were accessible by employees and updated as needed by management. Inspected security and availability policies and procedures and company intranet noting that security and availability policies and procedures were accessible by employees and updated as needed by management.	No exceptions noted. No exceptions noted.
		Everstream has an internal wiki available to employees to provide information on the design and operation of the system.	Inquired of the Director, Network Operations Center about the internal wiki noting that the wiki was available to provide employees information on the design and operation of the system. Inspected the internal wiki noting that the wiki was available to provide employees information on the design and operation of the system.	No exceptions noted. No exceptions noted.
		Internal and external users are provided information about the system and its boundaries on the public website.	Inquired of the Director, Network Operations Center about system information noting that internal and external users were provided information about the system and its boundaries on the public website. Inspected system information from the public website noting that internal and external users were provided information about the system and its boundaries on the public website.	No exceptions noted. No exceptions noted.
		Performance reviews are conducted at least annually between the employee and their manager.	Inquired of the VP of Human Resources about performance evaluations noting that performance reviews were conducted at least annually between employees and managers. Inspected performance evaluations for randomly selected employees during the examination period noting that each employee had an annual performance review conducted between the employee and their manager.	No exceptions noted. No exceptions noted.

CC 2.0 Communication and Information				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Everstream has customer support contact information on their website which includes a service support guide and Network Operations Center (NOC) escalation list that is available to internal and external users.	Inquired of the Director, Network Operations Center about customer support noting that Everstream had customer support contact information on their website which included a service support guide and NOC escalation list that was available to internal and external users. Inspected customer support information on the Company website noting that Everstream had customer support contact information on their website which included a service support guide and NOC escalation list that was available to internal and external users.	No exceptions noted. No exceptions noted.
		The ticketing system tracks all customer incidents and internally reported incidents from the time the ticket is opened until it is resolved.	Inquired of the Director, Network Operations Center about the ticketing system noting that the Operations staff utilized a ticketing system to track customer incidents and internally reported incidents from the time the ticket was opened until it was resolved. Inspected the tickets for randomly selected customer and internally reported incidents during the examination period noting that the ticketing system tracked customer incidents and internally reported incidents from the time the ticket was opened until it was resolved.	No exceptions noted. No exceptions noted.
		On any interruption of service, Everstream's NOC activates to monitor the departments required to ensure service is repaired quickly. Support tickets are opened for maintenance and outages. For customer impacting outages, once the interruption has been repaired, a reason for outage (RFO) is completed upon customer request.	Inquired of the Director, Network Operations Center about interruption of service noting that upon any interruption of service, Everstream's NOC activated to monitor the departments required to ensure service was repaired quickly. Noted that support tickets were opened for maintenance and outages. Also noted that once the interruption had been repaired, an RFO was completed upon customer request. Inspected support tickets for randomly selected interruption of service outages during the examination period noting that each ticket documented the status, progress, and if required, an RFO and resolution.	No exceptions noted. No exceptions noted.

CC 2.0 Communication and Information				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Each new customer is provided a master services agreement and product specific service agreement to define commitments.	Inquired of the VP, Service Delivery about new customer onboarding noting that each new customer was provided a master services agreement and product specific service agreement to define commitments. Also noted that there were no new customers onboarded during the examination period.	No exceptions noted.
		Internal and external users are provided information about the system and its boundaries on the public website.	Inquired of the Director, Network Operations Center about system information noting that internal and external users were provided information about the system and its boundaries on the public website. Inspected system information from the public website noting that internal and external users were provided information about the system and its boundaries on the public website.	No exceptions noted. No exceptions noted.
		Everstream has customer support contact information on their website which includes a service support guide and Network Operations Center (NOC) escalation list that is available to internal and external users.	Inquired of the Director, Network Operations Center about customer support noting that Everstream had customer support contact information on their website which included a service support guide and NOC escalation list that was available to internal and external users. Inspected customer support information on the Company website noting that Everstream had customer support contact information on their website which included a service support guide and NOC escalation list that was available to internal and external users.	No exceptions noted. No exceptions noted.

CC 2.0 Communication and Information				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		On any interruption of service, Everstream's NOC activates to monitor the departments required to ensure service is repaired quickly. Support tickets are opened for maintenance and outages. For customer impacting outages, once the interruption has been repaired, a reason for outage (RFO) is completed upon customer request.	Inquired of the Director, Network Operations Center about interruption of service noting that upon any interruption of service, Everstream's NOC activated to monitor the departments required to ensure service was repaired quickly. Noted that support tickets were opened for maintenance and outages. Also noted that once the interruption had been repaired, an RFO was completed upon customer request. Inspected support tickets for randomly selected interruption of service outages during the examination period noting that each ticket documented the status, progress, and if required, an RFO and resolution.	No exceptions noted. No exceptions noted.

CC 3.0 Risk Assessment				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Everstream conducts an annual risk assessment to (1) identify potential threats that would impair system security and availability commitments and requirements, (2) analyze the significance of risks associated with the identified threats, and (3) determine mitigation strategies for those risks.	Inquired of the Chief Technology Officer about the risk assessment process noting that Everstream conducted an annual risk assessment to (1) identify potential threats that could impair system security and availability commitments and requirements, (2) analyze the significance of risks associated with the identified threats, and (3) determine mitigation strategies for those risks. Inspected the Risk Assessment Report and Risk Mitigation Process noting that Everstream conducted an annual risk assessment to (1) identify potential threats that would impair system security and availability commitments and requirements, (2) analyze the significance of risks associated with the identified threats, and (3) determine mitigation strategies for those risks.	No exceptions noted. No exceptions noted.
		Vulnerability tests on the corporate network are performed weekly by utilizing common vulnerability testing toolkits such as Nessus.	Inquired of the IT Manager about vulnerability testing noting that vulnerability tests were conducted on the corporate network weekly by utilizing common vulnerability testing toolkits such as Nessus. Inspected the Nessus vulnerability scan log for randomly selected weeks during the examination period noting that a scan was conducted on the corporate network on a weekly basis utilizing common vulnerability testing toolkits such as Nessus.	No exceptions noted. No exceptions noted.

CC 3.0 Risk Assessment				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The Board of Directors meets once a quarter to review the financial position of the company, as well as strategic and operational initiatives and deficiencies. This includes any reported security events or instances of fraud.	Inquired of the VP, Service Delivery about Board Meetings noting that the Board of Directors met once a quarter to review the financial position of the company, as well as strategic and operational initiatives and deficiencies. Also noted that this included any reported security events or instances of fraud. Inspected board meeting summaries for randomly selected quarters during the examination period noting that the Board of Directors met once a quarter to review the financial position of the company, as well as strategic and operational initiatives and deficiencies. Also noted that this included any reported security events or instances of fraud.	No exceptions noted. No exceptions noted.
		Everstream conducts an annual risk assessment to (1) identify potential threats that would impair system security and availability commitments and requirements, (2) analyze the significance of risks associated with the identified threats, and (3) determine mitigation strategies for those risks.	Inquired of the Chief Technology Officer about the risk assessment process noting that Everstream conducted an annual risk assessment to (1) identify potential threats that could impair system security and availability commitments and requirements, (2) analyze the significance of risks associated with the identified threats, and (3) determine mitigation strategies for those risks. Inspected the Risk Assessment Report and Risk Mitigation Process noting that Everstream conducted an annual risk assessment to (1) identify potential threats that would impair system security and availability commitments and requirements, (2) analyze the significance of risks associated with the identified threats, and (3) determine mitigation strategies for those risks.	No exceptions noted. No exceptions noted.

CC 3.0 Risk Assessment				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Vulnerability tests on the corporate network are performed weekly by utilizing common vulnerability testing toolkits such as Nessus.	Inquired of the IT Manager about vulnerability testing noting that vulnerability tests were conducted on the corporate network weekly by utilizing common vulnerability testing toolkits such as Nessus. Inspected the Nessus vulnerability scan log for randomly selected weeks during the examination period noting that a scan was conducted on the corporate network on a weekly basis utilizing common vulnerability testing toolkits such as Nessus.	No exceptions noted. No exceptions noted.

CC 3.0 Risk Assessment				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The Board of Directors meets once a quarter to review the financial position of the company, as well as strategic and operational initiatives and deficiencies. This includes any reported security events or instances of fraud.	Inquired of the VP, Service Delivery about Board Meetings noting that the Board of Directors met once a quarter to review the financial position of the company, as well as strategic and operational initiatives and deficiencies. Also noted that this included any reported security events or instances of fraud. Inspected board meeting summaries for randomly selected quarters during the examination period noting that the Board of Directors met once a quarter to review the financial position of the company, as well as strategic and operational initiatives and deficiencies. Also noted that this included any reported security events or instances of fraud.	No exceptions noted. No exceptions noted.
		Everstream conducts an annual risk assessment to (1) identify potential threats that would impair system security and availability commitments and requirements, (2) analyze the significance of risks associated with the identified threats, and (3) determine mitigation strategies for those risks.	Inquired of the Chief Technology Officer about the risk assessment process noting that Everstream conducted an annual risk assessment to (1) identify potential threats that could impair system security and availability commitments and requirements, (2) analyze the significance of risks associated with the identified threats, and (3) determine mitigation strategies for those risks. Inspected the Risk Assessment Report and Risk Mitigation Process noting that Everstream conducted an annual risk assessment to (1) identify potential threats that would impair system security and availability commitments and requirements, (2) analyze the significance of risks associated with the identified threats, and (3) determine mitigation strategies for those risks.	No exceptions noted. No exceptions noted.

CC 3.0 Risk Assessment				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Vulnerability tests on the corporate network are performed weekly by utilizing common vulnerability testing toolkits such as Nessus.	Inquired of the IT Manager about vulnerability testing noting that vulnerability tests were conducted on the corporate network weekly by utilizing common vulnerability testing toolkits such as Nessus. Inspected the Nessus vulnerability scan log for randomly selected weeks during the examination period noting that a scan was conducted on the corporate network on a weekly basis utilizing common vulnerability testing toolkits such as Nessus.	No exceptions noted. No exceptions noted.
		A weekly trouble ticket report is reviewed and evaluated by the Chief Technology Officer, who provides metrics to the executive team during the weekly executive team meeting.	Inquired of the Chief Technology Officer about the weekly executive team meetings noting that a weekly trouble ticket report was reviewed and evaluated by the Chief Technology Officer, who provided metrics to the executive team during the weekly executive team meeting. Inspected executive team meeting minutes for randomly selected weeks during the examination period noting that a weekly trouble ticket report was reviewed and evaluated by the Chief Technology Officer, who provided metrics to the executive team during weekly executive team meetings.	No exceptions noted. No exceptions noted.

CC 4.0 Monitoring Activities				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	A weekly trouble ticket report is reviewed and evaluated by the Chief Technology Officer, who provides metrics to the executive team during the weekly executive team meeting.	Inquired of the Chief Technology Officer about the weekly executive team meetings noting that a weekly trouble ticket report was reviewed and evaluated by the Chief Technology Officer, who provided metrics to the executive team during the weekly executive team meeting.	No exceptions noted.
			Inspected executive team meeting minutes for randomly selected weeks during the examination period noting that a weekly trouble ticket report was reviewed and evaluated by the Chief Technology Officer, who provided metrics to the executive team during weekly executive team meetings.	No exceptions noted.
		Network and cloud monitoring is performed and logged in historical charts. The charts show performance metrics tracked over a set time period. These metrics include packets per second, packet loss, and downtime.	Inquired of the IT Manager about monitoring noting that network and cloud monitoring was performed and logged in historical charts. Noted that the charts showed performance metrics tracked over a set time period. Also noted that these metrics included packets per second, packet loss, and downtime.	No exceptions noted.
			Inspected network monitoring historical charts for the examination period noting that network and cloud monitoring was performed and logged in historical charts. Noted that the charts showed performance metrics tracked over a set time period. Also noted that these metrics included packets per second, packet loss, and downtime.	No exceptions noted.
		Vulnerability tests on the corporate network are performed weekly by utilizing common vulnerability testing toolkits such as Nessus.	Inquired of the IT Manager about vulnerability testing noting that vulnerability tests were conducted on the corporate network weekly by utilizing common vulnerability testing toolkits such as Nessus.	No exceptions noted.
			Inspected the Nessus vulnerability scan log for randomly selected weeks during the examination period noting that a scan was conducted on the corporate network on a weekly basis utilizing common vulnerability testing toolkits such as Nessus.	No exceptions noted.

CC 4.0 Monitoring Activities				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Firewall logs are maintained in Loggly Logs and retained three months for review as needed.	Inquired of the Manager, Information Systems about firewall logging noting that firewall logs were maintained in Loggly Logs and retained three months for review as needed. Inspected the firewall logging retention configuration and firewall logs noting that firewall logs were maintained in Loggly Logs and retained three months for review as needed.	No exceptions noted. No exceptions noted.

CC 4.0 Monitoring Activities				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The Board of Directors meets once a quarter to review the financial position of the company, as well as strategic and operational initiatives and deficiencies. This includes any reported security events or instances of fraud.	Inquired of the VP, Service Delivery about Board Meetings noting that the Board of Directors met once a quarter to review the financial position of the company, as well as strategic and operational initiatives and deficiencies. Also noted that this included any reported security events or instances of fraud. Inspected board meeting summaries for randomly selected quarters during the examination period noting that the Board of Directors met once a quarter to review the financial position of the company, as well as strategic and operational initiatives and deficiencies. Also noted that this included any reported security events or instances of fraud.	No exceptions noted. No exceptions noted.
		Everstream conducts an annual risk assessment to (1) identify potential threats that would impair system security and availability commitments and requirements, (2) analyze the significance of risks associated with the identified threats, and (3) determine mitigation strategies for those risks.	Inquired of the Chief Technology Officer about the risk assessment process noting that Everstream conducted an annual risk assessment to (1) identify potential threats that could impair system security and availability commitments and requirements, (2) analyze the significance of risks associated with the identified threats, and (3) determine mitigation strategies for those risks. Inspected the Risk Assessment Report and Risk Mitigation Process noting that Everstream conducted an annual risk assessment to (1) identify potential threats that would impair system security and availability commitments and requirements, (2) analyze the significance of risks associated with the identified threats, and (3) determine mitigation strategies for those risks.	No exceptions noted. No exceptions noted.

CC 4.0 Monitoring Activities				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		On any interruption of service, Everstream's NOC activates to monitor the departments required to ensure service is repaired quickly. Support tickets are opened for maintenance and outages. For customer impacting outages, once the interruption has been repaired, a reason for outage (RFO) is completed upon customer request.	Inquired of the Director, Network Operations Center about interruption of service noting that upon any interruption of service, Everstream's NOC activated to monitor the departments required to ensure service was repaired quickly. Noted that support tickets were opened for maintenance and outages. Also noted that once the interruption had been repaired, an RFO was completed upon customer request. Inspected support tickets for randomly selected interruption of service outages during the examination period noting that each ticket documented the status, progress, and if required, an RFO and resolution.	No exceptions noted. No exceptions noted.

CC 5.0 Control Activities				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Everstream conducts an annual risk assessment to (1) identify potential threats that would impair system security and availability commitments and requirements, (2) analyze the significance of risks associated with the identified threats, and (3) determine mitigation strategies for those risks.	Inquired of the Chief Technology Officer about the risk assessment process noting that Everstream conducted an annual risk assessment to (1) identify potential threats that could impair system security and availability commitments and requirements, (2) analyze the significance of risks associated with the identified threats, and (3) determine mitigation strategies for those risks. Inspected the Risk Assessment Report and Risk Mitigation Process noting that Everstream conducted an annual risk assessment to (1) identify potential threats that would impair system security and availability commitments and requirements, (2) analyze the significance of risks associated with the identified threats, and (3) determine mitigation strategies for those risks.	No exceptions noted. No exceptions noted.
		Vulnerability tests on the corporate network are performed weekly by utilizing common vulnerability testing toolkits such as Nessus.	Inquired of the IT Manager about vulnerability testing noting that vulnerability tests were conducted on the corporate network weekly by utilizing common vulnerability testing toolkits such as Nessus. Inspected the Nessus vulnerability scan log for randomly selected weeks during the examination period noting that a scan was conducted on the corporate network on a weekly basis utilizing common vulnerability testing toolkits such as Nessus.	No exceptions noted. No exceptions noted.

CC 5.0 Control Activities				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Group policy within Active Directory is used to enforce password parameters which are defined as: • Password History – Four passwords remembered • Maximum Password age – 181 days • Minimum password length – 8 characters • Minimum Password age – One day • Password must meet complexity requirements – Enabled	Inquired of the Manager, Information Systems about passwords noting that group policy within Active Directory was used to enforce password parameters which were defined as: • Password History – Four passwords remembered • Maximum Password age – 181 days • Minimum password length – 8 characters • Minimum Password age – One day • Password must meet complexity requirements – Enabled Inspected password policy for Active Directory during the examination period noting that group policy within Active Directory was used to enforce password parameters which were defined as: • Password History – Four passwords remembered • Maximum Password age – 181 days • Minimum Password age – One day • Password must meet complexity requirements – Enabled	No exceptions noted. No exceptions noted.
		For new customers, once the system implementation process is completed as ordered, the initial login credentials and password to the server are emailed to the customer and the customer is required to change their password.	Inquired of the VP, Service Delivery about new customer setups noting that once the order was completed, the login credentials and password to the server were emailed to the new customer. Noted that the customer was required to change their password. Also noted that there were no new customers during the examination period.	No exceptions noted.

CC 5.0 Control Activities				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Vulnerability tests on the corporate network are performed weekly by utilizing common vulnerability testing toolkits such as Nessus.	Inquired of the IT Manager about vulnerability testing noting that vulnerability tests were conducted on the corporate network weekly by utilizing common vulnerability testing toolkits such as Nessus. Inspected the Nessus vulnerability scan log for randomly selected weeks during the examination period noting that a scan was conducted on the corporate network on a weekly basis utilizing common vulnerability testing toolkits such as Nessus.	No exceptions noted. No exceptions noted.
		Each user has their own unique user ID. No shared accounts are in use except for certain network devices that do not support multiple authentication credentials.	Inquired of the Systems Engineer about unique user IDs noting that each user had their own unique user ID. Also noted that no shared accounts were in use except for certain network devices that did not support multiple authentication credentials. Inspected the Active Directory user listing noting that each user had their own unique user ID. Also noted that no shared accounts were in use except for certain network devices that did not support multiple authentication credentials.	No exceptions noted. No exceptions noted.
		Administrative access to the network is limited to IT and Network Administrator personnel. Administrator access to the badge system is limited to authorized personnel.	Inquired of the Manager, Information Systems about administrative access noting that administrative access to the network was limited to IT and Network Administrator personnel. Also noted that administrator access to the badge system was limited to authorized personnel. Inspected the Active Directory access listing and badge listing noting that administrative access to the network was limited to IT and Network Administrator personnel. Also noted that administrator access to the badge system was limited to authorized personnel.	No exceptions noted. No exceptions noted.

CC 5.0 Control Activities				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Security and availability policies and procedures are accessible by employees and updated as needed by management.	Inquired of the VP of Human Resources about security and availability policies noting that security and availability policies and procedures were accessible by employees and updated as needed by management. Inspected security and availability policies and procedures and company intranet noting that security and availability policies and procedures were accessible by employees and updated as needed by management.	No exceptions noted. No exceptions noted.
		Everstream has a written change management policy to guide the change management process.	Inquired of the Director, Network Operations Center about the change management policy and process noting that Everstream had a written change management policy to guide the change management process. Inspected the change management policy noting that Everstream had a written change management policy to guide the change management process.	No exceptions noted. No exceptions noted.
		The responsibility and accountability for the security and availability of the data center system is assigned to the Chief Technology Officer (CTO).	Inquired of the VP of Human Resources about responsibility and accountability for the data center system noting that the responsibility and accountability for the security and availability of the data center system was assigned to the CTO. Inspected job description of the CTO noting that the responsibility and accountability for the security and availability of the data center system was assigned to the CTO.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Group policy within Active Directory is used to enforce password parameters which are defined as: • Password History – Four passwords remembered • Maximum Password age – 181 days • Minimum password length – 8 characters • Minimum Password age – One day • Password must meet complexity requirements – Enabled	Inquired of the Manager, Information Systems about passwords noting that group policy within Active Directory was used to enforce password parameters which were defined as: • Password History – Four passwords remembered • Maximum Password age – 181 days • Minimum password length – 8 characters • Minimum Password age – One day • Password must meet complexity requirements – Enabled Inspected password policy for Active Directory during the examination period noting that group policy within Active Directory was used to enforce password parameters which were defined as: • Password History – Four passwords remembered • Maximum Password age – 181 days • Minimum Password age – One day • Password must meet complexity requirements – Enabled	No exceptions noted. No exceptions noted.
		Each user has their own unique user ID. No shared accounts are in use except for certain network devices that do not support multiple authentication credentials.	Inquired of the Systems Engineer about unique user IDs noting that each user had their own unique user ID. Also noted that no shared accounts were in use except for certain network devices that did not support multiple authentication credentials. Inspected the Active Directory user listing noting that each user had their own unique user ID. Also noted that no shared accounts were in use except for certain network devices that did not support multiple authentication credentials.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		For new customers, once the system implementation process is completed as ordered, the initial login credentials and password to the server are emailed to the customer and the customer is required to change their password.	Inquired of the VP, Service Delivery about new customer setups noting that once the order was completed, the login credentials and password to the server were emailed to the new customer. Noted that the customer was required to change their password. Also noted that there were no new customers during the examination period.	No exceptions noted.
		Administrative access to the network is limited to IT and Network Administrator personnel. Administrator access to the badge system is limited to authorized personnel.	Inquired of the Manager, Information Systems about administrative access noting that administrative access to the network was limited to IT and Network Administrator personnel. Also noted that administrator access to the badge system was limited to authorized personnel. Inspected the Active Directory access listing and badge listing noting that administrative access to the network was limited to IT and Network Administrator personnel. Also noted that administrator access to the badge system was limited to authorized personnel.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Access for new employees or changes in position is granted or updated based on authorization documented in a service ticket.	Inquired of the Human Resources Manager about new employee access noting that access for new employees or changes in position was granted or updated based on authorization documented in a service ticket. Also noted that there was no access modification for changes in position during the period. Inspected service tickets and access reports for randomly selected new hires during the examination period noting that access for new employees was granted based on authorization documented in a service ticket.	No exceptions noted. No exceptions noted.
		Everstream implemented a Ironsphere server, integrated with Active Directory, to allow for more granular access control over Everstream's network devices. This allows authorized individuals to authenticate to the network devices with their domain credentials.	Inquired of the Manager, Information Systems about the Ironsphere server noting that it integrated with Active Directory to allow Everstream more granular access control over network devices and authorized individuals to authenticate to network devices with their domain credentials. Inspected the Ironsphere settings noting that it integrated with Active Directory to allow Everstream more granular access control over network devices and authorized individuals to authenticate to network devices with their domain credentials.	No exceptions noted. No exceptions noted.
		When an employee separates from Everstream, a service ticket is created to ensure network and physical access are disabled.	Inquired of the Human Resources Manager about employee separations noting that Everstream created service tickets to ensure that network and physical access were disabled. Inspected service tickets, Active Directory reports, and badge access reports for randomly selected employee separations during the examination period noting that network and physical access were disabled.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		When customers are terminated, a disconnect order is initiated that triggers removal of logical and physical access.	Inquired of the Director, Network Operations Center about customer terminations noting that when customers were terminated, a disconnect order was initiated that triggered removal of logical and physical access. Inspected the disconnect order for randomly selected terminated customers during the examination period noting that when customers were terminated, a disconnect order was initiated that triggered removal of logical and physical access.	No exceptions noted. No exceptions noted.
		In the event that operations staff with access to client servers and network equipment is terminated, Everstream removes access through Active Directory which is integrated with the Terminal Access Controller Access-Control System (TACACS) server.	Inquired of the Manager, Information Systems about the termination of operations staff noting that when operations staff were terminated from the company, access to client servers and network equipment was terminated through the Active Directory which was integrated with the TACACS server. Inspected Active Directory access reports for randomly selected terminated operations staff during the examination period noting that access to servers and network equipment was terminated. Inspected Active Directory integration noting that Active Directory was integrated with the TACACS server.	No exceptions noted. No exceptions noted. No exceptions noted.
		Changes to customer access are documented with a service ticket and must be authorized by the Customer's Administrative User.	Inquired of the Director, Network Operations Center about customer access changes noting that changes to customer access were documented with a service ticket and were authorized by the Customer's Administrative User. Inspected service tickets for randomly selected customer access changes during the examination period noting that changes to customer access were authorized by the Customer's Administrative User.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Group policy within Active Directory is used to enforce password parameters which are defined as: • Password History – Four passwords remembered • Maximum Password age – 181 days • Minimum password length – 8 characters • Minimum Password age – One day • Password must meet complexity requirements – Enabled	Inquired of the Manager, Information Systems about passwords noting that group policy within Active Directory was used to enforce password parameters which were defined as: • Password History – Four passwords remembered • Maximum Password age – 181 days • Minimum password length – 8 characters • Minimum Password age – One day • Password must meet complexity requirements – Enabled Inspected password policy for Active Directory during the examination period noting that group policy within Active Directory was used to enforce password parameters which were defined as: • Password History – Four passwords remembered • Maximum Password age – 181 days • Minimum Password age – One day • Password must meet complexity requirements – Enabled	No exceptions noted. No exceptions noted.
		Access for new employees or changes in position is granted or updated based on authorization documented in a service ticket.	Inquired of the Human Resources Manager about new employee access noting that access for new employees or changes in position was granted or updated based on authorization documented in a service ticket. Also noted that there was no access modification for changes in position during the period. Inspected service tickets and access reports for randomly selected new hires during the examination period noting that access for new employees was granted based on authorization documented in a service ticket.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		For new customers, once the system implementation process is completed as ordered, the initial login credentials and password to the server are emailed to the customer and the customer is required to change their password.	Inquired of the VP, Service Delivery about new customer setups noting that once the order was completed, the login credentials and password to the server were emailed to the new customer. Noted that the customer was required to change their password. Also noted that there were no new customers during the examination period.	No exceptions noted.
		In the event that operations staff with access to client servers and network equipment is terminated, Everstream removes access through Active Directory which is integrated with the Terminal Access Controller Access-Control System (TACACS) server.	Inquired of the Manager, Information Systems about the termination of operations staff noting that when operations staff were terminated from the company, access to client servers and network equipment was terminated through the Active Directory which was integrated with the TACACS server.	No exceptions noted.
			Inspected Active Directory access reports for randomly selected terminated operations staff during the examination period noting that access to servers and network equipment was terminated.	No exceptions noted.
			Inspected Active Directory integration noting that Active Directory was integrated with the TACACS server.	No exceptions noted.
		When an employee separates from Everstream, a service ticket is created to ensure network and physical access are disabled.	Inquired of the Human Resources Manager about employee separations noting that Everstream created service tickets to ensure that network and physical access were disabled.	No exceptions noted.
			Inspected service tickets, Active Directory reports, and badge access reports for randomly selected employee separations during the examination period noting that network and physical access were disabled.	No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		When customers are terminated, a disconnect order is initiated that triggers removal of logical and physical access.	Inquired of the Director, Network Operations Center about customer terminations noting that when customers were terminated, a disconnect order was initiated that triggered removal of logical and physical access. Inspected the disconnect order for randomly selected terminated customers during the examination period noting that when customers were terminated, a disconnect order was initiated that triggered removal of logical and physical access.	No exceptions noted. No exceptions noted.
		Changes to customer access are documented with a service ticket and must be authorized by the Customer's Administrative User.	Inquired of the Director, Network Operations Center about customer access changes noting that changes to customer access were documented with a service ticket and were authorized by the Customer's Administrative User. Inspected service tickets for randomly selected customer access changes during the examination period noting that changes to customer access were authorized by the Customer's Administrative User.	No exceptions noted. No exceptions noted.
		Administrative access to the network is limited to IT and Network Administrator personnel. Administrator access to the badge system is limited to authorized personnel.	Inquired of the Manager, Information Systems about administrative access noting that administrative access to the network was limited to IT and Network Administrator personnel. Also noted that administrator access to the badge system was limited to authorized personnel. Inspected the Active Directory access listing and badge listing noting that administrative access to the network was limited to IT and Network Administrator personnel. Also noted that administrator access to the badge system was limited to authorized personnel.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Everstream sets up the server environment for the customer. A standard virtual local area network (VLAN) is configured for segmentation.	Inquired of the Manager, Information Systems about customer network set up noting that Everstream set up the server environment for customers and provisioned customers with their own VLAN for segmentation.	No exceptions noted.
			Observed the network management interface and firewall management interface console and reports with the Systems Engineer noting that Everstream set up the server environment for customers and provisioned customers with their own VLAN for segmentation.	No exceptions noted.
		Customer systems are configured on virtual machines running on a physical host server. All communications between virtual machines are required to pass through the gateway router first (for public-facing machines).	Inquired of the Manager, Information Systems about customer systems noting that VMware was used for customer virtual machines on physical servers. Also noted that all customer traffic traveled through the gateway router first.	No exceptions noted.
			Inspected the customer systems diagram noting that customer systems were configured on virtual machines running on a physical host server, and that all communications between virtual machines were required to pass through the gateway router first (for public-facing machines).	No exceptions noted.
			Observed the virtual machine management interface, noting that customer systems were configured on virtual machines running on a physical host server, and that all communications between virtual machines were required to pass through the gateway router first (for public-facing machines).	No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Everstream's management network is segmented from the customer colocation network.	Inquired of the Manager, Information Systems about network segmentation noting that Everstream's management network was segmented from the customer colocation network.	No exceptions noted.
			Observed the network management interface and firewall management interface console and reports with the Systems Engineer noting that Everstream's management network was segmented from the customer colocation network.	No exceptions noted.
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	All entrances to the Grand Rapids data center facility remain locked with the exception of the main office entry. A badge reader is positioned at all entrance points into the building and throughout the data center space. The badge reader system at the Grand Rapids data center is configured to trigger an alarm if any of the monitored doors are open for an extended period of time.	Inquired of the Facilities Operations Manager about the Grand Rapids data center noting that all entrances to the facility remained locked with the exception of the main office entry. Noted that a badge reader was positioned at all entrance points into the building and throughout the data center space. Also noted that the badge reader system at the Grand Rapids data center was configured to trigger an alarm if any of the monitored doors were open for an extended period of time.	No exceptions noted.
			Observed all entrances to the Grand Rapids data center facility noting that doors remained locked with the exception of the main entry, and that a badge reader was positioned at all entrance points into the building.	No exceptions noted.
			Inspected the badge reader system configuration setting noting that it was configured to trigger an alarm if any of the monitored doors were held open for an extended period of time.	No exceptions noted.
			Observed an instance for the opening of an internal door for an extended period of time at the Grand Rapids data center noting that an alarm was triggered, and a subsequent call was made if a response was not given.	No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		At the Grand Rapids data center, customer systems are physically protected from tampering, damage, and theft as they sit in single-tenant, dual-door, lockable, and fully sealed server cabinets. The customer is provided a three-digit combination code to unlock their cabinet.	Inquired of the Facilities Operations Manager about physical protection noting that at the Grand Rapids data center, customer systems were physically protected from tampering, damage, and theft as they sat in single-tenant, dual-door, lockable, and fully sealed server cabinets. Also noted that the customer was provided a three-digit combination code to unlock their cabinet. Observed the Grand Rapids data center noting that customer systems were physically protected from tampering, damage, and theft as they sat in single-tenant, dual-door, lockable, and fully sealed server cabinets. Also noted that a three-digit combination code was required to unlock the cabinets.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		At the Grand Rapids data center facility, in order to descend the elevator to the lower data center floor, a configured badge swipe is required. Once a co-located customer is at the basement lower level, they are required to swipe their badge and enter the PIN at the entrance to the customer work area, which sits between the elevator lobby and the data center floor. Co-located customers need to swipe their badge and enter the PIN again at the badge reader at the top of the ramp leading up to the data center floor entrance from the customer work area.	Inquired of the Facilities Operations Manager about the Grand Rapids data center facility noting that in order to descend the elevator to the lower data center floor, a configured badge swipe was required. Noted that once a co-located customer was at the basement lower level, they were required to swipe their badge and enter the PIN at the entrance to the customer work area, which sits between the elevator lobby and the data center floor. Also noted that co-located customers needed to swipe their badge and enter the PIN again at the badge reader at the top of the ramp leading up to the data center floor entrance from the customer work area. Observed the process for entrance into the lower data center floor area noting that: • The customer needed to proceed to the basement level of the building where they were taken to the elevator lobby before the customer work area. • A badge reader was at the entrance to the closed customer work area where customers swiped their badge to unlock the doors. • Once the badge was swiped, a PIN was necessary to gain access. • Customers needed to walk up a short anti-static ramp to swipe their badge at the entrance and enter the PIN to gain access to the data center floor.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Protection from unauthorized access by employees is implemented through the use of various physical security controls such as badge reader systems and surveillance cameras. Employees do not have the ability to access customer servers and equipment, either by console or remote access Virtual Private Network (VPN).	Inquired of the Facilities Operations Manager about unauthorized access noting that protection from unauthorized access by employees was implemented through the use of various physical security controls such as badge reader systems and surveillance cameras. Also noted that employees did not have the ability to access customer servers and equipment, either by console or remote access VPN. Observed the Grand Rapids data center facility noting that protection from unauthorized access by employees was implemented through the use of various physical security controls such as badge reader systems and surveillance cameras. Observed the Sr. Manager, Information Systems attempt to access the customer environment noting that employees did not have the ability to access customer servers and equipment, either by console or remote access VPN.	No exceptions noted. No exceptions noted. No exceptions noted.
		New customers are provided badge access once services are delivered and ready for customer use.	Inquired of the Facilities Operations Manager about new customer access noting that new customers were provided badge access once services were delivered and ready for customer use. Also noted that no new customers required badge access during the examination period.	No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Only authorized customers, Everstream employees, and subcontractors are provided badge-reader-controlled access to the data center.	Inquired of the Facilities Operations Manager about visitor access to the Grand Rapids data center noting that only authorized customers, Everstream employees, and subcontractors were given badge access to the data center. Inspected the data center visitor access policy for the Grand Rapids data center noting that the policy outlined the access controls for the data center. Inspected the badge access list for the Grand Rapids data center noting that only authorized customers, Everstream employees, and subcontractors were provided badge-reader-controlled access to the data center.	No exceptions noted. No exceptions noted. No exceptions noted.
		The NOC continually monitors all badge reader access live on a screen in the NOC work area. The monitor shows the person's name, picture of person, facility, and time.	Inquired of the Director, Network Operations Center about badge access noting that the NOC continually monitored all badge reader access live on a screen in the NOC work area. Also noted that the monitor showed the person's name, picture of person, facility, and time. Observed the NOC noting that a continual video feed on displayed monitors was monitored. Also noted that the monitor displayed the picture of the person, their name, to which facility they gained access, and the time of their activity.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Access to the data center in Grand Rapids is restricted to specific Everstream employees including the IT Data Engineering Team, Field Operations Team, Data Center Sales, CO and Data Center Engineer, NOC, executive staff, and the Data Center Project Manager.	Inquired of the Facilities Operations Manager about employees who had access to the data center in Grand Rapids noting that access to the data center in Grand Rapids was restricted to specific Everstream employees including the IT Data Engineering Team, Field Operations Team, Data Center Sales, CO and Data Center Engineer, NOC, executive staff, and the Data Center Project Manager. Inspected the badge access list for the Grand Rapids data center noting that access to the data center in Grand Rapids was restricted to specific Everstream employees, including the IT Data Engineering Team, Field Operations Team, Data Center Sales, CO and Data Center Engineer, NOC, executive staff, and the Data Center Project Manager.	No exceptions noted. No exceptions noted.
		When customers are terminated, a disconnect order is initiated that triggers removal of logical and physical access.	Inquired of the Director, Network Operations Center about customer terminations noting that when customers were terminated, a disconnect order was initiated that triggered removal of logical and physical access. Inspected the disconnect order for randomly selected terminated customers during the examination period noting that when customers were terminated, a disconnect order was initiated that triggered removal of logical and physical access.	No exceptions noted. No exceptions noted.
		When an employee separates from Everstream, a service ticket is created to ensure network and physical access are disabled.	Inquired of the Human Resources Manager about employee separations noting that Everstream created service tickets to ensure that network and physical access were disabled. Inspected service tickets, Active Directory reports, and badge access reports for randomly selected employee separations during the examination period noting that network and physical access were disabled.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		The Grand Rapids data center is located in the basement of a corporate office complex. Surveillance cameras dot the exterior of the building and are also strategically pointed toward the main office. Surveillance cameras are positioned near doorway entrances throughout the Grand Rapids office area and the data center.	Inquired of the Facilities Operations Manager about the Grand Rapids data center location noting that it was located in a basement of a corporate office complex. Noted that surveillance cameras dotted the exterior of the building to include door areas and other critical areas. Also noted that surveillance cameras were positioned near doorway entrances throughout the Grand Rapids office area and the data center. Observed the surveillance cameras at the Grand Rapids data center noting that several cameras dotted the interior and exterior of the building. Also noted that surveillance cameras were positioned near doorway entrances throughout the Grand Rapids office area and the data center.	No exceptions noted. No exceptions noted.
		There are multiple access levels to restrict access throughout the Grand Rapids facility, including an access level for customers whose access will be limited to just the data center entrances.	Inquired of the Facilities Operations Manager about the access level that was configured for the Grand Rapids facility noting that there was an access level for customers that limited access to just the data center entrances. Inspected the badge reader access list noting that there were several access levels which restricted data center access, and that there was an access level for customers whose access was limited to just the data center entrances.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Physical access to the data center for new employees or changes in position is granted or updated based on authorization documented in a service ticket.	Inquired of the Facilities Operations Manager about physical access to the data center noting that new employees or changes in position were granted or updated based on authorization documented in a service ticket. Also noted that there were no position changes during the examination period that required a change in physical access.	No exceptions noted.
			Inspected service tickets and badge access reports for randomly selected new hires during the examination period noting that physical access to the data center for new employees was granted based on authorization documented in a service ticket.	No exceptions noted.
		Electrical power to each server cabinet is provided via two power-distribution units configured for A/B circuits. Power to the data center floor is ensured with dual redundant 600kVA active flywheel enterprise-class UPS units and two 800kVA diesel generators. For air cooling, three Emerson Liebert 22-ton air conditioning units are configured to all run in either a reduced capacity, or N+1 configuration with the third unit on active standby.	Inquired of the Facilities Operations Manager about redundant environmental controls noting that electrical power to each server cabinet was provided via two power distribution units configured for A/B circuits. Noted that power to the data center floor was ensured with dual redundant 600kVA active flywheel enterprise-class UPS units and two 800kVA diesel generators. Also noted that for air cooling, 3 Emerson Liebert 22-ton air conditioning units were configured to all run in either a reduced capacity, or N+1 configuration with the third unit on active standby.	No exceptions noted.
			Observed redundant environmental controls noting that the data center implemented electrical power to each server cabinet was provided via two power-distribution units configured for A/B circuits.	No exceptions noted.
			Observed the dual, redundant 600kVA UPS units in the data center and the two 800kVA diesel generators noting that the units supplied power to the data center floor.	No exceptions noted.
			Observed air cooling unit noting that for air cooling, three Emerson Liebert 22-ton air conditioning units were configured to all run in either a reduced capacity, or N+1 configuration with the third unit on active standby.	No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	A Data Classification Policy is in place to help ensure that confidential and sensitive data, both for internal data and per HIPAA requirements, is properly secured and restricted to authorized personnel throughout collection, retention, and disposition processes.	Inquired of the VP, Service Delivery about the Data Classification Policy noting that a Data Classification Policy was in place to help ensure that confidential and sensitive data, both for internal data and per HIPAA requirements, was properly secured and restricted to authorized personnel throughout collection, retention, and disposition processes. Inspected the Data Classification Policy noting that a Data Classification Policy was in place to help ensure that confidential and sensitive data, both for internal data and per HIPAA requirements, was properly secured and restricted to authorized personnel throughout collection, retention, and disposition processes.	No exceptions noted. No exceptions noted.
		The Disposal of Media Policy, which covers both internal and HIPAA processes, is documented to provide guidance to internal personnel for the process of hardware disposal.	Inquired of the Manager, Information Systems about the Disposal of Media Policy noting that the Disposal of Media Policy, which covered both internal and HIPAA processes, was documented to provide guidance to internal personnel for the process of hardware disposal. Inspected the Disposal of Media Policy noting that the Disposal of Media Policy, which covered both internal and HIPAA processes, was documented to provide guidance to internal personnel for the process of hardware disposal.	No exceptions noted. No exceptions noted.
		Media is disposed according to the Disposal of Media Policy. A third party vendor provides certificates of destruction per the Disposal of Media policy.	Inquired of the Manager, Information Systems about media disposal noting that media was disposed according to the Disposal of Media Policy. Noted that a third party vendor provided certificates of destruction per the Disposal of Media policy. Also noted that no media was disposed of during the examination period.	No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Everstream sets up the server environment for the customer. A standard virtual local area network (VLAN) is configured for segmentation.	Inquired of the Manager, Information Systems about customer network set up noting that Everstream set up the server environment for customers and provisioned customers with their own VLAN for segmentation. Observed the network management interface and firewall management interface console and reports with the Systems Engineer noting that Everstream set up the server environment for customers and provisioned customers with their own VLAN for segmentation.	No exceptions noted. No exceptions noted.
		Everstream implemented a Ironsphere server, integrated with Active Directory, to allow for more granular access control over Everstream's network devices. This allows authorized individuals to authenticate to the network devices with their domain credentials.	Inquired of the Manager, Information Systems about the Ironsphere server noting that it integrated with Active Directory to allow Everstream more granular access control over network devices and authorized individuals to authenticate to network devices with their domain credentials. Inspected the Ironsphere settings noting that it integrated with Active Directory to allow Everstream more granular access control over network devices and authorized individuals to authenticate to network devices with their domain credentials.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Customer systems are configured on virtual machines running on a physical host server. All communications between virtual machines are required to pass through the gateway router first (for public-facing machines).	Inquired of the Manager, Information Systems about customer systems noting that VMware was used for customer virtual machines on physical servers. Also noted that all customer traffic traveled through the gateway router first.	No exceptions noted.
			Inspected the customer systems diagram noting that customer systems were configured on virtual machines running on a physical host server, and that all communications between virtual machines were required to pass through the gateway router first (for public-facing machines).	No exceptions noted.
			Observed the virtual machine management interface, noting that customer systems were configured on virtual machines running on a physical host server, and that all communications between virtual machines were required to pass through the gateway router first (for public-facing machines).	No exceptions noted.
		Everstream's management network is segmented from the customer colocation network.	Inquired of the Manager, Information Systems about network segmentation noting that Everstream's management network was segmented from the customer colocation network.	No exceptions noted.
			Observed the network management interface and firewall management interface console and reports with the Systems Engineer noting that Everstream's management network was segmented from the customer colocation network.	No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Administrative access to the network is limited to IT and Network Administrator personnel. Administrator access to the badge system is limited to authorized personnel.	Inquired of the Manager, Information Systems about administrative access noting that administrative access to the network was limited to IT and Network Administrator personnel. Also noted that administrator access to the badge system was limited to authorized personnel. Inspected the Active Directory access listing and badge listing noting that administrative access to the network was limited to IT and Network Administrator personnel. Also noted that administrator access to the badge system was limited to authorized personnel.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Anti-virus has been deployed on company machines to protect against security threats.	Inquired of the Manager, Information Systems about anti-virus noting that anti-virus had been deployed on company machines to protect against security threats. Inspected the anti-virus agent status and configuration on a random selection of machines noting that anti-virus was deployed on company machines to protect against security threats.	No exceptions noted. For two out of forty company machines selected, anti-virus software was not deployed. *Management's Response:* Everstream identified systems without antivirus installed via (2) methods. The methods used were Block64 reporting and the Viper antivirus dashboard. Block64 is an application we use to inventory applied software and OS versions. Viper is the anti-virus itself. Any systems found to be out of compliance were pushed anti-virus software. We are configuring Block64 and the Viper dashboard to send us weekly reports on the status of anti-virus installations on our managed devices. These reports generate a yes/no answer as to whether the client is installed, but also go further, giving us status on client version, definition updates, and report AV hits and quarantines. We will view this report weekly and remediate any issues we see.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Firewall logs are maintained in Loggly Logs and retained three months for review as needed.	Inquired of the Manager, Information Systems about firewall logging noting that firewall logs were maintained in Loggly Logs and retained three months for review as needed. Inspected the firewall logging retention configuration and firewall logs noting that firewall logs were maintained in Loggly Logs and retained three months for review as needed.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	A Data Classification Policy is in place to help ensure that confidential and sensitive data, both for internal data and per HIPAA requirements, is properly secured and restricted to authorized personnel throughout collection, retention, and disposition processes.	Inquired of the VP, Service Delivery about the Data Classification Policy noting that a Data Classification Policy was in place to help ensure that confidential and sensitive data, both for internal data and per HIPAA requirements, was properly secured and restricted to authorized personnel throughout collection, retention, and disposition processes. Inspected the Data Classification Policy noting that a Data Classification Policy was in place to help ensure that confidential and sensitive data, both for internal data and per HIPAA requirements, was properly secured and restricted to authorized personnel throughout collection, retention, and disposition processes.	No exceptions noted. No exceptions noted.
		The Disposal of Media Policy, which covers both internal and HIPAA processes, is documented to provide guidance to internal personnel for the process of hardware disposal.	Inquired of the Manager, Information Systems about the Disposal of Media Policy noting that the Disposal of Media Policy, which covered both internal and HIPAA processes, was documented to provide guidance to internal personnel for the process of hardware disposal. Inspected the Disposal of Media Policy noting that the Disposal of Media Policy, which covered both internal and HIPAA processes, was documented to provide guidance to internal personnel for the process of hardware disposal.	No exceptions noted. No exceptions noted.
		Media is disposed according to the Disposal of Media Policy. A third party vendor provides certificates of destruction per the Disposal of Media policy.	Inquired of the Manager, Information Systems about media disposal noting that media was disposed according to the Disposal of Media Policy. Noted that a third party vendor provided certificates of destruction per the Disposal of Media policy. Also noted that no media was disposed of during the examination period.	No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Customer systems are configured on virtual machines running on a physical host server. All communications between virtual machines are required to pass through the gateway router first (for public-facing machines).	Inquired of the Manager, Information Systems about customer systems noting that VMware was used for customer virtual machines on physical servers. Also noted that all customer traffic traveled through the gateway router first.	No exceptions noted.
			Inspected the customer systems diagram noting that customer systems were configured on virtual machines running on a physical host server, and that all communications between virtual machines were required to pass through the gateway router first (for public-facing machines).	No exceptions noted.
			Observed the virtual machine management interface, noting that customer systems were configured on virtual machines running on a physical host server, and that all communications between virtual machines were required to pass through the gateway router first (for public-facing machines).	No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Vulnerability tests on the corporate network are performed weekly by utilizing common vulnerability testing toolkits such as Nessus.	Inquired of the IT Manager about vulnerability testing noting that vulnerability tests were conducted on the corporate network weekly by utilizing common vulnerability testing toolkits such as Nessus. Inspected the Nessus vulnerability scan log for randomly selected weeks during the examination period noting that a scan was conducted on the corporate network on a weekly basis utilizing common vulnerability testing toolkits such as Nessus.	No exceptions noted. No exceptions noted.
		A weekly trouble ticket report is reviewed and evaluated by the Chief Technology Officer, who provides metrics to the executive team during the weekly executive team meeting.	Inquired of the Chief Technology Officer about the weekly executive team meetings noting that a weekly trouble ticket report was reviewed and evaluated by the Chief Technology Officer, who provided metrics to the executive team during the weekly executive team meeting. Inspected executive team meeting minutes for randomly selected weeks during the examination period noting that a weekly trouble ticket report was reviewed and evaluated by the Chief Technology Officer, who provided metrics to the executive team during weekly executive team meetings.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Anti-virus has been deployed on company machines to protect against security threats.	Inquired of the Manager, Information Systems about anti-virus noting that anti-virus had been deployed on company machines to protect against security threats. Inspected the anti-virus agent status and configuration on a random selection of machines noting that anti-virus was deployed on company machines to protect against security threats.	No exceptions noted. For two out of forty company machines selected, anti-virus software was not deployed. *Management's Response:* Everstream identified systems without antivirus installed via (2) methods. The methods used were Block64 reporting and the Viper antivirus dashboard. Block64 is an application we use to inventory applied software and OS versions. Viper is the anti-virus itself. Any systems found to be out of compliance were pushed anti-virus software. We are configuring Block64 and the Viper dashboard to send us weekly reports on the status of anti-virus installations on our managed devices. These reports generate a yes/no answer as to whether the client is installed, but also go further, giving us status on client version, definition updates, and report AV hits and quarantines. We will view this report weekly and remediate any issues we see.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Patches are applied automatically through a centralized management console on a weekly basis. Patches considered to be “zero-day” patches are applied immediately.	Inquired of the Manager, Information Systems about patch management noting that patches were applied automatically through a centralized management console on a weekly basis. Also noted that patches considered “zero-day” patches were applied immediately.	No exceptions noted.
			Inspected patches for randomly selected weeks during the examination period noting that patches were applied automatically though a centralized management console on a weekly basis.	No exceptions noted.
			Inspected the patch management centralized settings noting that patches considered to be “zero-day” patches were applied immediately.	No exceptions noted.

CC 7.0 System Operations				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Configuration and implementation changes for the network are managed through the CAB process.	Inquired of the Director, Network Operations Center about configuration and implementation changes for the network noting that configuration and implementation changes for the network were managed through the CAB process. Inspected change tickets for randomly selected changes during the examination period noting that configuration and implementation changes for the network were managed through the CAB process.	No exceptions noted. No exceptions noted.
		Vulnerability tests on the corporate network are performed weekly by utilizing common vulnerability testing toolkits such as Nessus.	Inquired of the IT Manager about vulnerability testing noting that vulnerability tests were conducted on the corporate network weekly by utilizing common vulnerability testing toolkits such as Nessus. Inspected the Nessus vulnerability scan log for randomly selected weeks during the examination period noting that a scan was conducted on the corporate network on a weekly basis utilizing common vulnerability testing toolkits such as Nessus.	No exceptions noted. No exceptions noted.
		A weekly trouble ticket report is reviewed and evaluated by the Chief Technology Officer, who provides metrics to the executive team during the weekly executive team meeting.	Inquired of the Chief Technology Officer about the weekly executive team meetings noting that a weekly trouble ticket report was reviewed and evaluated by the Chief Technology Officer, who provided metrics to the executive team during the weekly executive team meeting. Inspected executive team meeting minutes for randomly selected weeks during the examination period noting that a weekly trouble ticket report was reviewed and evaluated by the Chief Technology Officer, who provided metrics to the executive team during weekly executive team meetings.	No exceptions noted. No exceptions noted.

CC 7.0 System Operations				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Anti-virus has been deployed on company machines to protect against security threats.	Inquired of the Manager, Information Systems about anti-virus noting that anti-virus had been deployed on company machines to protect against security threats. Inspected the anti-virus agent status and configuration on a random selection of machines noting that anti-virus was deployed on company machines to protect against security threats.	No exceptions noted. For two out of forty company machines selected, anti-virus software was not deployed. *Management's Response:* Everstream identified systems without antivirus installed via (2) methods. The methods used were Block64 reporting and the Viper antivirus dashboard. Block64 is an application we use to inventory applied software and OS versions. Viper is the anti-virus itself. Any systems found to be out of compliance were pushed anti-virus software. We are configuring Block64 and the Viper dashboard to send us weekly reports on the status of anti-virus installations on our managed devices. These reports generate a yes/no answer as to whether the client is installed, but also go further, giving us status on client version, definition updates, and report AV hits and quarantines. We will view this report weekly and remediate any issues we see.

CC 7.0 System Operations				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Vulnerability tests on the corporate network are performed weekly by utilizing common vulnerability testing toolkits such as Nessus.	Inquired of the IT Manager about vulnerability testing noting that vulnerability tests were conducted on the corporate network weekly by utilizing common vulnerability testing toolkits such as Nessus. Inspected the Nessus vulnerability scan log for randomly selected weeks during the examination period noting that a scan was conducted on the corporate network on a weekly basis utilizing common vulnerability testing toolkits such as Nessus.	No exceptions noted. No exceptions noted.
		A weekly trouble ticket report is reviewed and evaluated by the Chief Technology Officer, who provides metrics to the executive team during the weekly executive team meeting.	Inquired of the Chief Technology Officer about the weekly executive team meetings noting that a weekly trouble ticket report was reviewed and evaluated by the Chief Technology Officer, who provided metrics to the executive team during the weekly executive team meeting. Inspected executive team meeting minutes for randomly selected weeks during the examination period noting that a weekly trouble ticket report was reviewed and evaluated by the Chief Technology Officer, who provided metrics to the executive team during weekly executive team meetings.	No exceptions noted. No exceptions noted.
		There are escalation procedures for all types of outages, and the escalation procedures work in conjunction with the change management process to define priority for outages based on severity.	Inquired of the Director, Network Operations Center about escalation procedures noting that there were escalation procedures for all types of outages, and that the escalation procedures worked in conjunction with the change management process to define priority for outages based on severity. Inspected escalation procedures and change management process documentation noting that procedures were in place for all types of outages, and that the escalation procedures worked in conjunction with the change management process to define priority for outages based on severity.	No exceptions noted. No exceptions noted.

CC 7.0 System Operations				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		The ticketing system tracks all customer incidents and internally reported incidents from the time the ticket is opened until it is resolved.	Inquired of the Director, Network Operations Center about the ticketing system noting that the Operations staff utilized a ticketing system to track customer incidents and internally reported incidents from the time the ticket was opened until it was resolved. Inspected the tickets for randomly selected customer and internally reported incidents during the examination period noting that the ticketing system tracked customer incidents and internally reported incidents from the time the ticket was opened until it was resolved.	No exceptions noted. No exceptions noted.
		On any interruption of service, Everstream's NOC activates to monitor the departments required to ensure service is repaired quickly. Support tickets are opened for maintenance and outages. For customer impacting outages, once the interruption has been repaired, a reason for outage (RFO) is completed upon customer request.	Inquired of the Director, Network Operations Center about interruption of service noting that upon any interruption of service, Everstream's NOC activated to monitor the departments required to ensure service was repaired quickly. Noted that support tickets were opened for maintenance and outages. Also noted that once the interruption had been repaired, an RFO was completed upon customer request. Inspected support tickets for randomly selected interruption of service outages during the examination period noting that each ticket documented the status, progress, and if required, an RFO and resolution.	No exceptions noted. No exceptions noted.

CC 7.0 System Operations				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Anti-virus has been deployed on company machines to protect against security threats.	Inquired of the Manager, Information Systems about anti-virus noting that anti-virus had been deployed on company machines to protect against security threats. Inspected the anti-virus agent status and configuration on a random selection of machines noting that anti-virus was deployed on company machines to protect against security threats.	No exceptions noted. For two out of forty company machines selected, anti-virus software was not deployed. *Management's Response:* Everstream identified systems without antivirus installed via (2) methods. The methods used were Block64 reporting and the Viper antivirus dashboard. Block64 is an application we use to inventory applied software and OS versions. Viper is the anti-virus itself. Any systems found to be out of compliance were pushed anti-virus software. We are configuring Block64 and the Viper dashboard to send us weekly reports on the status of anti-virus installations on our managed devices. These reports generate a yes/no answer as to whether the client is installed, but also go further, giving us status on client version, definition updates, and report AV hits and quarantines. We will view this report weekly and remediate any issues we see.

CC 7.0 System Operations				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	There are escalation procedures for all types of outages, and the escalation procedures work in conjunction with the change management process to define priority for outages based on severity.	Inquired of the Director, Network Operations Center about escalation procedures noting that there were escalation procedures for all types of outages, and that the escalation procedures worked in conjunction with the change management process to define priority for outages based on severity. Inspected escalation procedures and change management process documentation noting that procedures were in place for all types of outages, and that the escalation procedures worked in conjunction with the change management process to define priority for outages based on severity.	No exceptions noted. No exceptions noted.
		The ticketing system tracks all customer incidents and internally reported incidents from the time the ticket is opened until it is resolved.	Inquired of the Director, Network Operations Center about the ticketing system noting that the Operations staff utilized a ticketing system to track customer incidents and internally reported incidents from the time the ticket was opened until it was resolved. Inspected the tickets for randomly selected customer and internally reported incidents during the examination period noting that the ticketing system tracked customer incidents and internally reported incidents from the time the ticket was opened until it was resolved.	No exceptions noted. No exceptions noted.

CC 7.0 System Operations				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		On any interruption of service, Everstream's NOC activates to monitor the departments required to ensure service is repaired quickly. Support tickets are opened for maintenance and outages. For customer impacting outages, once the interruption has been repaired, a reason for outage (RFO) is completed upon customer request.	Inquired of the Director, Network Operations Center about interruption of service noting that upon any interruption of service, Everstream's NOC activated to monitor the departments required to ensure service was repaired quickly. Noted that support tickets were opened for maintenance and outages. Also noted that once the interruption had been repaired, an RFO was completed upon customer request. Inspected support tickets for randomly selected interruption of service outages during the examination period noting that each ticket documented the status, progress, and if required, an RFO and resolution.	No exceptions noted. No exceptions noted.
CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	There are escalation procedures for all types of outages, and the escalation procedures work in conjunction with the change management process to define priority for outages based on severity.	Inquired of the Director, Network Operations Center about escalation procedures noting that there were escalation procedures for all types of outages, and that the escalation procedures worked in conjunction with the change management process to define priority for outages based on severity. Inspected escalation procedures and change management process documentation noting that procedures were in place for all types of outages, and that the escalation procedures worked in conjunction with the change management process to define priority for outages based on severity.	No exceptions noted. No exceptions noted.

CC 7.0 System Operations				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Everstream has customer support contact information on their website which includes a service support guide and Network Operations Center (NOC) escalation list that is available to internal and external users.	Inquired of the Director, Network Operations Center about customer support noting that Everstream had customer support contact information on their website which included a service support guide and NOC escalation list that was available to internal and external users. Inspected customer support information on the Company website noting that Everstream had customer support contact information on their website which included a service support guide and NOC escalation list that was available to internal and external users.	No exceptions noted. No exceptions noted.
		The ticketing system tracks all customer incidents and internally reported incidents from the time the ticket is opened until it is resolved.	Inquired of the Director, Network Operations Center about the ticketing system noting that the Operations staff utilized a ticketing system to track customer incidents and internally reported incidents from the time the ticket was opened until it was resolved. Inspected the tickets for randomly selected customer and internally reported incidents during the examination period noting that the ticketing system tracked customer incidents and internally reported incidents from the time the ticket was opened until it was resolved.	No exceptions noted. No exceptions noted.
		On any interruption of service, Everstream's NOC activates to monitor the departments required to ensure service is repaired quickly. Support tickets are opened for maintenance and outages. For customer impacting outages, once the interruption has been repaired, a reason for outage (RFO) is completed upon customer request.	Inquired of the Director, Network Operations Center about interruption of service noting that upon any interruption of service, Everstream's NOC activated to monitor the departments required to ensure service was repaired quickly. Noted that support tickets were opened for maintenance and outages. Also noted that once the interruption had been repaired, an RFO was completed upon customer request. Inspected support tickets for randomly selected interruption of service outages during the examination period noting that each ticket documented the status, progress, and if required, an RFO and resolution.	No exceptions noted. No exceptions noted.

CC 7.0 System Operations				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	There are escalation procedures for all types of outages, and the escalation procedures work in conjunction with the change management process to define priority for outages based on severity.	Inquired of the Director, Network Operations Center about escalation procedures noting that there were escalation procedures for all types of outages, and that the escalation procedures worked in conjunction with the change management process to define priority for outages based on severity. Inspected escalation procedures and change management process documentation noting that procedures were in place for all types of outages, and that the escalation procedures worked in conjunction with the change management process to define priority for outages based on severity.	No exceptions noted. No exceptions noted.
		Everstream has customer support contact information on their website which includes a service support guide and Network Operations Center (NOC) escalation list that is available to internal and external users.	Inquired of the Director, Network Operations Center about customer support noting that Everstream had customer support contact information on their website which included a service support guide and NOC escalation list that was available to internal and external users. Inspected customer support information on the Company website noting that Everstream had customer support contact information on their website which included a service support guide and NOC escalation list that was available to internal and external users.	No exceptions noted. No exceptions noted.
		The ticketing system tracks all customer incidents and internally reported incidents from the time the ticket is opened until it is resolved.	Inquired of the Director, Network Operations Center about the ticketing system noting that the Operations staff utilized a ticketing system to track customer incidents and internally reported incidents from the time the ticket was opened until it was resolved. Inspected the tickets for randomly selected customer and internally reported incidents during the examination period noting that the ticketing system tracked customer incidents and internally reported incidents from the time the ticket was opened until it was resolved.	No exceptions noted. No exceptions noted.

CC 7.0 System Operations				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		On any interruption of service, Everstream's NOC activates to monitor the departments required to ensure service is repaired quickly. Support tickets are opened for maintenance and outages. For customer impacting outages, once the interruption has been repaired, a reason for outage (RFO) is completed upon customer request.	Inquired of the Director, Network Operations Center about interruption of service noting that upon any interruption of service, Everstream's NOC activated to monitor the departments required to ensure service was repaired quickly. Noted that support tickets were opened for maintenance and outages. Also noted that once the interruption had been repaired, an RFO was completed upon customer request. Inspected support tickets for randomly selected interruption of service outages during the examination period noting that each ticket documented the status, progress, and if required, an RFO and resolution.	No exceptions noted. No exceptions noted.
		The disaster recovery plan is tested on an annual basis.	Inquired of the Chief Technology Officer about disaster recovery noting that the disaster recovery plan was tested on an annual basis. Inspected the disaster recovery plan noting that the section titled "Disaster Recovery Plan Exercising" described the purpose of regular testing and rehearsal. Inspected the disaster recovery testing documentation noting that the disaster recovery plan was tested on an annual basis.	No exceptions noted. No exceptions noted. No exceptions noted.

CC 8.0 Change Management				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Everstream has a written change management policy to guide the change management process.	Inquired of the Director, Network Operations Center about the change management policy and process noting that Everstream had a written change management policy to guide the change management process. Inspected the change management policy noting that Everstream had a written change management policy to guide the change management process.	No exceptions noted. No exceptions noted.
		All changes are documented in the ticketing system and include details of the change, what systems are affected, rollback procedures, and expected impacts.	Inquired of the Chief Technology Officer and the Director, Network Operations Center about the documentation of change details within the ticketing system noting that all changes were documented in the ticketing system and included details of the change, what systems were affected, rollback procedures, and expected impacts. Inspected change tickets for randomly selected changes during the examination period noting that changes were documented in the ticketing system and included details of the change, what systems were affected, rollback procedures, and expected impacts.	No exceptions noted. No exceptions noted.
		Data center changes are reviewed and approved by the Change Advisory Board (CAB). Changes that affect customers are communicated to internal and external users.	Inquired of the Chief Technology Officer and the Director, Network Operations Center about the review and approval of data center changes noting that data center changes were reviewed and approved by the CAB. Also noted that changes that affect customers, were communicated to internal and external users. Inspected change tickets for randomly selected changes during the examination period noting that data center changes were reviewed and approved by the CAB. Also noted that changes that affected customers, were communicated to internal and external users.	No exceptions noted. No exceptions noted.

CC 8.0 Change Management				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Administrative access to the network is limited to IT and Network Administrator personnel. Administrator access to the badge system is limited to authorized personnel.	Inquired of the Manager, Information Systems about administrative access noting that administrative access to the network was limited to IT and Network Administrator personnel. Also noted that administrator access to the badge system was limited to authorized personnel. Inspected the Active Directory access listing and badge listing noting that administrative access to the network was limited to IT and Network Administrator personnel. Also noted that administrator access to the badge system was limited to authorized personnel.	No exceptions noted. No exceptions noted.

CC 9.0 Risk Mitigation				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from business disruption.	The disaster recovery plan is tested on an annual basis.	Inquired of the Chief Technology Officer about disaster recovery noting that the disaster recovery plan was tested on an annual basis.	No exceptions noted.
			Inspected the disaster recovery plan noting that the section titled “Disaster Recovery Plan Exercising” described the purpose of regular testing and rehearsal.	No exceptions noted.
			Inspected the disaster recovery testing documentation noting that the disaster recovery plan was tested on an annual basis.	No exceptions noted.
		Redundancy is built into customer requirements. RAID 1 (disk mirroring) is utilized as a minimum level of redundancy for disk storage. Dual power supplies and network interface cards (NICs) are installed as needed depending on customer requests and agreed-upon service level agreements.	Inquired of the Facilities Operations Manager and Manager, Information Systems about redundancy noting that the level of redundancy built into systems depended on customer requirements and that at a minimum RAID 1 was used for disk storage. Also noted that dual power supplies and NICs were installed as needed depending on customer requests and agreed-upon service level agreements and that systems critical to the infrastructure had dual power supplies and NICs.	No exceptions noted.
			Inspected the data center disk array monitoring tool noting that all disk arrays were configured for RAID 1 (disk mirroring) and were utilized as a minimum level of redundancy for disk storage.	No exceptions noted.
			Inspected the controller management interface noting that dual power supplies and NICs were installed on critical infrastructure systems.	No exceptions noted.

CC 9.0 Risk Mitigation				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Everstream carries limited liability insurance for its office space and data center.	Inquired of the VP, Service Delivery about the limited liability insurance noting that Everstream carried limited liability insurance for its office space and data center. Inspected the limited liability insurance noting that Everstream carried limited liability insurance for its office space and data center.	No exceptions noted. No exceptions noted.
CC 9.2	The entity assesses and manages risks associated with vendors and business partners.	All vendors are required to sign a Business Associate Agreement (BAA) and/or Non-Disclosure Agreement (NDA) at the time of onboarding. Privacy and security commitments are defined within the BAA and/or NDA.	Inquired of the IT Manager about vendors noting that all vendors were required to sign a BAA and/or NDA, at the time of onboarding. Noted that privacy and security commitments were defined within the BAA and/or NDA. Also noted that no vendors that had access to the data center were onboarded during the examination period.	No exceptions noted.
		Everstream conducts an annual risk assessment to (1) identify potential threats that would impair system security and availability commitments and requirements, (2) analyze the significance of risks associated with the identified threats, and (3) determine mitigation strategies for those risks.	Inquired of the Chief Technology Officer about the risk assessment process noting that Everstream conducted an annual risk assessment to (1) identify potential threats that could impair system security and availability commitments and requirements, (2) analyze the significance of risks associated with the identified threats, and (3) determine mitigation strategies for those risks. Inspected the Risk Assessment Report and Risk Mitigation Process noting that Everstream conducted an annual risk assessment to (1) identify potential threats that would impair system security and availability commitments and requirements, (2) analyze the significance of risks associated with the identified threats, and (3) determine mitigation strategies for those risks.	No exceptions noted. No exceptions noted.

A.0 Additional Criteria for Availability				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
A 1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Network and cloud monitoring is performed and logged in historical charts. The charts show performance metrics tracked over a set time period. These metrics include packets per second, packet loss, and downtime.	Inquired of the IT Manager about monitoring noting that network and cloud monitoring was performed and logged in historical charts. Noted that the charts showed performance metrics tracked over a set time period. Also noted that these metrics included packets per second, packet loss, and downtime. Inspected network monitoring historical charts for the examination period noting that network and cloud monitoring was performed and logged in historical charts. Noted that the charts showed performance metrics tracked over a set time period. Also noted that these metrics included packets per second, packet loss, and downtime.	No exceptions noted. No exceptions noted.
		Capacity planning is assessed weekly by the CTO based on reports gathered from monitoring data on compute capacity, and a report provided by the storage vendor.	Inquired of the Chief Technology Officer about capacity planning noting that capacity planning was assessed weekly by the CTO based on reports gathered from monitoring data on compute capacity, and a report provided by the storage vendor. Inspected the CTO's summary engineering and network operations reports for randomly selected weeks during the examination period noting that capacity planning was assessed monthly by the CTO based on weekly reports gathered from monitoring data on compute capacity, and a monthly report provided by the storage vendor.	No exceptions noted. No exceptions noted.

A.0 Additional Criteria for Availability				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Network performance is monitored based on preconfigured thresholds. NOC staff is alerted if thresholds are exceeded. Alerts can be in the form of email, visual alerts on the NOC monitors, or both.	Inquired of the Director, Network Operations Center about network performance monitoring noting that network performance was monitored based on preconfigured thresholds. Noted that NOC staff was alerted if thresholds were exceeded. Also noted that alerts could be in the form of email, visual alerts on the NOC monitors, or both.	No exceptions noted.
			Inspected the monitoring configuration, alert configuration, and sample alerts noting that network performance was monitored based on preconfigured thresholds. Noted that NOC staff was alerted if thresholds were exceeded. Also noted that alerts could be in the form of email, visual alerts on the NOC monitors, or both.	No exceptions noted.
		On any interruption of service, Everstream's NOC activates to monitor the departments required to ensure service is repaired quickly. Support tickets are opened for maintenance and outages. For customer impacting outages, once the interruption has been repaired, a reason for outage (RFO) is completed upon customer request.	Inquired of the Director, Network Operations Center about interruption of service noting that upon any interruption of service, Everstream's NOC activated to monitor the departments required to ensure service was repaired quickly. Noted that support tickets were opened for maintenance and outages. Also noted that once the interruption had been repaired, an RFO was completed upon customer request.	No exceptions noted.
			Inspected support tickets for randomly selected interruption of service outages during the examination period noting that each ticket documented the status, progress, and if required, an RFO and resolution.	No exceptions noted.

A.0 Additional Criteria for Availability				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
A 1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	At the data center, each server cabinet's environmental health is monitored through temperature and humidity sensors that provide data via simple network management protocol (SNMP).	Inquired of the Facilities Operations Manager about environmental health noting that each server cabinet's environmental health was monitored through temperature and humidity sensors that provided data via SNMP. Observed data center cabinets with the Facilities Operations Manager that temperature and humidity sensors were present in each server cabinet. Inspected the environmental health monitoring program with the Facilities Operations Manager noting that temperature and humidity for the server racks were monitored via SNMP.	No exceptions noted. No exceptions noted. No exceptions noted.
		Fire suppression at the data center comes from an FM200 system that is supplemented by a very early smoke detection apparatus (VESDA) system. In addition, multiple ceiling-mounted smoke detectors dot the ceiling of the data center. Handheld fire extinguishers are also available in the data center.	Inquired of the Facilities Operations Manager about fire suppression in the data center noting that fire suppression at the Grand Rapids data center came from an FM200 system that was supplemented by a VESDA system. Also noted that multiple ceiling mounted smoke detectors dotted the ceiling of the data center, and handheld fire extinguishers were available in the data center. Observed the fire suppression system at the Grand Rapids data center noting that fire suppression came from an FM200 system that was supplemented by a VESDA system. Also noted that multiple ceiling mounted smoke detectors and handheld fire extinguishers were in place.	No exceptions noted. No exceptions noted.

A.0 Additional Criteria for Availability				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Generator preventative maintenance occurs on a semiannual basis (every six months), with one of the visits involving a full load test.	Inquired of the Facilities Operations Manager about generator preventative maintenance noting that maintenance occurred every six months. Also noted that one of the two maintenance visits included a full load test of the generators.	No exceptions noted.
			Inspected the vendor documentation of generator maintenance visits for the Grand Rapids data center during the examination period noting that maintenance was performed twice during the examination period, and at least one visit included a full load test.	No exceptions noted.
		Air conditioning units and the fire suppression system undergo a semiannual preventative maintenance check, and the UPS system was maintained on a four-year cyclical basis.	Inquired of the Facilities Operations Manager about the schedule of preventive maintenance noting that air conditioning units and the fire suppression system at the data center underwent semiannual preventative maintenance checks. Also noted that the UPS system was maintained on a four-year cyclical basis.	No exceptions noted.
			Inspected HVAC maintenance receipts for one of the semiannual occurrences during the examination period of the Grand Rapids data center noting that the air conditioning units received preventative maintenance on a semiannual basis.	No exceptions noted.
			Inspected maintenance receipts for one of the semiannual occurrences during the examination period of the Grand Rapids data center noting that fire suppression systems receive preventative maintenance on a semiannual basis.	No exceptions noted.
			Inspected the maintenance receipt for the UPS at the data center noting that the four-year cycle of preventative maintenance had been performed.	No exceptions noted.

A.0	Additional Criteria for Availability			
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		Dual, redundant 600kVA active flywheel Uninterruptible Power Supply (UPS) units provide backup power to the data center floor in the event of a sudden outage. There are two diesel 800kw generators secured in a bunker area that take the single electrical power feed from the local utility to power the data center floor. To ensure that the generators can start up with no issues, an Active Power GenStart unit provides A/C power from the enterprise class UPS for initial startup. Air cooling is handled by three 22-ton air conditioning units that run simultaneously in the data center.	Inquired of the Facilities Operations Manager about environmental controls noting that the data center was equipped with dual, redundant 600kVA active flywheel UPS units to provide backup power to the data center floor in the event of a sudden outage. Noted that there were two diesel 800kw generators secured in a bunker area that took the single electrical power feed from the local utility to power the data center floor. Noted that to ensure that the generators could start up with no issues, an Active Power GenStart unit provided A/C power from the enterprise class UPS for initial startup. Also noted that air cooling was handled by three 22-ton air conditioning units that ran simultaneously in the data center. Observed the dual, redundant 600kVA active flywheel UPS units that provide backup power to the data center floor in the event of a sudden outage. Noted that there were two diesel 800kw generators secured in a bunker area that took the single electrical power feed from the local utility to power the data center floor. Noted that to ensure the generators could start up with no issues, an Active Power GenStart unit provided A/C power from the enterprise class UPS for initial startup. Also noted that air cooling was handled by three 22-ton air conditioning units that ran simultaneously in the data center.	No exceptions noted. No exceptions noted.

A.0 Additional Criteria for Availability				
	Trust Services Criteria Related to Security and Availability	**Controls Specified by Everstream Solutions, LLC**	**Tests Performed by Moss Adams LLP**	**Test Results**
		The use of Storage Area Networks (SANs) greatly reduces failure to a critical component of servers, the data storage. A SAN presents shared pools of storage devices to multiple servers. Each server can access the storage as if it were directly attached to that server. A SAN supports centralized storage management and path redundancy to that storage. SANs make it possible to move data between various storage devices, share data between multiple servers, and backup and restore data rapidly and efficiently. In addition, Everstream configured SAN facilitates both disaster recovery and high availability. Dual power supplies and network interface cards (NICs) are installed as needed depending on customer requests and agreed-upon service level agreements.	Inquired of the Facilities Operations Manager and Manager, Information Systems about redundancy noting that the level of redundancy built into systems depended on customer requirements and that at a minimum RAID 1 was used for disk storage. Also noted that dual power supplies and NICs were installed as needed depending on customer requests and agreed-upon service level agreements and that systems critical to the infrastructure had dual power supplies and NICs. Inspected the data center disk array monitoring tool noting that all disk arrays were configured for RAID 1 (disk mirroring) and were utilized as a minimum level of redundancy for disk storage. Inspected the controller management interface noting that dual power supplies and NICs were installed on critical infrastructure systems.	No exceptions noted. No exceptions noted. No exceptions noted.
A 1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	The disaster recovery plan is tested on an annual basis.	Inquired of the Chief Technology Officer about disaster recovery noting that the disaster recovery plan was tested on an annual basis. Inspected the disaster recovery plan noting that the section titled “Disaster Recovery Plan Exercising” described the purpose of regular testing and rehearsal. Inspected the disaster recovery testing documentation noting that the disaster recovery plan was tested on an annual basis.	No exceptions noted. No exceptions noted. No exceptions noted.

MOSSADAMS