*Proprietary & Confidential*

everstream™

FASTER FIBER. BETTER BUSINESS.

# Grand Rapids Data Center System

**SOC 1**

Report on Management's Description
of a Service Organization's System and the Suitability
of the Design and Operating Effectiveness of Controls


JUNE 1, 2020 THROUGH 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 description of its Grand Rapids Data Center System entitled "Description of Everstream Solutions, LLC's Grand Rapids Data Center System" for processing user entities' transactions throughout the period June 1, 2020 to May 31, 2021 (description) and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Everstream Solutions, LLC's Assertion" (assertion). The controls and control objectives included in the description are those that management of Everstream Solutions, LLC believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Grand Rapids Data Center System that are not likely to be relevant to user entities' internal control over financial reporting.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Everstream Solutions, LLC's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

## Service Organization's Responsibilities

In Section II, Everstream Solutions, LLC has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Everstream Solutions, LLC is responsible for preparing the description and its assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

## Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives 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 the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period June 1, 2020 to May 31, 2021. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

## Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

## Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section IV.

## Opinion

In our opinion, in all material respects, based on the criteria described in Everstream Solutions, LLC's assertion:

- the description fairly presents the Grand Rapids Data Center System that was designed and implemented throughout the period June 1, 2020 to May 31, 2021.
- the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period June 1, 2020 to May 31, 2021, and the user entities applied the complementary controls assumed in the design of Everstream Solutions, LLC's controls throughout the period June 1, 2020 to May 31, 2021.
- the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period June 1, 2020 to May 31, 2021, if complementary user entity controls assumed in the design of Everstream Solutions, LLC's controls operated effectively throughout the period June 1, 2020 to May 31, 2021.

## 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, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. 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 description of Everstream Solutions, LLC's Grand Rapids Data Center System entitled "Description of Everstream Solutions, LLC's Grand Rapids Data Center System" for processing user entities' transactions throughout the period June 1, 2020 to May 31, 2021 (description) for user entities of the system during some or all of the period June 1, 2020 to May 31, 2021, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, when assessing the risks of material misstatements of user entities' financial statements.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Everstream Solutions, LLC's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

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

a. The description fairly presents the Grand Rapids Data Center System made available to user entities of the system during some or all of the period June 1, 2020 to May 31, 2021 for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description

   *i.* presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including, if applicable,

      (1) the types of services provided, including, as appropriate, the classes of transactions processed.

      (2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.

      (3) the information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

      (4) how the system captures and addresses significant events and conditions other than transactions.

(5) the process used to prepare reports and other information for user entities.

(6) the specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls assumed in the design of the service organization's controls.

(7) other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

*ii.* includes relevant details of changes to the service organization's system during the period covered by the description.

*iii.* does not omit or distort information relevant to the service organization's system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and the user auditors, and may not, therefore, include every aspect of the Grand Rapids Data Center System that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period June 1, 2020 to May 31, 2021 to achieve those control objectives if user entities applied the complementary controls assumed in the design of Everstream Solutions, LLC's controls throughout the period June 1, 2020 to May 31, 2021. The criteria we used in making this assertion were that

*i.* the risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization.

*ii.* the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

*iii.* the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

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

## A. Overview of Everstream Solutions, LLC

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. Scope of the Description

This description of Everstream Solutions, LLC's Grand Rapids Data Center System addresses only Everstream Solutions, LLC's Grand Rapids Data Center System provided to its user entities and excludes other services provided by Everstream Solutions, LLC. The description is intended to provide information for user entities of the Grand Rapids Data Center System and their independent auditors who audit and report on such user entities' financial statements to be used in obtaining an understanding of the Grand Rapids Data Center System and the controls over that system that are likely to be relevant to user entities' internal control over financial reporting. The description of the system includes certain business process controls and IT general controls that support the delivery of Everstream Solutions, LLC's Grand Rapids Data Center System.

## C. Internal Control Framework

This section provides information about the five interrelated components of internal control at Everstream Solutions, LLC, including Everstream Solutions, LLC's:

- Control Environment
- Risk Assessment Process
- Monitoring Activities
- Information and Communications
- Control Activities

## 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.

## 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. Monitoring Activities

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.

## 4. Information and Communications

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.

# 5. Control Activities

## *a) Organization and Management*

Control Objective – Controls provide reasonable assurance that Everstream Solutions, LLC has an organizational structure, with established policies and procedures for onboarding, training, and monitoring performance.

### SEGREGATION OF DUTIES

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. 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 responsibility and accountability for the security and availability of the data center system is assigned to the Chief Technology Officer (CTO). The corporate organizational chart is maintained by the Manager, Office Administration and is available for viewing on the Company's shared drive.

### JOB DESCRIPTIONS

Job descriptions are available for each position that define roles and responsibilities and can be found on the Company's share drive in the compliance folder.

### 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.

### PERSONNEL SECURITY CLEARANCE

The offer letter and employment application state that hiring of the candidate is contingent upon receipt of a satisfactory background check. Background checks are required for all new employees. Candidates sign a consent form agreeing to a background check.

The Company uses a third-party background check service provider. The third-party service provider checks criminal history and Social Security Number.

The Company obtains a resume and employment application that have the employee's qualifications, work history, education, and references. Everstream also verifies qualifications, work history, education, and references, and searches social media websites.

### ORIENTATION AND TRAINING

On a new employee's first day on the job, the new employee attends a HR Orientation and is provided a tour of the facility, employee benefits package, and the employee handbook. Upon hire, employees acknowledge receipt of the employee handbook which covers security and confidentiality of information, and workforce conduct standards. After the initial orientation and manuals are read and signed off by the new employee, the employee's direct manager provides on-the-job training with the employee observing standard operating procedures and overall operations.

To supplement ongoing educational efforts, internal customer wikis have been developed that contain customer contact information, specific procedures, system narratives, examples, and script language. These wikis are located on Everstream's intranet site.

### CONTRACTORS

At times, Everstream uses contractors for the performance of work. New Contractors must sign a non-disclosure agreement before beginning work.

### 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.

### POLICY DIRECTIVES

Company policies are communicated in the Director meetings, employee handbooks, management emails, DocuSign, and electronic memos.

In addition, the Organization Policy states all policy, new or modified, must be approved by an executive officer or his or her designee.

## *b) Communications*

| Control Objective – Controls provide reasonable assurance that Everstream Solutions, LLC has an organizational structure, with established policies and procedures for onboarding, training, and monitoring performance. |
|---|

Good communications within Everstream to employees and contractors (internal users) is important, as well as communications with customer (external users). Internal and external users are provided information about the system and its boundaries on the public website.

When a new customer is onboarded, each new customer is provided a master services agreement and product specific service agreement to define commitments.

If a customer has any issues, 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.

In addition, maintenance notifications, including system changes that affect customers, are communicated to internal and external users 7-10 days in advance for routine maintenance changes. Emergency change notifications are communicated as necessary.

### SUPPORT

Customer support requests are received via email to Everstream's support email address or phone call to the NOC Technical staff. These support requests are tracked, recorded, and maintained in a ticketing system utilized by all operations staff. The ticketing system tracks all customer incidents and internally reported incidents from the time the ticket is opened until it is resolved.

The ticket is opened by and assigned to the first NOC staff who responds to the support request. The NOC staff is responsible for performing initial troubleshooting and escalating the issue if needed. When the issue is resolved, the NOC staff is responsible for closing the ticket so that response times and mean time to repair can be derived from the ticket.

Escalation procedures are determined based on the issue and service that is affected and the network component (router or firewall) that is impacted. NOC staff follows an escalation procedure that includes five levels that may involve technical specialists. 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. Multiple outages are automatically escalated to second and third level support.

### *c) Risk Management*

| |
|---|
| Control Objective – Controls provide reasonable assurance that Everstream Solutions, LLC identifies potential threats that could impair system security and availability commitments and system requirements, analyzes the significance of risks associated with the identified threats, and determines mitigation strategies for those risks. |

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.

### *d) Monitoring Controls*

| |
|---|
| Control Objective – Controls provide reasonable assurance that the design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and availability. |

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.

Patches are applied automatically through a centralized management console on a weekly basis. Patches considered to be "zero-day" patches are applied immediately.

Firewall logs are maintained in Loggly Logs and retained three months for review as needed.

Everstream has deployed a Security Information and Event Management system (SIEM) which is a tool that provides real-time analysis of security events generated by office network and server hardware and applications.

Vulnerability tests on the corporate network are performed weekly by utilizing common vulnerability testing toolkits such as Nessus. As a supplemental service, if the Company is notified of a zero-day attack, a vulnerability assessment scan is performed against customer systems to check for the existence of the exploitable vulnerability. If found, Everstream notifies the customer of the weakness.

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.

Anti-virus has been deployed on company machines to protect against security threats.

## *e) Logical and Physical Controls*

Control Objective – Controls provide reasonable assurance that access to Grand Rapids data center is limited to personnel authorized by management and controls provide reasonable assurance that access to data is restricted to appropriate personnel.

### 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 with cameras strategically located outside pointing to 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 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 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.

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.

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.

### 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.

### EMPLOYEE SECURITY CLEARANCE

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. There are multiple security zones to restrict access throughout the facility. The Grand Rapids data center adds a third security zone for customers whose access will be limited to just the data center entrances.

### VISITOR MANAGEMENT

Everstream has implemented a sign-in iPad Visitor Management System for entry into the office. Also, each visitor wears a picture badge. Each visitor must sign in upon entering the building and sign out upon leaving.

### SECURITY ADMINISTRATION

Logical security of the data center is the shared responsibility of the Compliance and HR Director, the Director of Technology and Systems, the Director of IT & NOC, the CO and Data Center Engineer, and the NOC Manager. Procedures around security administration are detailed in the Everstream Security Policy and the Access Control Policy, which describe staff responsibilities and security protocol around site entry, remote registration for Point of Presence (POP) sites, site exiting, trespassing, and physical security.

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. 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

Administrative access is limited to authorized IT and Network Administrator personnel.

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.

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

### 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.

## PROTECTION OF CUSTOMER DATA

Everstream's Order Management Team facilitates communication and setup from the customer order request to the completion of system implementation. 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. The initial password is randomly generated and consists of eight characters in a combination of upper and lowercase letters and special characters. In addition, new customers are provided badge access once services are delivered and ready for customer use.

Responsibility for system security for colocation customers is the responsibility of the customer. Everstream sets up the server environment for the customer. A standard virtual local area network (VLAN) is configured for segmentation.

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). Each virtual machine is assigned a unique IP address and distinct MAC address. The MAC address is tied to the physical host server.

Everstream's management network is segmented from the customer colocation network.

Changes to customer access are documented with a service ticket and must be authorized by the Customer's Administrative User.

When customers are terminated, a disconnect order is initiated that triggers removal of logical and physical access. A data wipe is performed on the server using a US Department of Defense-approved disk wiping utility before the machine is repurposed. For hard disks that are retired, Everstream uses a third-party shredding service to physically destroy the disk drive. A certification of destruction is provided to Everstream as proof of the hard disk destruction.

### PROTECTION FROM EMPLOYEES

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).

## *f) System Operations*

Control Objective – Controls provide reasonable assurance that key systems are monitored and supported through a defined support process.

The ticketing system tracks all customer incidents and internally reported incidents from the time the ticket is opened until it is resolved. 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. 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.

### SECURITY MEASURES

Network security is an element of the Operations Team's monitoring activities.

## *g) Change Management*

Control Objective – Controls provide reasonable assurance that changes to the Grand Rapids data center are executed according to established policies and procedures.

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 Change Advisory Board (CAB). Changes that affect customers are communicated to internal and external users.

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 for the network are managed through the CAB process.

## *h) Availability*

Control Objective – Controls provide reasonable assurance that procedures exist to permit the continuance of business operations in the event the operations are disabled, including backup and recovery.

### 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 both front and back 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.

### CAPACITY PLANNING

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. During this meeting, future network rollout plans, capacity, and scheduled maintenance tasks are discussed. Minutes of the meeting are maintained to report on capacity.

Network performance is logged in historical charts. The charts show performance metrics tracked over a set time period. These metrics include packets per second, bits per second, router memory utilization, process utilization, power utilization, and temperature. The charts are created whenever a new router is deployed or when a circuit is turned up.

In addition, capacity planning analysis is augmented with netflow information such as packet source and destination that is maintained to determine next peering targets.

## 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, bits per second, router memory utilization, process utilization, power utilization, and temperature.

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 was 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. Everstream provides client backup services to virtual private server (VPS) customers where Everstream has the responsibility to house the customer's data on a shared system. The VPS server environment is backed up based on customer specifications.

### RESTORATION

On any interruption of service, Everstream's NOC goes into action to monitor the departments required to ensure service is repaired quickly. Support tickets are opened for maintenance and outages. For outages, once the interruption has been repaired, a RFO (reason for outage) is completed.

### RECOVERY TESTING

The disaster recovery plan is tested on an annual basis.

## D. Control Objectives and Related Controls

Everstream Solutions, LLC has specified the control objectives and identified the controls that are designed to achieve the related control objective. The specified control objectives and related controls are presented in Section IV, "Description of Everstream Solutions, LLC's Control Objectives and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results," and are an integral component of Everstream Solutions, LLC's Grand Rapids Data Center System.

## E. Complementary User Entity Controls

Everstream Solutions, LLC's controls related to the Grand Rapids Data Center System cover only a portion of overall internal control for each user entity of Everstream Solutions, LLC. It is not feasible for the control objectives related to the Grand Rapids Data Center System to be achieved solely by Everstream Solutions, LLC. Therefore, each user entity's internal control over financial reporting should be evaluated in conjunction with Everstream Solutions, LLC's controls and the related tests and results described in Section IV of this report, taking into account the related complementary user entity controls identified below, where applicable.

In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control to determine whether the identified complementary user entity controls have been implemented and are operating effectively.

| | Complementary User Entity Controls | Related Control Objective |
|---|---|---|
| 1 | Alerting Everstream about any regulatory changes within their industry that might affect their services. | **Control Objective 2:** Communications |
| 2 | Adhering to the terms and conditions stated within their contracts with Everstream. | **Control Objective 2:** Communications |

| | Complementary User Entity Controls | Related Control Objective |
|---|---|---|
| 3 | Reporting to Everstream in a timely manner any material changes to their overall control environment that may adversely affect services being performed by Everstream. | **Control Objective 2:** Communications |
| 4 | Implementing sound and consistent internal controls regarding general IT system access, and system usage appropriateness for all internal user entity components associated with Everstream. | **Control Objective 5:** Logical and Physical Controls |
| 5 | Updating the initial password provided by Everstream upon login. | **Control Objective 5:** Logical and Physical Controls |
| 6 | 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. | **Control Objective 5:** Logical and Physical Controls |
| 7 | Ensuring transactions for user entities relating to Everstream's data center products and services are appropriately authorized, and transactions are secure, timely, and complete. | **Control Objective 5:** Logical and Physical Controls |
| 8 | For user entities sending data to Everstream, data must be protected by appropriate methods for ensuring confidentiality, privacy, integrity, availability, and non-repudiation. | **Control Objective 5:** Logical and Physical Controls |
| 9 | 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. | **Control Objective 5:** Logical and Physical Controls |
| 10 | Notifying Everstream of any accompanying vendors or contractors that are not on the authorization list that will be escorted by authorized company personnel. | **Control Objective 5:** Logical and Physical Controls |
| 11 | Developing and, if necessary, implementing a business continuity and disaster recovery plan that will aid in the continuation of services provided by Everstream. | **Control Objective 8:** Availability |
| 12 | Maintaining appropriate disaster recovery processes and procedures, including backups of data. | **Control Objective 8:** Availability |

# IV. Description of Everstream Solutions, LLC's Control Objectives and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results

## A. Information Provided by the Independent Service Auditor

This SOC 1 Type 2 report was prepared in accordance with the AICPA attestation standards and, when combined with an understanding of the controls at user entities, is intended to assist auditors in planning the audit of user entities' financial statements or user entities' internal control over financial reporting and in assessing control risk for assertions in user entities' financial statements that may be affected by controls at Everstream Solutions, LLC.

Our examination was limited to the control objectives and related controls specified by Everstream Solutions, LLC in Sections III and IV of the report, and did not extend to controls in effect at user entities.

It is the responsibility of each user entity and its independent auditor to evaluate this information in conjunction with the evaluation of internal control over financial reporting at the user entity in order to assess total internal control. If internal control is not effective at user entities, Everstream Solutions, LLC's controls may not compensate for such weaknesses.

Everstream Solutions, LLC's internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by Everstream Solutions, LLC. In planning the nature, timing, and extent of our testing of the controls to achieve the control objectives specified by Everstream Solutions, LLC, we considered aspects of Everstream Solutions, LLC's control environment, risk assessment process, monitoring activities, and information and communications.

THE FOLLOWING TABLE CLARIFIES CERTAIN TERMS USED IN THIS SECTION TO DESCRIBE THE NATURE OF THE TESTS PERFORMED:

| 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. |

In addition, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

## B. Test of Controls and Results

### 1. Organization and Management

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 1:** Controls provide reasonable assurance that Everstream Solutions, LLC has an organizational structure, with established policies and procedures for onboarding, training, and monitoring performance. | | |
| 1. 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.<br><br>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.<br><br>No exceptions noted. |
| 2. 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.<br><br>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.<br><br>No exceptions noted. |
| 3. 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.<br><br>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.<br><br>No exceptions noted. |

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 1:** Controls provide reasonable assurance that Everstream Solutions, LLC has an organizational structure, with established policies and procedures for onboarding, training, and monitoring performance. | | |
| 4. 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.<br><br>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.<br><br>No exceptions noted. |
| 5. 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.<br><br>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.<br><br>No exceptions noted. |
| 6. 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.<br><br>Inspected the employee handbook noting that the employee handbook covered security and confidentiality of information, and workforce conduct standards.<br><br>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.<br><br>No exceptions noted.<br><br>No exceptions noted. |

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 1:** Controls provide reasonable assurance that Everstream Solutions, LLC has an organizational structure, with established policies and procedures for onboarding, training, and monitoring performance. | | |
| 7. 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.<br><br>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.<br><br>No exceptions noted. |

## 2. Communications

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 2:** Controls provide reasonable assurance that Everstream customers are implemented and administered based on client expectations and that internal users are provided information on operation of the data center. | | |
| 1. 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.<br><br>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.<br><br>No exceptions noted. |
| 2. 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. |
| 3. 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.<br><br>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.<br><br>No exceptions noted. |
| 4. 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.<br><br>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.<br><br>No exceptions noted. |

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 2:** Controls provide reasonable assurance that Everstream customers are implemented and administered based on client expectations and that internal users are provided information on operation of the data center. | | |
| 5. 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.<br><br>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.<br><br>No exceptions noted. |

## 3. Risk Management

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 3:** Controls provide reasonable assurance that Everstream Solutions, LLC identifies potential threats that could impair system security and availability commitments and system requirements, analyzes the significance of risks associated with the identified threats, and determines mitigation strategies for those risks. | | |
| 1. 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.<br><br>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.<br><br>No exceptions noted. |

## 4. Monitoring Controls

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 4:** Controls provide reasonable assurance that the design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and availability. | | |
| 1. 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.<br><br>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.<br><br>No exceptions noted. |
| 2. 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.<br><br>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.<br><br>Inspected the patch management centralized settings noting that patches considered to be "zero-day" patches were applied immediately. | No exceptions noted.<br><br>No exceptions noted.<br><br>No exceptions noted. |
| 3. 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.<br><br>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.<br><br>No exceptions noted. |

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 4:** Controls provide reasonable assurance that the design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and availability. | | |
| 4. 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.<br><br>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.<br><br>No exceptions noted. |
| 5. 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.<br><br>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.<br><br>No exceptions noted. |

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 4:** Controls provide reasonable assurance that the design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and availability. | | |
| 6. 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.<br><br>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.<br><br>For two out of forty company machines selected, anti-virus software was not deployed.<br><br>*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. |

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 4:** Controls provide reasonable assurance that the design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and availability. | | |
| | | 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. |

## 5. Logical and Physical Controls

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 5:** Controls provide reasonable assurance that access to Grand Rapids data center is limited to personnel authorized by management and controls provide reasonable assurance that access to data is restricted to appropriate personnel. | | |
| 1. 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. | No exceptions noted. |
| | 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. | No exceptions noted. |
| | 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. |

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 5:** Controls provide reasonable assurance that access to Grand Rapids data center is limited to personnel authorized by management and controls provide reasonable assurance that access to data is restricted to appropriate personnel. | | |
| 2. 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. |
| 3. 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. | No exceptions noted. |
| | 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. | No exceptions noted. |
| | 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. |

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 5:** Controls provide reasonable assurance that access to Grand Rapids data center is limited to personnel authorized by management and controls provide reasonable assurance that access to data is restricted to appropriate personnel. | | |
| 4. 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.<br><br>Observed the process for entrance into the lower data center floor area noting that:<br>• 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.<br>• A badge reader was at the entrance to the closed customer work area where customers swiped their badge to unlock the doors.<br>• Once the badge was swiped, a PIN was necessary to gain access.<br>• 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.<br><br>No exceptions noted. |
| 5. 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.<br><br>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.<br><br>No exceptions noted. |

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 5:** Controls provide reasonable assurance that access to Grand Rapids data center is limited to personnel authorized by management and controls provide reasonable assurance that access to data is restricted to appropriate personnel. | | |
| 6. 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.<br><br>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.<br><br>No exceptions noted. |
| 7. 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.<br><br>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.<br><br>No exceptions noted. |
| 8. 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.<br><br>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.<br><br>No exceptions noted. |

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 5:** Controls provide reasonable assurance that access to Grand Rapids data center is limited to personnel authorized by management and controls provide reasonable assurance that access to data is restricted to appropriate personnel. | | |
| 9. 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.<br><br>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.<br><br>No exceptions noted. |
| 10. 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.<br><br>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.<br><br>No exceptions noted. |

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 5:** Controls provide reasonable assurance that access to Grand Rapids data center is limited to personnel authorized by management and controls provide reasonable assurance that access to data is restricted to appropriate personnel. | | |
| 11. Group policy within Active Directory is used to enforce password parameters which are defined as:<br>• Password History – Four passwords remembered<br>• Maximum Password age – 181 days<br>• Minimum password length – 8 characters<br>• Minimum Password age – One day<br>• 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:<br>• Password History – Four passwords remembered<br>• Maximum Password age – 181 days<br>• Minimum password length – 8 characters<br>• Minimum Password age – One day<br>• Password must meet complexity requirements – Enabled<br><br>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:<br>• Password History – Four passwords remembered<br>• Maximum Password age – 181 days<br>• Minimum Password age – One day<br>• Password must meet complexity requirements – Enabled | No exceptions noted.<br><br>No exceptions noted. |
| 12. 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.<br><br>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.<br><br>No exceptions noted. |
| 13. 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.<br><br>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.<br><br>No exceptions noted. |

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 5:** Controls provide reasonable assurance that access to Grand Rapids data center is limited to personnel authorized by management and controls provide reasonable assurance that access to data is restricted to appropriate personnel. | | |
| 14. 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.<br><br>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.<br><br>No exceptions noted. |
| 15. 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.<br><br>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.<br><br>Inspected Active Directory integration noting that Active Directory was integrated with the TACACS server. | No exceptions noted.<br><br>No exceptions noted.<br><br>No exceptions noted. |
| 16. 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. |
| 17. 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. |

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 5:** Controls provide reasonable assurance that access to Grand Rapids data center is limited to personnel authorized by management and controls provide reasonable assurance that access to data is restricted to appropriate personnel. | | |
| 18. 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.<br><br>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.<br><br>No exceptions noted. |
| 19. 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.<br><br>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).<br><br>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.<br><br>No exceptions noted.<br><br>No exceptions noted. |
| 20. 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.<br><br>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.<br><br>No exceptions noted. |

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 5:** Controls provide reasonable assurance that access to Grand Rapids data center is limited to personnel authorized by management and controls provide reasonable assurance that access to data is restricted to appropriate personnel. | | |
| 21. 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.<br><br>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.<br><br>No exceptions noted. |
| 22. 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.<br><br>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.<br><br>No exceptions noted. |

## 6. System Operations

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 6:** Controls provide reasonable assurance that key systems are monitored and supported through a defined support process. | | |
| 1. 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.<br><br>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.<br><br>No exceptions noted. |
| 2. 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.<br><br>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.<br><br>No exceptions noted. |
| 3. 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.<br><br>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.<br><br>No exceptions noted. |

## 7. Change Management

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 7:** Controls provide reasonable assurance that changes to the Grand Rapids data center are executed according to established policies and procedures. | | |
| 1. 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.<br><br>Inspected the change management policy noting that Everstream had a written change management policy to guide the change management process. | No exceptions noted.<br><br>No exceptions noted. |
| 2. 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.<br><br>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.<br><br>No exceptions noted. |
| 3. 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.<br><br>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.<br><br>No exceptions noted. |

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 7:** Controls provide reasonable assurance that changes to the Grand Rapids data center are executed according to established policies and procedures. | | |
| 4. 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.<br><br>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.<br><br>No exceptions noted. |

## 8. Availability

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 8:** Controls provide reasonable assurance that procedures exist to permit the continuance of business operations in the event the operations are disabled, including backup and recovery. | | |
| 1. 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. |
| 2. 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. | No exceptions noted. |
| | 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. |

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 8:** Controls provide reasonable assurance that procedures exist to permit the continuance of business operations in the event the operations are disabled, including backup and recovery. | | |
| 3. 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. |
| 4. 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. | No exceptions noted. |
| | Observed data center cabinets with the Facilities Operations Manager that temperature and humidity sensors were present in each server cabinet. | No exceptions noted. |
| | 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. |

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 8:** Controls provide reasonable assurance that procedures exist to permit the continuance of business operations in the event the operations are disabled, including backup and recovery. | | |
| 5. 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.<br><br>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.<br><br>No exceptions noted. |
| 6. 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.<br><br>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.<br><br>No exceptions noted. |
| 7. 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.<br><br>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.<br><br>No exceptions noted. |

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 8:** Controls provide reasonable assurance that procedures exist to permit the continuance of business operations in the event the operations are disabled, including backup and recovery. | | |
| 8. 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. |
| 9. 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. |

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 8:** Controls provide reasonable assurance that procedures exist to permit the continuance of business operations in the event the operations are disabled, including backup and recovery. | | |
| 10. 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.<br><br>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.<br><br>No exceptions noted. |
| 11. 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.<br><br>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.<br><br>No exceptions noted. |

| Controls Specified by Everstream Solutions, LLC | Tests Performed by Moss Adams LLP | Test Results |
|---|---|---|
| **Control Objective 8:** Controls provide reasonable assurance that procedures exist to permit the continuance of business operations in the event the operations are disabled, including backup and recovery. | | |
| 12. 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.<br><br>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.<br><br>No exceptions noted. |
| 13. 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.<br><br>Inspected the disaster recovery plan noting that the section titled "Disaster Recovery Plan Exercising" described the purpose of regular testing and rehearsal.<br><br>Inspected the disaster recovery testing documentation noting that the disaster recovery plan was tested on an annual basis. | No exceptions noted.<br><br>No exceptions noted.<br><br>No exceptions noted. |

MOSSADAMS