



A-LIGN



ColoHouse LLC  
Type 2 SOC 2  
2018

COLOHOUSE

**REPORT ON COLOHOUSE LLC'S DESCRIPTION OF ITS SYSTEM AND ON THE  
SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS  
CONTROLS RELEVANT TO SECURITY, AVAILABILITY,  
AND CONFIDENTIALITY**

**Pursuant to Reporting on Service Organization Controls 2 (SOC 2)  
Type 2 examination performed under AT-C 105 and AT-C 205**

**January 1, 2018 To December 14, 2018**

# Table of Contents

<b>SECTION 1 INDEPENDENT SERVICE AUDITOR'S REPORT .....</b>	<b>1</b>
<b>SECTION 2 MANAGEMENT OF COLOHOUSE LLC'S ASSERTION REGARDING ITS SYSTEM THROUGHOUT THE PERIOD JANUARY 1, 2018 TO DECEMBER 14, 2018.....</b>	<b>4</b>
<b>SECTION 3 DESCRIPTION OF COLOHOUSE LLC'S SYSTEM THROUGHOUT THE PERIOD JANUARY 1, 2018 TO DECEMBER 14, 2018.....</b>	<b>7</b>
OVERVIEW OF OPERATIONS.....	8
Company Background .....	8
Description of Services Provided .....	8
CONTROL ENVIRONMENT .....	13
Integrity and Ethical Values .....	13
Commitment to Competence .....	13
Management's Philosophy and Operating Style.....	13
Organizational Structure and Assignment of Authority and Responsibility .....	13
Human Resources Policies and Practices .....	13
RISK ASSESSMENT .....	14
TRUST SERVICES PRINCIPLES AND CRITERIA.....	14
MONITORING .....	15
INFORMATION AND COMMUNICATION SYSTEMS .....	16
COMPLEMENTARY USER ENTITY CONTROLS.....	16
<b>SECTION 4 INFORMATION PROVIDED BY THE SERVICE AUDITOR .....</b>	<b>18</b>
GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR .....	19
COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES .....	20
AVAILABILITY CRITERIA .....	72
CONFIDENTIALITY CRITERIA .....	79

**SECTION 1**  
**INDEPENDENT SERVICE AUDITOR'S REPORT**



## INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS AT COLOHOUSE LLC RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY

To ColoHouse LLC:

We have examined the attached description titled "Description of ColoHouse LLC's Colocation and Managed Services System Throughout the Period January 1, 2018 To December 14, 2018" (the description) and the suitability of the design and operating effectiveness of controls to meet the criteria for the Security, Availability, and Confidentiality principles set forth in TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Technical Practice Aids*) (applicable trust services criteria), throughout the period January 1, 2018 to December 14, 2018. The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of ColoHouse LLC's ('ColoHouse' or 'the Company') controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

ColoHouse uses Digital Realty Trust, L.P. ("subservice organization") for data center physical security services. The description indicates that certain applicable trust services criteria can only be met if controls at the subservice organization are suitably designed and operating effectively. The description presents ColoHouse's system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organization to meet certain applicable trust services criteria. The description does not include any of the controls implemented at the subservice organization. Our examination did not extend to the services provided by the subservice organization.

ColoHouse has provided the attached assertion titled "Management of ColoHouse's Assertion Regarding Its Colocation and Managed Services System Throughout the Period January 1, 2018 To December 14, 2018," which is based on the criteria identified in management's assertion. ColoHouse is responsible for (1) preparing the description and assertion; (2) the completeness, accuracy, and method of presentation of both the description and assertion; (3) providing the services covered by the description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in ColoHouse's assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period January 1, 2018 to December 14, 2018.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. 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 meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

In our opinion, in all material respects, based on the description criteria identified in ColoHouse's assertion and the applicable trust services criteria:

- a. the description fairly presents the system that was designed and implemented throughout the period January 1, 2018 to December 14, 2018.
- b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period January 1, 2018 to December 14, 2018, and user entities applied the complementary user-entity controls contemplated in the design of ColoHouse's controls throughout the period January 1, 2018 to December 14, 2018 and the subservice organization applied, throughout the period January 1, 2018 to December 14, 2018, the types of controls expected to be implemented at the subservice organization and incorporated in the design of the system.
- c. the controls tested, which together with the complementary user-entity controls referred to in the scope paragraph of this report, and together with the types of controls expected to be implemented at the subservice organization and incorporated in the design of the system, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period January 1, 2018 to December 14, 2018.

The specific controls we tested and the nature, timing, and results of our tests are presented in the section of our report titled "Information Provided by the Service Auditor".

This report and the description of tests of controls and results thereof are intended solely for the information and use of ColoHouse; user entities of ColoHouse's Colocation and Managed Services System during some or all throughout the period January 1, 2018 to December 14, 2018; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, subservice organizations, or other parties.
- Internal control and its limitations.
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

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

A-LIGN ASSURANCE

January 11, 2019  
Tampa, Florida

## **SECTION 2**

### **MANAGEMENT OF COLOHOUSE LLC'S ASSERTION REGARDING ITS SYSTEM THROUGHOUT THE PERIOD JANUARY 1, 2018 TO DECEMBER 14, 2018**

**Management of ColoHouse LLC's Assertion Regarding Its System Throughout the Period  
January 1, 2018 To December 14, 2018**

January 11, 2019

We have prepared the attached description titled "Description of ColoHouse LLC's Colocation and Managed Services System Throughout the Period January 1, 2018 To December 14, 2018" (the description), based on the criteria in items (a)(i)-(ii) below, which are the criteria for a description of a service organization's system in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (the description criteria). The description is intended to provide users with information about the Colocation and Managed Services System, particularly system controls intended to meet the criteria for the Security, Availability, and Confidentiality principles set forth in TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Technical Practice Aids*) (applicable trust services criteria). We confirm, to the best of our knowledge and belief, that:

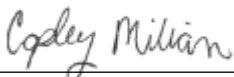
- a. The description fairly presents the Colocation and Managed Services System throughout the period January 1, 2018 to December 14, 2018, based on the following description criteria:
  - i. The description contains the following information:
    - (1) The types of services provided.
    - (2) The components of the system used to provide the services, which are the following:
      - *Infrastructure*. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).
      - *Software*. The application programs and IT systems software that supports application programs (operating systems, middleware, and utilities).
      - *People*. The personnel involved in governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
      - *Processes*. The automated and manual procedures.
      - *Data*. Transaction streams, files, databases, tables, and output used or processed by a system.
    - (3) The boundaries or aspects of the system covered by the description.
    - (4) How the system captures and addresses significant events and conditions.
    - (5) The process used to prepare and deliver reports and other information to user entities or other parties.
    - (6) If information is provided to, or received from, subservice organizations or other parties, how such information is provided or received; the role of the subservice organization or other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.
    - (7) For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the service organization's system.
    - (8) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons therefore.



(9) Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

(10) Relevant details of changes to the service organization's system during the period covered by the description.

- ii. The description 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 users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.
- b. The controls stated in description were suitably designed throughout the specified period to meet the applicable trust services criteria.
- c. The controls stated in the description operated effectively throughout the specified period to meet the applicable trust services criteria.



---

Copley Milian  
SVP of Business Operations  
ColoHouse LLC

### **SECTION 3**

#### **DESCRIPTION OF COLOHOUSE LLC'S SYSTEM THROUGHOUT THE PERIOD JANUARY 1, 2018 TO DECEMBER 14, 2018**

## OVERVIEW OF OPERATIONS

### Company Background

In 2007, ColoHouse LLC (ColoHouse) was founded with the mission of delivering businesses with carrier-neutral IT infrastructure services, while also facilitating growth for complimentary service providers and clients globally. With over 250 clients and technology partners, ColoHouse delivers on its mission through a mix of best-in-class data center management and a service-oriented company culture.

ColoHouse's infrastructure solutions are delivered via a recurring-revenue based business model. The data center is based in downtown Miami, Florida. The city's telecommunications infrastructure solidifies Miami's spot as one the top five most interconnected cities in the world; ideal for numerous industries seeking stable connectivity domestically and internationally.

Industries served by ColoHouse include Information Technology, Telecommunications, Financial Services, Manufacturing, Legal Services, Advertising, Healthcare and Retail.

### Description of Services Provided

ColoHouse provides colocation and managed services to clients and technology partners.

ColoHouse has three facilities, one in the United States and two in The Netherlands. ColoHouse also has Point of Presence locations throughout the US, Asia, Europe, and South America.

ColoHouse Miami colocation services are delivered within a purpose-built, Category 5 Hurricane protected facility, which is also outside the FEMA 500 year Flood Zone. The 24,000 sq. ft. ColoHouse facility houses two data centers, MIA I and MIA II. The infrastructure was designed and engineered for secure, redundant colocation. The data center provides N+1 redundancy on all environmental systems; ColoHouse also leverages separate utility power feeds (three) on diversified grids.

ColoHouse's electrical and mechanical systems all utilize high-performance equipment that is continuously monitored and tested to guarantee peak performance. Redundant infrastructure is guaranteed in the company's iron-clad 100% uptime Service Level Agreement.

The carrier-neutral data center has more than 20 directly available bandwidth providers through the facility's Meet-Me-Room, along with interconnectivity to the Florida Internet Exchange FL-IX. ColoHouse offers its own blend of bandwidth to its customers. This allows for an all-inclusive colocation offering.

In addition to the facilities and bandwidth, ColoHouse offers customers and prospects a full-suite of network and managed service solutions. Customers are able to have a blend of service options in addition to their colocation services or as standalone products.

With services, like private, public, or hybrid cloud, managed services, DDoS protection, dedicated servers, and per unit colocation, ColoHouse's provides the most customizable packages that meet the unique requirements of ColoHouse's customers' businesses.

ColoHouse support is rooted in a service-oriented company culture. Staff is available onsite, by phone or via the company's web-based Customer Portal 24/7/365. Support services provided are comprehensive and responsive - backed by trained, experienced IT specialists.

## Infrastructure

Primary infrastructure used to provide ColoHouse's Colocation and Managed services system includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
Security Cameras	MIA I - Coax MIA II - POE	Monitor activity within the data center and administrative floor
(2) Automatic Transfer Switch (ATS)	Cutler-Hammer	Monitors connection to power supply and activates load transfer to generator if an interruption occurs
(6) Uninterrupted Power Supply (UPS)	Eaton	Provides emergency backup power prior to going on generator - ensures no interruption in power
(8) PDU/ (8)RPP	Eaton	Distributes power to customer space and monitors usage
(2) Generators	Cummins 1Meg Each	Provide power to the data center in a power emergency
HVAC	MIA I - 10 Leibert 22 Ton MIA II - 3 Leibert 30 Ton	Provide proper cooling and humidity to the data center and monitors levels
Fire Detection & Suppression System	Dry pipe	Protect against fires
Cloud platform	Supermicro FatTwin hypervisors and Dell Equallogic PS6100XV storages	Internal systems and ColoHouse Cloud services
Core Network	Juniper MX240, EX4200, QFX3500 and Brocade RX8	Enables backbone connectivity for key ColoHouse services

## Software

Primary software used to provide ColoHouse's Colocation and Managed services system includes the following:

Primary Software		
Software	Operating System	Purpose
KeyScan	N/A	Access control management software used to regulate access to both the front and back doors of MIA I and MIA II
Falcon	N/A	Email emergency notification system set up to notify Operations of changes within major infrastructure

Primary Software		
Software	Operating System	Purpose
ConnectWise	N/A	Business management software used to generate customer support tickets and customer power alerts
OnPage	N/A	Virtual pager application used to assist with emergency notifications regarding changes within major infrastructure and SLA requirements
GitLab	CentOS 6	Development tracking software for internal systems
Zabbix	CentOS 7	Infrastructure monitoring software for ColoHouse NL datacenter and Netrouting managed services
LibreNMS	Ubuntu 18.04	Network monitoring software for ColoHouse core network and managed services customers
INT	CentOS 7	Full featured datacenter and cloud management system for Netrouting managed services, network and shared colocation customers
WHMCS	CentOS 7	Billing system for Netrouting customers

### *People*

The ColoHouse staff provides support for the above services in each of the following functional areas:

- Executive management - provides general oversight and strategic planning of operations
- Technical Support team - responsible for the resolution of all technical requests made by customers, to satisfaction of the customer. Responsible for delivering a responsive system that fully complies with the functional specification. Verifies that the system complies with the functional specification through functional testing procedures. Responsible for effective provisioning, installation/configuration, operation, and maintenance of systems
- Customer Support - serves customers by providing product and service information that includes resolving product and service issues

### *Processes*

#### *Physical and Environmental Procedures*

Physical access to the Company's data center, servers, and premises is restricted to appropriate individuals using a key card and a biometric system. On a quarterly basis, a user access review of the data center key card and biometric systems is performed. Any identified discrepancies are documented and resolved. Data center access is monitored 24 hours a day, 7 days per week, through video surveillance and on-site security guards to prevent unauthorized access. Access to the Company's data center key card and biometric system and office premises is formally documented and approved and is removed upon employee termination or notification from the client.

Access to server cages is secured by key to prevent unauthorized access. In addition, access to the server racks is secured by a custom key code determined by the client. In case of an emergency, the Company's management maintains a master key to access the server cages and racks.

All visitor access must be approved by a Company employee or a valid badge holder. Visitors must be properly identified with a current valid form of identification, given a temporary facility badge allowing access to certain areas within the Company's facility, photographed, and logged in the ticketing system. While in the Company's facility, visitors must be accompanied by active employees. An authorized vendor and client list is maintained and distributed to prevent unauthorized access.

Video surveillance equipment is placed in key areas throughout the facility (lobby, elevator, hallway, and all access points to the data center) and actively monitored. All video is retained for a predetermined minimum period. Main components of the physical security of the data center are managed by Digital Realty Trust, L.P.

The Company's data center is protected with a dry fire suppression system to prevent damage to the servers located in the data center in the case of fire. The Company's data center has multiple independent air conditioning units and is monitored for significant temperature and humidity fluctuations. Automated e-mail notifications are sent to the Company's support staff when air conditioning, fire, leak detection, and power issues occur. Incidents are followed up on and their resolution is documented.

Raised floors are in place throughout the Company's data center server rooms to protect servers from flood damage. On an annual basis, the leak detection system in the Company's data center is tested to prevent water damage to the servers located in the Company's data center.

The Company's data center has a redundant configuration and multiple power panels with circuit breakers to minimize the disruption of operations during a power outage. Automatic transfer switches (ATS) are in place to utilize the generators and uninterruptible power supply (UPS) in the case of an emergency. In addition, at least semi-annually, the UPS and generators are tested with the critical load through the use of ATS. To help ensure operations during prolonged power outages, generators undergo scheduled maintenance on a quarterly basis. Maintenance contracts are in place for all significant electrical equipment (generators, power panels and heating, ventilating, and air conditioning (HVAC) systems).

### *Data*

Colocation data is managed in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. Colocation data is captured which is utilized by ColoHouse in delivering its colocation services system. Such data includes, but is not limited to, the following:

- Alert notifications and monitoring reports generated from the monitoring applications
- Alert notifications received from automated physical and environmental monitoring systems
- Incident reports documented via the ticketing systems

### **Boundaries of the System**

The scope of this report includes the Colocation and Managed services system performed in the Miami, Florida and New York, New York facilities.

This report does not include the data center services provided by Digital Realty Trust, L.P (Digital Realty).

### **Significant Events and Conditions**

ColoHouse has implemented automated and manual procedures to capture and address significant event and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with detailed information that impacts the colocation services system. Please see the procedures, monitoring, and risk assessment procedures described in the relevant sections of this report for further details.

## Preparation and Delivery of Reports and Data

ColoHouse utilizes the services and procedures described above to capture, prepare, and deliver reports and other information (described in the data section above) to user entities and other parties.

## Subservice Organizations

The data center physical security services provided by Digital Realty are monitored by management; however, they have not been included in the scope of this review. The following criteria and controls are expected to be implemented by Digital Realty:

Subservice Organization Controls		
Principle	Criteria	Applicable Controls
Common Criteria/Security	CC5.5	Physical access controls are in place to restrict access to and within the data center facilities.
Common Criteria/Security	CC5.5	Physical access requests are documented and require the approval of the site manager.
Common Criteria/Security	CC5.5	A review of Digital Realty employees and contractors with physical access to customer suites is performed on a quarterly basis and unnecessary access is identified, modified, and removed as necessary.
Common Criteria/Security	CC5.5	A termination notification ticket is completed by HR and physical access is revoked by the corporate security team for Digital Realty employee and contractor terminations within one business day of termination.
Common Criteria/Security	CC5.5	Visitors are required to surrender their badges upon exit. Access badges for visitors that do not require an escort are configured to expire at the end of the day.
Common Criteria/Security	CC5.5	Surveillance cameras are in place to monitor and record access to and within the data centers. Surveillance cameras are located along the building perimeters and within the data centers.
Common Criteria/Security	CC5.5	Digital surveillance systems are required to retain video footage for the data centers for a minimum of 90 days.

## Criteria Not Applicable to the System

All Common, Availability, and Confidentiality criterion were applicable to the ColoHouse colocation and managed services system.

## Significant Changes

Since the last organization review ColoHouse acquired Netrouting Inc and Data Facilities data centers based in the Netherlands. This acquisition gave ColoHouse a global presence with locations in 7 countries and a new suite of services including bandwidth, cloud, managed services, DDoS protection, dedicated servers, and per unit colocation.

## **CONTROL ENVIRONMENT**

### **Integrity and Ethical Values**

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of ColoHouse's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of ColoHouse's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

### **Commitment to Competence**

ColoHouse's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

### **Management's Philosophy and Operating Style**

ColoHouse's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel. The ColoHouse philosophy and operating style are demonstrated through the following:

- Client Focused - anticipating, understanding and responding to client needs with excellence in order to facilitate growth as well as build lasting trust and loyalty
- Pledge to Quality Assurance - dedication to continuous internal and external improvement of their practices, procedures, and the ColoHouse value offering in order to always provide clients with optimal solutions
- Engagement - commitment to supporting an environment in which all team members openly communicate frequently, with an emphasis on trust, integrity and mutual respect
- Relationship Building - the success of ColoHouse is dependent on the quality of their relationships. All business relationships are formalized with mutual respect and understanding

### **Organizational Structure and Assignment of Authority and Responsibility**

ColoHouse's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

ColoHouse's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

### **Human Resources Policies and Practices**

ColoHouse's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. ColoHouse's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.



Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment
- Company new hires undergo criminal background checks. The results of the background checks are reviewed by management and/or recruiters to determine final employment eligibility
- Evaluations for each employee are performed on an annual basis
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

## **RISK ASSESSMENT**

ColoHouse's risk assessment process identifies and manages risks that could potentially affect ColoHouse's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. ColoHouse identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by ColoHouse, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

## **TRUST SERVICES PRINCIPLES AND CRITERIA**

### **In-Scope Trust Services Principles**

#### **Common Criteria (to the Security, Availability, and Confidentiality Principles)**

The security principle refers to the protection of the system resources through logical and physical access control measures in order to enable the entity to meet its commitments and system requirements related to security, availability, processing integrity, confidentiality, and privacy. Controls over the security of a system prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of data or system resources, misuse of software, and improper access to, or use of, alteration, destruction, or disclosure of information.

#### **Availability**

The availability principle refers to the accessibility of the system, products, or services as committed by contract, service-level agreement, or other agreements. This principle does not, in itself, set a minimum acceptable performance level for system availability. The availability principle does not address system functionality (the specific functions a system performs) and system usability (the ability of users to apply system functions to the performance of specific tasks or problems), but does address whether the system includes controls to support system accessibility for operation, monitoring, and maintenance.

## Confidentiality

The confidentiality principle addresses the system's ability to protect information designated as confidential, including, its final disposition and removal from the system in accordance with management's commitments and system requirements. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention, and restrict its disclosure to defined parties (including those who may otherwise have authorized access within the boundaries of the system). Such requirements may be contained in laws or regulations, or commitments in user contracts. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel. Confidentiality is distinguished from privacy in that the privacy applies only to personal information, while the confidentiality principle applies to various types of sensitive information. In addition, the privacy principle addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

## Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of ColoHouse's Colocation and Managed services system; as well as the nature of the components of the system result in risks that the criteria will not be met. ColoHouse addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, ColoHouse's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

## Control Activities Specified by the Service Organization

The applicable trust criteria, risks, and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section. Although the applicable trust criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of ColoHouse's description of the system. Any applicable trust services criteria that are not addressed by control activities at ColoHouse are described within Section 4 and within the Subservice Organization and Criteria Not Applicable to the System sections above.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

## MONITORING

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. ColoHouse's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

## **On-Going Monitoring**

ColoHouse's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in ColoHouse's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of ColoHouse's personnel. Specific tools used in monitoring controls include the following:

- Key Scan - access control management software used to regulate access to both the front and back doors of MIA I and MIA II
- Falcon - email emergency notification system set up to notify Operations of changes within major infrastructure
- ConnectWise - business management software used to generate customer support tickets and customer power alerts
- OnPage - Virtual pager application used to assist with emergency notifications regarding changes within major infrastructure and SLA requirements

## **Reporting Deficiencies**

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

## **INFORMATION AND COMMUNICATION SYSTEMS**

Information and communication is an integral component of ColoHouse's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At ColoHouse, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. General updates to entity-wide security policies and procedures are usually communicated to the appropriate ColoHouse personnel via e-mail messages.

Specific information systems used to support ColoHouse's Colocation and Managed services system are described in the Description of Services section above.

## **COMPLEMENTARY USER ENTITY CONTROLS**

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

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

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

**SECTION 4**  
**INFORMATION PROVIDED BY THE SERVICE AUDITOR**

# GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-LIGN ASSURANCE’s examination of the controls of ColoHouse was limited to the Trust Services Principles and related criteria and control activities specified by the management of ColoHouse and did not encompass all aspects of ColoHouse’s operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client’s knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity’s internal control.

In determining whether the report meets the user auditor’s objectives, the user auditor should perform the following procedures:

- Understand the aspects of the service organization’s controls that may affect the processing of the user entity’s transactions;
- Understand the flow of significant transactions through the service organization;
- Determine whether the control objectives are relevant to the user entity’s financial statement assertions; and
- Determine whether the service organization’s controls are suitably designed to prevent or detect processing errors that could result in material misstatements in the user entity’s financial statements and determine whether they have been implemented.

**Control Activities Specified by the Service Organization**

<b>COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES</b>				
<b>CC1.0</b>	<b>Common Criteria Related to Organization and Management</b>			
<b>Control Point</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security, availability, and confidentiality.	<p>A documented organizational chart is in place to communicate organizational structures, lines of reporting, and areas of authority.</p> <p>Reporting relationships and organizational structures are reviewed annually by management.</p> <p>Roles and responsibilities are defined in written job descriptions and communicated to personnel.</p> <p>Hiring procedures are in place to guide personnel in the onboarding process.</p>	<p>Inspected the organizational chart to determine that a documented organizational chart was in place to communicate organizational structures, lines of reporting, and areas of authority.</p> <p>Inquired of the VP of Operations regarding the review of reporting relationships and organizational structure to determine that reporting relationships and organizational structures were reviewed annually by management.</p> <p>Inspected the organizational chart versioning date to determine that the reporting relationships and organizational structures were reviewed annually by management.</p> <p>Inspected a sample of job descriptions to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel.</p> <p>Inspected the hiring procedures to determine that hiring procedures were in place to guide personnel in the onboarding process.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC1.0	Common Criteria Related to Organization and Management			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	Management reviews job descriptions and makes updates, if necessary.	Inquired of the VP of Operations regarding senior management review of job descriptions to determine that management reviewed job descriptions and made updates, if necessary.	No exceptions noted.
			Inspected a sample of job descriptions to determine that management reviewed job descriptions and made updates, if necessary.	No exceptions noted.
		A documented organizational chart is in place to assign responsibility and delegate lines of authority to personnel.	Inspected the organizational chart to determine that a documented organizational chart was in place to assign responsibility and delegate lines of authority to personnel.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel.	Inspected a sample of job descriptions to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel.	No exceptions noted.
		Management reviews job descriptions and makes updates, if necessary.	Inquired of the VP of Operations regarding senior management review of job descriptions to determine that management reviewed job descriptions and made updates, if necessary.	No exceptions noted.



**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC1.0	Common Criteria Related to Organization and Management			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security, availability, and confidentiality and provides resources necessary for personnel to fulfill their responsibilities.	Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process.	<p>Inspected a sample of job descriptions to determine that management reviewed job descriptions and made updates, if necessary.</p> <p>Inspected a sample of job descriptions, hiring procedures, and interview evaluation for a sample of new hires to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements were evaluated as part of the hiring or transfer evaluation process.</p>	No exceptions noted.
		The experience and training of candidates for employment or transfer are evaluated before they assess the responsibilities of their position.	Inspected the hiring procedures to determine that the experience and training of candidates for employment or transfer were evaluated before they assessed the responsibilities of their position.	No exceptions noted.
		Management documents skills and continued training to establish the organization's commitments and requirements for employees.	Inspected the training materials and completed training for a sample of current employees to determine that management documented skills and continued training to establish the organization's commitments and requirements for employees.	No exceptions noted.



**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC1.0	Common Criteria Related to Organization and Management			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Personnel are required to sign and accept the employee handbook and code of conduct upon hire.</p> <p>Personnel are required to complete a background check provided by a third-party vendor upon hire.</p>	<p>Inspected the signed employee handbook and code of conduct acknowledgements for a sample of new hires to determine that personnel were required to sign and accept the employee handbook and code of conduct upon hire.</p> <p>Inspected the completed background check for a sample of new hires to determine that personnel were required to complete a background check provided by a third-party vendor upon hire.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC2.0	Common Criteria Related to Communications			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.	System descriptions are communicated to authorized external users via service level agreement (SLA) and company website that delineate the boundaries of the system and describe relevant system components.	Inspected the entity website and the contracts for a sample of customers to determine that system descriptions were communicated to authorized external users via service level agreement (SLA) and company website that delineated the boundaries of the system and describe relevant system components.	No exceptions noted.
		A description of the system delineating the boundaries of the system is posted on the SharePoint site and is available to personnel.	Inspected the entity website and policies and procedures posted on the SharePoint site to determine that a description of the system delineating the boundaries of the system was posted on the SharePoint site and was available to personnel.	No exceptions noted.
		A documented organizational chart is in place to communicate organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place to communicate organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Reporting relationships and organizational structures are reviewed annually by management.	Inquired of the VP of Operations regarding the review of reporting relationships and organizational structure to determine that reporting relationships and organizational structures were reviewed annually by management.	No exceptions noted.

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC2.0	Common Criteria Related to Communications			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2	The entity's security, availability, and confidentiality commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.		Inspected the organizational chart versioning date to determine that the reporting relationships and organizational structures were reviewed annually by management.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel.	Inspected a sample of job descriptions to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel.	No exceptions noted.
		Customer responsibilities are outlined and communicated through service level agreements.	Inspected the contracts for a sample of customers to determine that customer responsibilities were outlined and communicated through service level agreements.	No exceptions noted.
		Security, availability, and confidentiality commitments are communicated to external users via defined service level agreements (SLA), master service agreements (MSA) and/or the entity website.	Inspected the contracts for a sample of customers to determine that security, availability, and confidentiality commitments were communicated to external users via defined SLA, MSA and/or the entity website.	No exceptions noted.
		Policy and procedure are documented for significant processes and are available on the entity's intranet.	Inspected the company SharePoint site to determine that policy and procedure were documented for significant processes and were available on the entity's intranet.	No exceptions noted.

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC2.0	Common Criteria Related to Communications			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Personnel are required to sign and accept the employee handbook and code of conduct upon hire.	Inspected the signed employee handbook and code of conduct acknowledgements for a sample of new hires to determine that personnel were required to sign and accept the employee handbook and code of conduct upon hire.	No exceptions noted.
		Personnel are required to attend security awareness training at least annually.	Inquired of the VP of Operations regarding the completion of training to determine that personnel were required to attend security awareness training at least annually.	No exceptions noted.
			Inspected the completed training for a sample of current employees to determine that personnel were required to attend security awareness training at least annually.	No exceptions noted.
		Management tracks and monitors compliance with training requirements.	Inquired of the VP of Operations regarding the monitoring of training to determine that management tracked and monitored compliance with training requirements.	No exceptions noted.
			Inspected the completed training for a sample of current employees to determine that management tracked and monitored compliance with training requirements.	No exceptions noted.

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC2.0	Common Criteria Related to Communications			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	Policy and procedure are documented for significant processes and are available on the entity's intranet.	Inspected the company SharePoint site to determine that policy and procedure were documented for significant processes and were available on the entity's intranet.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel.	Inspected a sample of job descriptions to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel.	No exceptions noted.
		Management reviews job descriptions and makes updates, if necessary.	Inquired of the VP of Operations regarding senior management review of job descriptions to determine that management reviewed job descriptions and made updates, if necessary.	No exceptions noted.
			Inspected a sample of job descriptions to determine that management reviewed job descriptions and made updates, if necessary.	No exceptions noted.
		Personnel are required to attend annual security, availability, and confidentiality training.	Inquired of the VP of Operations regarding the monitoring of training to determine that personnel were required to attend annual security, availability, and confidentiality training.	No exceptions noted.

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC2.0	Common Criteria Related to Communications			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security, availability, and confidentiality of the system, is provided to personnel to carry out their responsibilities.		Inspected the completed training for a sample of current employees to determine that personnel were required to attend annual security, availability, and confidentiality training.	No exceptions noted.
		Customer responsibilities are outlined and communicated through defined service level agreements (SLA), master service agreements (MSA) and/or the entity website.	Inspected the contracts for a sample of customers to determine that customer responsibilities were outlined and communicated through defined service level agreements (SLA), master service agreements (MSA) and/or the entity website.	No exceptions noted.
		Processes are monitored through service level management procedures to help ensure compliance with service level commitments and agreements.	Inspected the monitoring system configurations, notification configurations and an example alert to determine that processes were monitored through service level management procedures to help ensure compliance with service level commitments and agreements.	No exceptions noted.
		Policy and procedure documents for significant processes are available to assist personnel in carrying out their responsibilities.	Inspected the company SharePoint site to determine that policy and procedure documents for significant processes were available to assist personnel in carrying out their responsibilities.	No exceptions noted.



**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC2.0	Common Criteria Related to Communications			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Personnel are required to attend annual security, availability, and confidentiality training.	Inquired of the VP of Operations regarding the monitoring of training to determine that personnel were required to attend annual security, availability, and confidentiality training.	No exceptions noted.
		Customer responsibilities are outlined and communicated through defined service level agreements (SLA), master service agreements (MSA) and/or the entity website.	Inspected the completed training for a sample of current employees to determine that personnel were required to attend annual security, availability, and confidentiality training.  Inspected the entity website and the contracts for a sample of customers to determine that customer responsibilities were outlined and communicated through defined service level agreements (SLA), master service agreements (MSA) and/or the entity website.	No exceptions noted.  No exceptions noted.
CC2.5	Internal and external users have been provided with information on how to report security, availability, and confidentiality failures, incidents, concerns, and other complaints to appropriate personnel.	The organization's security policies and code of conduct are communicated to employees in the employee handbook.	Inspected the information security policy and employee handbook to determine that the organization's security policies and code of conduct were communicated to employees in the employee handbook.	No exceptions noted.

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC2.0	Common Criteria Related to Communications			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security, availability, and confidentiality are communicated to those users in a timely manner.	Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	Inspected the emergency action plan to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident.	No exceptions noted.
		Defined SLAs, MSAs, and policies available on the entity website are in place and communicated to authorized external users. The SLAs include communication procedures for reporting security, availability, and confidentiality related failure, incidents, and concerns to personnel.	Inspected the entity website and the contracts for a sample of customers to determine that defined SLAs, MSAs, and policies available on the entity website were in place and communicated to authorized external users. The SLAs included communication procedures for reporting security, availability, and confidentiality related failure, incidents, and concerns to personnel.	No exceptions noted.
		System changes are authorized, tested, and approved by management prior to implementation.	Inspected the tickets for a sample of application changes and a sample of infrastructure changes to determine that system changes were authorized, tested, and approved by management prior to implementation.	No exceptions noted.
		Changes are communicated to both internal and external users.	Inspected the email communication and tickets for a sample of application changes and infrastructure changes to determine that changes were communicated to both internal and external users.	No exceptions noted.

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC2.0	Common Criteria Related to Communications			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Access to the data center key card and biometric system and office premises is removed upon employee termination or notification from the client.	Inspected the badge access listing and termination checklist and email requesting the access removal of a sample of terminated employees to determine that access to the data center key card and biometric system and office premises was removed upon employee termination or notification from the client.	No exceptions noted.

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.1	<p>The entity (1) identifies potential threats that could impair system security, availability, and confidentiality commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.</p>	<p>A master list of the entity's system components is maintained, accounting for additions and removals, for management's use.</p> <p>Documented policies and procedures are in place to guide personnel when performing the risk assessment process.</p> <p>A formal risk assessment is performed on an annual basis to identify threats that could impair systems security, availability, and confidentiality commitments and requirements.</p> <p>Identified risks are rated using a risk evaluation process and ratings are reviewed by management.</p>	<p>Inspected the master list of system components to determine that a master list of the entity's system components was maintained, accounting for additions and removals, for management's use.</p> <p>Inspected the risk assessment policy to determine that documented policies and procedures were in place to guide personnel when performing the risk assessment process.</p> <p>Inspected the most recent risk assessment to determine that a formal risk assessment was performed on an annual basis to identify threats that could impair systems security, availability, and confidentiality commitments and requirements.</p> <p>Inspected the risk assessment policy and the most recent risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were reviewed by management.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Management develops risk mitigation strategies to address risks identified during the risk assessment process.</p> <p>The entity has implemented daily, weekly, and monthly risk assessment checklists to be completed by facility personnel to identify threats that could impair systems security, availability, and confidentiality commitments and requirements.</p>	<p>Inspected the risk assessment policy and the most recent risk assessment to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.</p> <p>Inquired of the VP of Operations regarding risk assessment checklists to determine that the entity had implemented daily, weekly, and monthly risk assessment checklists to be completed by facility personnel to identify threats that could impair systems security, availability, and confidentiality commitments and requirements.</p> <p>Inspected the daily checklist for a sample of days, the weekly checklist for a sample of weeks, and the monthly checklist for a sample of months to determine that the entity had implemented daily, weekly, and monthly risk assessment checklists to be completed by facility personnel to identify threats that could impair systems security, availability, and confidentiality commitments and requirements.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES				
CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.	Management has defined a formal risk management process that specifies the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk assessment policy and the most recent risk assessment to determine that management had defined a formal risk management process that specified the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
		The disaster recovery plan is developed and updated on an annual basis.	Inspected the disaster recovery plan to determine that the disaster recovery plan was developed and updated on an annual basis.	No exceptions noted.
		The disaster recovery plan is tested on an annual basis.	Inspected the most recent disaster recovery test results to determine that the disaster recovery plan was tested on an annual basis.	No exceptions noted.
		Emergency action plans have been developed and are updated annually.	Inspected the emergency action plan to determine that emergency action plans had been developed and were updated annually.	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk assessment policy and the most recent risk assessment to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>The entity has implemented daily, weekly, and monthly risk assessment checklists to be completed by facility personnel to identify threats that could impair systems security, availability, and confidentiality commitments and requirements.</p>	<p>Inquired of the VP of Operations regarding risk assessment checklists to determine that the entity had implemented daily, weekly, and monthly risk assessment checklists to be completed by facility personnel to identify threats that could impair systems security, availability, and confidentiality commitments and requirements.</p> <p>Inspected the daily checklist for a sample of days, the weekly checklist for a sample of weeks, and the monthly checklist for a sample of months to determine that the entity had implemented daily, weekly, and monthly risk assessment checklists to be completed by facility personnel to identify threats that could impair systems security, availability, and confidentiality commitments and requirements.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES				
CC4.0	Common Criteria Related to Monitoring of Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security, availability, and confidentiality, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring system configurations, notification configurations and an example alert to determine that monitoring software was used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.
		The monitoring software is configured to alert appropriate personnel when thresholds have been exceeded.	Inspected the monitoring system configurations, notification configurations and an example alert to determine that the monitoring software was configured to alert appropriate personnel when thresholds had been exceeded.	No exceptions noted.
		Operations and security personnel follow defined protocols for resolving and escalating reported events.	Inspected the emergency action plan to determine that operations and security personnel followed defined protocols for resolving and escalating reported events.	No exceptions noted.
		A formal risk assessment is performed on an annual basis to identify threats that could impair systems security, availability, and confidentiality commitments and requirements.	Inspected the most recent risk assessment to determine that a formal risk assessment was performed on an annual basis to identify threats that could impair systems security, availability, and confidentiality commitments and requirements.	No exceptions noted.



**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC4.0	Common Criteria Related to Monitoring of Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Identified risks are rated using a risk evaluation process and rating are reviewed by management.	Inspected the risk assessment policy and the most recent risk assessment to determine that identified risks were rated using a risk evaluation process and rating were reviewed by management.	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk assessment policy and the most recent risk assessment to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
		The entity has implemented daily, weekly, and monthly risk assessment checklists to be completed by facility personnel to identify threats that could impair systems security, availability, and confidentiality commitments and requirements.	Inquired of the VP of Operations regarding risk assessment checklists to determine that the entity had implemented daily, weekly, and monthly risk assessment checklists to be completed by facility personnel to identify threats that could impair systems security, availability, and confidentiality commitments and requirements.	No exceptions noted.

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

<b>COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES</b>				
<b>CC4.0</b>	<b>Common Criteria Related to Monitoring of Controls</b>			
<b>Control Point</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
			Inspected the daily checklist for a sample of days, the weekly checklist for a sample of weeks, and the monthly checklist for a sample of months to determine that the entity had implemented daily, weekly, and monthly risk assessment checklists to be completed by facility personnel to identify threats that could impair systems security, availability, and confidentiality commitments and requirements.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.	Inspected the information security policy to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
		Logical and physical access to systems is granted to an employee as a component of the hiring process.	Inspected the hiring procedures, hiring checklist and access request for a sample of new hires to determine that logical and physical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical and physical access to systems is revoked as a component of the termination process.	Inspected the badge access listing, network user listing, termination checklist and email requesting the access removal for a sample of terminated employees to determine that logical and physical access to systems was revoked as a component of the termination process.	No exceptions noted.
	<b>Network</b>			
		Network user access is restricted via role-based security privileges defined within the access control system.	Inspected the network user listing to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Network administrative access is restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul> <p>Network users are authenticated via individually-assigned user accounts and passwords. Networks are configured to enforce password requirements that include:</p> <ul style="list-style-type: none"> <li>• Password length</li> <li>• Complexity</li> </ul> <p>Network account lockout policies are in place that include:</p> <ul style="list-style-type: none"> <li>• Account lockout threshold</li> </ul> <p>Network audit policy configurations are in place that include:</p> <ul style="list-style-type: none"> <li>• Any commands executed on the network</li> </ul>	<p>Inspected the network administrator listing to determine that network administrative access was restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul> <p>Inspected the network configurations policy to determine that network users were authenticated via individually-assigned user accounts and passwords. Networks were configured to enforce password requirements that included:</p> <ul style="list-style-type: none"> <li>• Password length</li> <li>• Complexity</li> </ul> <p>Inspected the network access configuration to determine that network account lockout policies were in place that included:</p> <ul style="list-style-type: none"> <li>• Account lockout threshold</li> </ul> <p>Inspected the network configurations policy and example network log extract to determine that network audit policy configurations were in place that included:</p> <ul style="list-style-type: none"> <li>• Any commands executed on the network</li> </ul>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Alerts are generated to notify network administrators of suspicious activity.	Inspected example network alerts to determine that alerts were generated to notify network administrators of suspicious activity.	No exceptions noted.
	<b>Database</b>			
		<p>Database user access is restricted via role-based security privileges defined within the access control system.</p> <p>Database administrative access is restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• VP of Operations</li> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul>	<p>Inspected the database user listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system.</p> <p>Inspected the database administrator listing and access rights to determine that database administrative access was restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• VP of Operations</li> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Database users are authenticated via individually-assigned user accounts and passwords. Databases are configured to enforce password requirements that include:</p> <ul style="list-style-type: none"> <li>• Minimum password length</li> <li>• Minimum password strength</li> <li>• Uppercase letter</li> <li>• Lowercase letter</li> <li>• Numeric characters</li> </ul> <p>Database account lockout policies are in place that include:</p> <ul style="list-style-type: none"> <li>• Account lockout duration</li> <li>• Account lockout threshold</li> </ul> <p>Database audit policy configurations are in place that include:</p> <ul style="list-style-type: none"> <li>• User updates</li> <li>• Logon events</li> </ul>	<p>Inspected the database authentication settings to determine that database users were authenticated via individually-assigned user accounts and passwords. Networks were configured to enforce password requirements that included:</p> <ul style="list-style-type: none"> <li>• Minimum password length</li> <li>• Minimum password strength</li> <li>• Uppercase letter</li> <li>• Lowercase letter</li> <li>• Numeric characters</li> </ul> <p>Inspected the database account lockout configurations to determine that database account lockout policies were in place that included:</p> <ul style="list-style-type: none"> <li>• Account lockout duration</li> <li>• Account lockout threshold</li> </ul> <p>Inspected the database audit logging policy and example database log extract to determine that database audit policy configurations were in place that included:</p> <ul style="list-style-type: none"> <li>• User updates</li> <li>• Logon events</li> </ul>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Alerts are generated to notify database administrators of suspicious activity.	Inspected the monitoring system configurations, notification configurations and an example alert to determine that alerts were generated to notify database administrators of suspicious activity.	No exceptions noted.
	<b>Application</b>			
		<p>Application user access is restricted via role-based security privileges defined within the access control system.</p> <p>Application administrative access is restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• VP of Operations</li> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul>	<p>Inspected the application user listing to determine that application user access was restricted via role-based security privileges defined within the access control system.</p> <p>Inspected the application administrator listing and access rights to determine that application administrative access was restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• VP of Operations</li> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Application users are authenticated via individually-assigned user accounts and passwords. The application is configured to enforce password requirements that include:</p> <ul style="list-style-type: none"> <li>• Minimum password strength</li> <li>• Letters</li> <li>• Numbers</li> <li>• Numeric characters</li> </ul> <p>Application account lockout policies are in place that include:</p> <ul style="list-style-type: none"> <li>• Account lockout duration</li> <li>• Account lockout threshold</li> <li>• Account lockout counter reset</li> </ul> <p>Application audit policy configurations are in place that include:</p> <ul style="list-style-type: none"> <li>• Account logon events</li> </ul>	<p>Inspected the application authentication settings to determine that application users were authenticated via individually-assigned user accounts and passwords. The application was configured to enforce password requirements that included:</p> <ul style="list-style-type: none"> <li>• Minimum password strength</li> <li>• Letters</li> <li>• Numbers</li> <li>• Numeric characters</li> </ul> <p>Inspected the application account lockout policy to determine that application account lockout policies were in place that included:</p> <ul style="list-style-type: none"> <li>• Account lockout duration</li> <li>• Account lockout threshold</li> <li>• Account lockout counter reset</li> </ul> <p>Inspected the application audit logging policy and example application log extract to determine that application audit policy configurations were in place that included:</p> <ul style="list-style-type: none"> <li>• Account logon events</li> </ul>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>



COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Alerts are generated to notify application administrators of suspicious activity.	Inspected the monitoring system configurations, notification configurations and an example alert to determine that alerts were generated to notify application administrators of suspicious activity.	No exceptions noted.
	<b>Remote Access</b>			
		<p>VPN user access is restricted via role-based security privileges defined within the access control system.</p> <p>The ability to administer VPN access is restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul> <p>VPN users are authenticated via username and password.</p>	<p>Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.</p> <p>Inspected the VPN administrator listing to determine that the ability to administer VPN access was restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul> <p>Inquired of the VP of Operations regarding logging into the VPN to determine that VPN users were authenticated via username and password.</p> <p>Observed a user login to the VPN to determine that VPN users were authenticated via multifactor authentication.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	VPN users are authenticated via multifactor authentication.	<p>Inspected the VPN configurations policy to determine that VPN users were authenticated via username and password.</p> <p>Inquired of the VP of Operations regarding logging into the VPN to determine that VPN users were authenticated via multifactor authentication.</p> <p>Observed a user login to the VPN to determine that VPN users were authenticated via multifactor authentication.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
		Privileged access to sensitive resources is restricted to defined user roles.	Inspected the user access listings and access rights to determine that privileged access to sensitive resources were restricted to defined user roles.	No exceptions noted.
		Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.	Inspected the information security policy to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
		Logical and physical access to systems is granted to an employee as a component of the hiring process.	Inspected the hiring procedures, hiring checklist and access request for a sample of new hires to determine that logical and physical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	Logical and physical access to systems is revoked as a component of the termination process.	Inspected the badge access listing, network user listing, termination checklist and email requesting the access removal for a sample of terminated employees to determine that logical and physical access to systems was revoked as a component of the termination process.	No exceptions noted.
		Account sharing is prohibited by policy.	Inspected the information security policy to determine that account sharing was prohibited by policy.	No exceptions noted.
		Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.	Inspected the information security policy to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
		Logical and physical access to systems is granted to an employee as a component of the hiring process.	Inspected the hiring procedures, hiring checklist and access request for a sample of new hires to determine that logical and physical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.
	<b>Network</b>			
		Network user access is restricted via role-based security privileges defined within the access control system.	Inspected the network user listing to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Network administrative access is restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul> <p>Network users are authenticated via individually-assigned user accounts and passwords. Networks are configured to enforce password requirements that include:</p> <ul style="list-style-type: none"> <li>• Password length</li> <li>• Complexity</li> </ul> <p>Network account lockout policies are in place that include:</p> <ul style="list-style-type: none"> <li>• Account lockout threshold</li> </ul> <p>Network audit policy configurations are in place that include:</p> <ul style="list-style-type: none"> <li>• Any commands executed on the network</li> </ul>	<p>Inspected the network administrator listing to determine that network administrative access was restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul> <p>Inspected the network configurations policy to determine that network users were authenticated via individually-assigned user accounts and passwords. Networks were configured to enforce password requirements that included:</p> <ul style="list-style-type: none"> <li>• Password length</li> <li>• Complexity</li> </ul> <p>Inspected the network access configuration to determine that network account lockout policies were in place that included:</p> <ul style="list-style-type: none"> <li>• Account lockout threshold</li> </ul> <p>Inspected the network configurations policy and example network log extract to determine that network audit policy configurations were in place that included:</p> <ul style="list-style-type: none"> <li>• Any commands executed on the network</li> </ul>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Alerts are generated to notify network administrators of suspicious activity.	Inspected example network alerts to determine that alerts were generated to notify network administrators of suspicious activity.	No exceptions noted.
	<b>Application</b>			
		<p>Application user access is restricted via role-based security privileges defined within the access control system.</p> <p>Application administrative access is restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• VP of Operations</li> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul>	<p>Inspected the application user listing to determine that application user access was restricted via role-based security privileges defined within the access control system.</p> <p>Inspected the application administrator listing and access rights to determine that application administrative access was restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• VP of Operations</li> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Application users are authenticated via individually-assigned user accounts and passwords. The application is configured to enforce password requirements that include:</p> <ul style="list-style-type: none"> <li>• Minimum password strength</li> <li>• Letters</li> <li>• Numbers</li> <li>• Numeric characters</li> </ul> <p>Application account lockout policies are in place that include:</p> <ul style="list-style-type: none"> <li>• Account lockout duration</li> <li>• Account lockout threshold</li> <li>• Account lockout counter reset</li> </ul> <p>Application audit policy configurations are in place that include:</p> <ul style="list-style-type: none"> <li>• Account logon events</li> </ul>	<p>Inspected the application authentication settings to determine that application users were authenticated via individually-assigned user accounts and passwords. The application was configured to enforce password requirements that included:</p> <ul style="list-style-type: none"> <li>• Minimum password strength</li> <li>• Letters</li> <li>• Numbers</li> <li>• Numeric characters</li> </ul> <p>Inspected the application account lockout policy to determine that application account lockout policies were in place that included:</p> <ul style="list-style-type: none"> <li>• Account lockout duration</li> <li>• Account lockout threshold</li> <li>• Account lockout counter reset</li> </ul> <p>Inspected the application audit logging policy and example application log extract to determine that application audit policy configurations were in place that included:</p> <ul style="list-style-type: none"> <li>• Account logon events</li> </ul>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Alerts are generated to notify application administrators of suspicious activity.	Inspected the monitoring system configurations, notification configurations and an example alert to determine that alerts were generated to notify application administrators of suspicious activity.	No exceptions noted.
	<b>Remote Access</b>			
		<p>VPN user access is restricted via role-based security privileges defined within the access control system.</p> <p>The ability to administer VPN access is restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul> <p>VPN users are authenticated via username and password.</p>	<p>Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.</p> <p>Inspected the VPN administrator listing to determine that the ability to administer VPN access was restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul> <p>Inquired of the VP of Operations regarding logging into the VPN to determine that VPN users were authenticated via username and password.</p> <p>Observed a user login to the VPN to determine that VPN users were authenticated via multifactor authentication.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>





**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	<p>Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.</p> <p>Logical and physical access to systems is granted to an employee as a component of the hiring process.</p> <p>Logical and physical access to systems is revoked as a component of the termination process.</p>	<p>Inspected the VPN configuration policy and SSL certificates to determine that users can only access the system remotely through the use of the VPN, secure sockets layer (SSL), or other encrypted communication system.</p> <p>Inspected the information security policy to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.</p> <p>Inspected the hiring procedures, hiring checklist and access request for a sample of new hires to determine that logical and physical access to systems was granted to an employee as a component of the hiring process.</p> <p>Inspected the badge access listing, network user listing, termination checklist and email requesting the access removal for a sample of terminated employees to determine that logical and physical access to systems was revoked as a component of the termination process.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	<p>Policies and procedures are in place to guide personnel in physical security activities.</p> <p>A badge access system controls access to and within the office facility.</p> <p>Personnel are assigned to predefined badge access security zones based on job responsibilities.</p> <p>Physical access to systems is granted to an employee as a component of the hiring process.</p>	<p>Inspected the physical security policy to determine that policies and procedures were in place to guide personnel in physical security activities.</p> <p>Observed the presence of badge access points within the facility to determine that a badge access system controlled access to and within the office facility.</p> <p>Inspected the badge access listing and zone definitions to determine that a badge access system controlled access to and within the office facility.</p> <p>Inspected the badge access listing and zone definitions to determine that personnel were assigned to predefined badge access security zones based on job responsibilities.</p> <p>Inspected the hiring procedures, hiring checklist and access request for a sample of new hires to determine that physical access to systems was granted to an employee as a component of the hiring process.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Access to the data center is restricted to badge access cards assigned to appropriate personnel.	Inspected the badge access listing and zone definitions to determine that access to the data center was restricted to badge access cards assigned to appropriate personnel.	No exceptions noted.
		A video surveillance system is in place with footage retained for at least 30 days.	Observed the video surveillance system throughout the facility to determine that a video surveillance system was in place with footage retained for at least 30 days.	No exceptions noted.
		Visitors to the facility and server room are required to be escorted by an authorized employee.	Inspected the oldest retained video surveillance footage to determine that a video surveillance system was in place with footage retained for at least 30 days.	No exceptions noted.
			Observed the visitor process throughout the facility to determine that visitors to the facility and server room were required to be escorted by an authorized employee.	No exceptions noted.
			Inspected the physical security policy to determine that visitors to the facility and server room were required to be escorted by an authorized employee.	No exceptions noted.

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Visitors to the facility and server room are required to sign a visitor log prior upon arrival.</p> <p>Physical access privileges to the corporate office facility are revoked as a component of the termination process.</p> <p>User access to the badge access system is reviewed on an annual basis.</p> <p>Additional controls are implemented by the subservice organization. Refer to the system description of this report for additional details.</p>	<p>Observed the visitor process throughout the facility to determine that visitors to the facility and server room were required to sign a visitor log prior upon arrival.</p> <p>Inspected the visitor logs to the facility and server room for a sample of months to determine that visitors to the facility and server room were required to sign a visitor log prior upon arrival.</p> <p>Inspected the badge access listing, termination checklist and email requesting the access removal for a sample of terminated employees to determine that physical access privileges to the corporate office facility are revoked as a component of the termination process.</p> <p>Inspected the most recent badge access review to determine that user access to the badge access system was reviewed on an annual basis.</p> <p>Not Applicable.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>Not Applicable.</p>

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.6	Logical access security measures have been implemented to protect against security, availability, and confidentiality threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.	A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the firewall rule set to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the firewall rule set to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority.	Inspected the SSL certificate to determine that server certificate-based authentication was used as part of the SSL/TLS encryption with a trusted certificate authority.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inquired of the VP of Operations regarding logging into the VPN to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Observed a user login to the VPN to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security, availability, and confidentiality.	An intrusion detection system (IDS) is utilized to analyze network events and report possible or actual network security breaches.	Inspected the VPN configuration policy and SSL certificates to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS dashboard to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		VPN, SSL, secure file transfer program (SFTP), and other encryption technologies are used for defined points of connectivity.	Inspected an example intrusion alert and example IDS log extract to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		Backup media is stored in an encrypted format.	Inspected the VPN configuration policy and SSL certificate to determine that encryption technologies are used for defined points of connectivity.	No exceptions noted.
		The ability to recall backed up data is restricted to authorized personnel.	Inspected the backup encryption settings to determine that backup media was stored in an encrypted format.	No exceptions noted.
			Inspected the listing of users with the ability to recall backup media to determine that the ability to recall backed up data was restricted to authorized personnel.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	The ability to migrate changes into the production environment is restricted to authorized and appropriate users.	Inspected the listing of users with access to the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
		A file integrity monitor is in place to ensure only authorized changes are deployed into the production environment.	Inspected the file integrity monitoring configurations to determine that a file integrity monitor was in place to ensure only authorized changes were deployed into the production environment.	No exceptions noted.
		The file integrity monitoring application is configured to notify appropriate personnel via e-mail alert when a change to the production application code files is detected.	Inspected the file integrity monitoring configurations and an example alert to determine that the file integrity monitoring application was configured to notify appropriate personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		An intrusion detection system (IDS) is utilized to analyze network events and report possible or actual network security breaches.	Inspected the IDS dashboard to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected an example intrusion alert and example IDS log extract to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC5.0	Common Criteria Related to Logical and Physical Access Controls			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.</p> <p>The antivirus software is configured to scan workstations on a bi-weekly basis.</p>	<p>Inspected the antivirus settings to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.</p> <p>Inspected the antivirus scan settings to determine that the antivirus software was configured to scan workstations on a bi-weekly basis.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>



**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC6.0	Common Criteria Related to System Operations			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1	<p>Vulnerabilities of system components to security, availability, and confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.</p>	<p>Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.</p> <p>The monitoring software is configured to alert appropriate personnel when thresholds have been exceeded.</p> <p>Documented incident response policies and procedures are in place to guide personnel in the event of an incident.</p> <p>An automated backup system is utilized to perform scheduled system backups.</p>	<p>Inspected the monitoring system configurations, notification configurations and an example alert to determine that monitoring software was used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.</p> <p>Inspected the monitoring system configurations, notification configurations and an example alert to determine that the monitoring software was configured to alert appropriate personnel when thresholds had been exceeded.</p> <p>Inspected the emergency action plan to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident.</p> <p>Inspected the backup system configurations to determine that an automated backup system was utilized to perform scheduled system backups.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC6.0	Common Criteria Related to System Operations			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>IT personnel monitor the success or failure of backups, and are notified of backup job status via email notifications.</p> <p>Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the anti-virus software.</p> <p>The antivirus software is configured to scan workstations on a bi-weekly basis.</p> <p>A firewall is in place to filter unauthorized inbound network traffic from the internet.</p>	<p>Inquired of the CTO regarding the monitoring of system backups to determine that IT personnel monitored the success or failure of backups, and were notified of backup job status via email notifications.</p> <p>Inspected the backup notification configurations and an example backup status alert to determine that IT personnel monitored the success or failure of backups, and were notified of backup job status via email notifications.</p> <p>Inspected the antivirus settings to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the anti-virus software.</p> <p>Inspected the antivirus scan settings to determine that the antivirus software was configured to scan workstations on a bi-weekly basis.</p> <p>Inspected the firewall rule set to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC6.0	Common Criteria Related to System Operations			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2	Security, availability, and confidentiality incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.	The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the firewall rule set to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An intrusion detection system (IDS) is utilized to analyze network events and report possible or actual network security breaches.	Inspected the IDS dashboard to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected an example intrusion alert and example IDS log extract to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	Inspected the emergency action plan to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident.	No exceptions noted.
		A ticket tracking application is utilized to track and respond to incidents.	Inspected the tickets for a sample of incidents to determine that a ticket tracking application was utilized to track and respond to incidents.	No exceptions noted.
Resolution of events is communicated to users within the corresponding ticket.	Inspected the tickets for a sample of incidents to determine that the resolution of events was communicated to users within the corresponding ticket.	No exceptions noted.		

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC6.0	Common Criteria Related to System Operations			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Change management requests are opened for events that require permanent fixes.</p> <p>Entity policies include probation, suspension, and termination as potential sanctions for employee misconduct.</p>	<p>Inspected the tickets for a sample of application changes and a sample of infrastructure changes to determine that change management requests were opened for events that require permanent fixes.</p> <p>Inspected the employee handbook to determine that entity policies include probation, suspension, and termination as potential sanctions for employee misconduct.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC7.0	Common Criteria Related to Change Management			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1	The entity's commitments and system requirements, as they relate to security, availability, and confidentiality, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	Documented change control policies and procedures are in place to guide personnel in the handling system changes.	Inspected the development policy to determine that documented change control procedures were in place to guide personnel in the handling of system changes.	No exceptions noted.
		System changes are authorized, tested, and approved by management prior to implementation.	Inspected the tickets for a sample of application changes and a sample of infrastructure changes to determine that system changes were authorized, tested, and approved by management prior to implementation.	No exceptions noted.
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	Management has defined a formal risk management process that specifies the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk assessment policy and the most recent risk assessment to determine that management had defined a formal risk management process that specified the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
		A formal risk assessment is performed on an annual basis to identify threats that could impair systems security, availability, and confidentiality commitments and requirements.	Inspected the most recent risk assessment to determine that a formal risk assessment was performed on an annual basis to identify threats that could impair systems security, availability, and confidentiality commitments and requirements.	No exceptions noted.

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC7.0	Common Criteria Related to Change Management			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Identified risks are rated using a risk evaluation process and rating are reviewed by management.</p> <p>Management develops risk mitigation strategies to address risks identified during the risk assessment process.</p> <p>The entity has implemented daily, weekly, and monthly risk assessment checklists to be completed by facility personnel to identify threats to the security and availability of the system.</p>	<p>Inspected the risk assessment policy and the most recent risk assessment to determine that identified risks were rated using a risk evaluation process and rating were reviewed by management.</p> <p>Inspected the risk assessment policy and the most recent risk assessment to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.</p> <p>Inquired of the VP of Operations regarding risk assessment checklists to determine that the entity had implemented daily, weekly, and monthly risk assessment checklists to be completed by facility personnel to identify threats to the security and availability of the system.</p> <p>Inspected the daily checklist for a sample of days, the weekly checklist for a sample of weeks, and the monthly checklist for a sample of months to determine that the entity had implemented daily, weekly, and monthly risk assessment checklists to be completed by facility personnel to identify threats to the security and availability of the system.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC7.0	Common Criteria Related to Change Management			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	Documented escalation procedures for reporting security incidents are in place to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the emergency action plan to determine that documented escalation procedures for reporting security incidents were in place to guide users in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inspected the tickets for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security, availability, and confidentiality commitments and system requirements.	Documented change control policies and procedures are in place to guide personnel in the handling system changes.	Inspected the development policy to determine that documented change control procedures were in place to guide personnel in the handling of system changes.	No exceptions noted.
		System change requests are documented and tracked in a ticketing system.	Inspected the tickets for a sample of application changes and a sample of infrastructure changes to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC7.0	Common Criteria Related to Change Management			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>System changes are tested prior to implementation. Types of testing performed depend on the nature of the change.</p> <p>Changes are approved by management prior to implementation.</p> <p>Changes are communicated to both internal and external users.</p> <p>Development and test environments are physically and logically separated from the production environment.</p>	<p>Inspected the tickets for a sample of application changes and a sample of infrastructure changes to determine that system changes were tested prior to implementation. Types of testing performed depended on the nature of the change.</p> <p>Inspected the tickets for a sample of application changes and a sample of infrastructure changes to determine that changes were approved by management prior to implementation.</p> <p>Inspected the email communication and tickets for a sample of application changes and infrastructure changes to determine that changes were communicated to both internal and external users.</p> <p>Inquired of the VP of Operations regarding separate environments to determine that development and test environments were physically and logically separated from the production environment.</p> <p>Observed the separate environments to determine that development and test environments were physically and logically separated from the production environment.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>



**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC7.0	Common Criteria Related to Change Management			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Access to implement changes in the production environment is restricted to authorized IT personnel.</p> <p>Prior code is held in the repository for rollback capability in the event that a system change does not function as designed.</p> <p>The ability to migrate changes into the production environment is restricted to authorized and appropriate users.</p> <p>A file integrity monitor is in place to ensure only authorized changes are deployed into the production environment.</p>	<p>Inspected the listing of users with access to the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel.</p> <p>Inspected the version control software to determine that prior code was held in the repository for rollback capability in the event that a system change did not function as designed.</p> <p>Inspected the listing of users with access to the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.</p> <p>Inspected the file integrity monitoring configurations and an example alert to determine that a file integrity monitor was in place to ensure only authorized changes were deployed into the production environment.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES**

CC7.0	Common Criteria Related to Change Management			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The file integrity monitoring application is configured to notify appropriate personnel via e-mail alert when a change to the production application code files is detected.	Inspected the file integrity monitoring configurations and an example alert to determine that the file integrity monitoring application was configured to notify appropriate personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.

A1.0	AVAILABILITY CRITERIA			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.	Enterprise monitoring software is utilized to notify personnel when predefined thresholds are exceeded on production systems.	Inspected the monitoring system configurations, notification configurations and an example alert to determine that enterprise monitoring software was utilized to notify personnel when predefined thresholds were exceeded on production systems.	No exceptions noted.
Processing capacity is monitored 24x7x365.		Inspected the monitoring system configurations, notification configurations and an example alert to determine that processing capacity was monitored 24x7x365.	No exceptions noted.	
Future processing demand is forecasted and compared to scheduled capacity on an annual basis.		Inspected the operations strategy to determine that future processing demand is forecasted and compared to scheduled capacity on an annual basis.	No exceptions noted.	
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.	Fire detection and prevention systems are present throughout the facility including smoke detection devices, hand held fire extinguishers, and pre-action dry pipe fire suppression.	Observed the office facility/data center facility to determine that fire detection and prevention systems were present throughout the facility including smoke detection devices, hand held fire extinguishers, and pre-action dry pipe fire suppression.	No exceptions noted.
Handheld fire extinguishers are inspected on an annual basis to ensure that the pressure is within the recommended levels.		Inspected the fire extinguisher inspection tags to determine that handheld fire extinguishers were inspected on an annual basis to ensure that the pressure was within the recommended levels.	No exceptions noted.	

A1.0	AVAILABILITY CRITERIA			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>The pre-action dry pipe fire suppression systems are tested and inspected by a third-party provider on an annual basis.</p>	<p>Inspected the pre-action dry pipe suppression system inspection report to determine that the pre-action dry pipe fire suppression systems were tested and inspected by a third-party provider on an annual basis.</p>	<p>No exceptions noted.</p>
		<p>An uninterruptable power supply (UPS) is in place to provide power to critical infrastructure equipment in the event of a temporary power loss or power surge.</p>	<p>Observed the UPS units to determine that a UPS was in place to provide power to critical infrastructure equipment in the event of a temporary power loss or power surge.</p>	<p>No exceptions noted.</p>
		<p>The UPS units are inspected for any alarms on a daily basis.</p>	<p>Inquired of the VP of Operations regarding UPS units to determine that the UPS units were inspected and maintained by a third-party on a daily basis.</p>	<p>No exceptions noted.</p>
			<p>Observed the UPS inspection report for a sample of days to determine that the UPS units were inspected and maintained by a third-party on a daily basis.</p>	<p>No exceptions noted.</p>
		<p>The UPS units' KVA readings and battery time are inspected on a weekly basis.</p>	<p>Inquired of the VP of Operations regarding UPS units to determine that the UPS units' KVA readings and battery time were inspected on a weekly basis.</p>	<p>No exceptions noted.</p>
			<p>Observed the UPS inspection report for a sample of weeks to determine that the UPS units' KVA readings and battery time were inspected on a weekly basis.</p>	<p>No exceptions noted.</p>

A1.0	AVAILABILITY CRITERIA			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Generators fueled by diesel fuel are in place to provide power to the data center in the event of an extended power outage.</p> <p>The generators are tested on an annual basis.</p> <p>Preventive maintenance inspections and service is performed on the generators on a quarterly basis.</p> <p>Temperature and humidity sensor systems are in place in the facility that notifies authorized personnel via email distribution group of readings outside of the defined parameters.</p>	<p>Observed the onsite generator to determine that generators fueled by diesel fuel were in place to provide power to the data center in the event of an extended power outage.</p> <p>Inspected the most recent generator testing results to determine that the generators were tested on an annual basis.</p> <p>Inspected the generator inspection report for a sample of quarters to determine that preventive maintenance inspections and service was performed on the generators on a quarterly basis.</p> <p>Observed the environmental monitoring system to determine that temperature and humidity sensor systems were in place in the facility that notified authorized personnel via email distribution group of readings outside of the defined parameters.</p> <p>Inspected the environmental monitoring system dashboard and notification configurations to determine that temperature and humidity sensor systems were in place in the facility that notified authorized personnel via email distribution group of readings outside of the defined parameters.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

A1.0	AVAILABILITY CRITERIA			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>The facility is equipped with multiple HVAC units that provide redundancy in the event of one unit's failure.</p>	<p>Observed the onsite HVAC units to determine that the facility was equipped with multiple HVAC units that provided redundancy in the event of one unit's failure.</p>	<p>No exceptions noted.</p>
		<p>The HVAC units are inspected and maintained by a third-party on a quarterly basis.</p>	<p>Inspected the HVAC inspection report for a sample of quarters to determine that the HVAC units were inspected and maintained by a third-party on a quarterly basis.</p>	<p>No exceptions noted.</p>
		<p>The HVAC units are inspected for any alarms and the temperature readings are taken on a daily basis.</p>	<p>Inquired of the VP of Operations regarding HVAC units to determine that the HVAC units were inspected for any alarms and the temperature readings were taken on a daily basis.</p>	<p>No exceptions noted.</p>
		<p>The HVAC units are inspected for any alarms and the temperature readings are taken on a daily basis.</p>	<p>Observed the HVAC inspection report for a sample of days to determine that the HVAC units were inspected for any alarms and the temperature readings were taken on a daily basis.</p>	<p>No exceptions noted.</p>
		<p>The HVAC units gas and oil level of compressors and vibrations within each unit are inspected on a weekly basis.</p>	<p>Inquired of the VP of Operations regarding HVAC units to determine that the HVAC units gas and oil level of compressors and vibrations within each unit were inspected on a weekly basis.</p>	<p>No exceptions noted.</p>
		<p>The HVAC units gas and oil level of compressors and vibrations within each unit are inspected on a weekly basis.</p>	<p>Inspected the HVAC inspection report for a sample of weeks to determine that the HVAC units gas and oil level of compressors and vibrations within each unit were inspected on a weekly basis.</p>	<p>No exceptions noted.</p>

A1.0	AVAILABILITY CRITERIA			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Production equipment within the colocation areas of the data center facilities is placed on racks to protect infrastructure from localized flooding.	Observed the racks housing the equipment to determine that production equipment within the colocation areas of the data center facilities was placed on racks to protect infrastructure from localized flooding.	No exceptions noted.
		The data center facilities are equipped with raised flooring to elevate equipment and help facilitate cooling.	Observed the raised floors within the colocation center to determine that the data center facilities were equipped with raised flooring to elevate equipment and help facilitate cooling.	No exceptions noted.
		The data center facilities are equipped with leak detection systems to detect water in the event of a flood or water leakage.	Observed the leak detection devices to determine that the data center facilities were equipped with leak detection systems to detect water in the event of a flood or water leakage.	No exceptions noted.
			Inspected the environmental monitoring system dashboard and notification configurations to determine that the data center facilities were equipped with leak detection systems to detect water in the event of a flood or water leakage.	No exceptions noted.
		IT personnel monitor the success or failure of backups, and are notified of backup job status via email notifications.	Inquired of the CTO regarding the monitoring of system backups to determine that IT personnel monitored the success or failure of backups, and were notified of backup job status via email notifications.	No exceptions noted.

A1.0	AVAILABILITY CRITERIA			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Restore tests are performed on backed up data upon notification of a failed backup job.</p> <p>Backup media is stored in an encrypted format.</p> <p>The ability to recall backed up data is restricted to authorized personnel.</p> <p>A disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.</p> <p>The disaster recovery plan is tested on an annual basis.</p>	<p>Inspected the backup notification configurations and an example backup status alert to determine that IT personnel monitored the success or failure of backups, and were notified of backup job status via email notifications.</p> <p>Inspected an example backup restore to determine that restore tests were performed on backed up data upon notification of a failed backup job.</p> <p>Inspected the backup encryption settings to determine that backup media was stored in an encrypted format.</p> <p>Inspected the listing of users with the ability to recall backup media to determine that the ability to recall backed up data was restricted to authorized personnel.</p> <p>Inspected the disaster recovery plan to determine that a disaster recovery plan was documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.</p> <p>Inspected the most recent disaster recovery test results to determine that the disaster recovery plan was tested on an annual basis.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>



A1.0	AVAILABILITY CRITERIA			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.3	Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.	<p>A disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.</p> <p>The disaster recovery plan is tested on an annual basis.</p>	<p>Inspected the disaster recovery plan to determine that a disaster recovery plan was documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.</p> <p>Inspected the most recent disaster recovery test results to determine that the disaster recovery plan was tested on an annual basis.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

C1.0		CONFIDENTIALITY CRITERIA		
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.1	Confidential information is protected during the system design, development, testing, implementation, and change processes to meet the entity's confidentiality commitments and system requirements.	Mantraps or other physical devices are used for controlling accessing highly sensitive facilities.	Inquired of the VP of Operations regarding physical security to determine that mantraps or other physical devices were used for controlling accessing highly sensitive facilities.  Observed mantraps at the facility to determine that mantraps or other physical devices were used for controlling accessing highly sensitive facilities.	No exceptions noted.  No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in the handling system changes.	Inspected the development policy to determine that documented change control procedures were in place to guide personnel in the handling of system changes.	No exceptions noted.
C1.2	Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity's confidentiality commitments and system requirements.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.	Inspected the information security policy to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
		Logical and physical access to systems is granted to an employee as a component of the hiring process.	Inspected the hiring procedures, hiring checklist and access request for a sample of new hires to determine that logical and physical access to systems was granted to an employee as a component of the hiring process.	No exceptions noted.

C1.0	CONFIDENTIALITY CRITERIA			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Logical and physical access to systems is revoked as a component of the termination process.</p>	<p>Inspected the badge access listing, network user listing termination checklist and email requesting the access removal for a sample of terminated employees to determine that logical and physical access to systems was revoked as a component of the termination process.</p>	<p>No exceptions noted.</p>
	<b>Network</b>			
		<p>Network user access is restricted via role-based security privileges defined within the access control system.</p> <p>Network administrative access is restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul> <p>Network users are authenticated via individually-assigned user accounts and passwords. Networks are configured to enforce password requirements that include:</p> <ul style="list-style-type: none"> <li>• Password length</li> <li>• Complexity</li> </ul>	<p>Inspected the network user listing to determine that network user access was restricted via role-based security privileges defined within the access control system.</p> <p>Inspected the network administrator listing to determine that network administrative access was restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul> <p>Inspected the network configurations policy to determine that network users were authenticated via individually-assigned user accounts and passwords. Networks were configured to enforce password requirements that included:</p> <ul style="list-style-type: none"> <li>• Password length</li> <li>• Complexity</li> </ul>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

C1.0	CONFIDENTIALITY CRITERIA			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Network account lockout policies are in place that include:</p> <ul style="list-style-type: none"> <li>• Account lockout threshold</li> </ul> <p>Network audit policy configurations are in place that include:</p> <ul style="list-style-type: none"> <li>• Any commands executed on the network</li> </ul> <p>Alerts are generated to notify network administrators of suspicious activity.</p>	<p>Inspected the network access configuration to determine that network account lockout policies were in place that included:</p> <ul style="list-style-type: none"> <li>• Account lockout threshold</li> </ul> <p>Inspected the network configurations policy and example network log extract to determine that network audit policy configurations were in place that included:</p> <ul style="list-style-type: none"> <li>• Any commands executed on the network</li> </ul> <p>Inspected example network alerts to determine that alerts were generated to notify network administrators of suspicious activity.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
	<b>Database</b>			
		<p>Database user access is restricted via role-based security privileges defined within the access control system.</p>	<p>Inspected the database user listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system.</p>	<p>No exceptions noted.</p>

C1.0	CONFIDENTIALITY CRITERIA			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Database administrative access is restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• VP of Operations</li> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul> <p>Database users are authenticated via individually-assigned user accounts and passwords. Databases are configured to enforce password requirements that include:</p> <ul style="list-style-type: none"> <li>• Minimum password length</li> <li>• Minimum password strength</li> <li>• Uppercase letter</li> <li>• Lowercase letter</li> <li>• Numeric characters</li> </ul> <p>Database account lockout policies are in place that include:</p> <ul style="list-style-type: none"> <li>• Account lockout duration</li> <li>• Account lockout threshold</li> </ul>	<p>Inspected the database administrator listing and access rights to determine that database administrative access was restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• VP of Operations</li> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul> <p>Inspected the database authentication settings to determine that database users were authenticated via individually-assigned user accounts and passwords. Networks were configured to enforce password requirements that included:</p> <ul style="list-style-type: none"> <li>• Minimum password length</li> <li>• Minimum password strength</li> <li>• Uppercase letter</li> <li>• Lowercase letter</li> <li>• Numeric characters</li> </ul> <p>Inspected the database account lockout configurations to determine that database account lockout policies were in place that included:</p> <ul style="list-style-type: none"> <li>• Account lockout duration</li> <li>• Account lockout threshold</li> </ul>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

C1.0	CONFIDENTIALITY CRITERIA			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Database audit policy configurations are in place that include:</p> <ul style="list-style-type: none"> <li>• User updates</li> <li>• Logon events</li> </ul> <p>Alerts are generated to notify database administrators of suspicious activity.</p>	<p>Inspected the database audit logging policy and example database log extract to determine that database audit policy configurations were in place that included:</p> <ul style="list-style-type: none"> <li>• User updates</li> <li>• Logon events</li> </ul> <p>Inspected the monitoring system configurations, notification configurations and an example alert to determine that alerts were generated to notify database administrators of suspicious activity.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
	<b>Application</b>			
		<p>Application user access is restricted via role-based security privileges defined within the access control system.</p> <p>Application administrative access is restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• VP of Operations</li> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul>	<p>Inspected the application user listing to determine that application user access was restricted via role-based security privileges defined within the access control system.</p> <p>Inspected the application administrator listing and access rights to determine that application administrative access was restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• VP of Operations</li> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

C1.0	CONFIDENTIALITY CRITERIA			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Application users are authenticated via individually-assigned user accounts and passwords. The application is configured to enforce password requirements that include:</p> <ul style="list-style-type: none"> <li>• Minimum password strength</li> <li>• Letters</li> <li>• Numbers</li> <li>• Numeric characters</li> </ul> <p>Application account lockout policies are in place that include:</p> <ul style="list-style-type: none"> <li>• Account lockout duration</li> <li>• Account lockout threshold</li> <li>• Account lockout counter reset</li> </ul> <p>Application audit policy configurations are in place that include:</p> <ul style="list-style-type: none"> <li>• Account logon events</li> </ul>	<p>Inspected the application authentication settings to determine that application users were authenticated via individually-assigned user accounts and passwords. The application was configured to enforce password requirements that included:</p> <ul style="list-style-type: none"> <li>• Minimum password strength</li> <li>• Letters</li> <li>• Numbers</li> <li>• Numeric characters</li> </ul> <p>Inspected the application account lockout policy to determine that application account lockout policies were in place that included:</p> <ul style="list-style-type: none"> <li>• Account lockout duration</li> <li>• Account lockout threshold</li> <li>• Account lockout counter reset</li> </ul> <p>Inspected the application audit logging policy and example application log extract to determine that application audit policy configurations were in place that included:</p> <ul style="list-style-type: none"> <li>• Account logon events</li> </ul>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

C1.0	CONFIDENTIALITY CRITERIA			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Alerts are generated to notify application administrators of suspicious activity.	Inspected the monitoring system configurations, notification configurations and an example alert to determine that alerts were generated to notify application administrators of suspicious activity.	No exceptions noted.
	<b>Remote Access</b>			
		<p>VPN user access is restricted via role based security privileges defined within the access control system.</p> <p>The ability to administer VPN access is restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul> <p>VPN users are authenticated via username and password.</p>	<p>Inspected the VPN user listing to determine that VPN user access was restricted via role based security privileges defined within the access control system.</p> <p>Inspected the VPN administrator listing to determine that the ability to administer VPN access was restricted to user accounts accessible by the following personnel:</p> <ul style="list-style-type: none"> <li>• CTO</li> <li>• Manager of Operations, EU</li> </ul> <p>Inquired of the VP of Operations regarding logging into the VPN to determine that VPN users were authenticated via username and password.</p> <p>Observed a user login to the VPN to determine that VPN users were authenticated via multifactor authentication.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>



C1.0	CONFIDENTIALITY CRITERIA			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>VPN users are authenticated via multifactor authentication.</p> <p>Privileged access to sensitive resources is restricted to defined user roles.</p>	<p>Inspected the VPN configurations policy to determine that VPN users were authenticated via username and password.</p> <p>Inquired of the VP of Operations regarding logging into the VPN to determine that VPN users were authenticated via multifactor authentication.</p> <p>Observed a user login to the VPN to determine that VPN users were authenticated via multifactor authentication.</p> <p>Inspected the user access listings and access rights to determine that privileged access to sensitive resources were restricted to defined user roles.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
	<b>Physical Access</b>			
		Confidential data output from the system is marked and maintained per confidentiality practices.	Inspected the confidentiality policies to determine that confidential data output from the system was marked and maintained per confidentiality practices.	No exceptions noted.
	<b>Training</b>			
		Awareness training is provided to personnel around the policy and usage of personal information.	Inspected the training materials and completed training for a sample of current employees to determine that awareness training was provided to personnel around the policy and usage of personal information.	No exceptions noted.

C1.0	CONFIDENTIALITY CRITERIA			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.3	Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity's confidentiality commitments and system requirements.	<p>Application security restricts output to approved roles or user IDs.</p> <p>Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority.</p> <p>Transmission of digital output beyond the boundary of the system occurs through the use authorized software supporting the AES.</p> <p>Logical access to stored data is restricted to application and database administrators.</p> <p>Use of removable media is prohibited by policy.</p> <p>VPN users are authenticated via username and password.</p>	<p>Inspected application authentication settings to determine that application security restricted output to approved roles or user IDs.</p> <p>Inspected the SSL certificate to determine that server certificate-based authentication was used as part of the SSL/TLS encryption with a trusted certificate authority.</p> <p>Inspected file encryption configurations to determine that transmission of digital output beyond the boundary of the system occurred through the use authorized software supporting the AES.</p> <p>Inspected the database and application administrator listings to determine that logical access to stored data was restricted to application and database administrators.</p> <p>Inspected the IT security and acceptable use policy to determine that the use of removable media was prohibited by policy except when authorized by management.</p> <p>Inquired of the VP of Operations regarding logging into the VPN to determine that VPN users were authenticated via username and password.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

C1.0	CONFIDENTIALITY CRITERIA			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			<p>Observed a user login to the VPN to determine that VPN users were authenticated via multifactor authentication.</p> <p>Inspected the VPN configurations policy to determine that VPN users were authenticated via username and password.</p> <p>Inquired of the VP of Operations regarding logging into the VPN to determine that VPN users were authenticated via multifactor authentication.</p> <p>Observed a user login to the VPN to determine that VPN users were authenticated via multifactor authentication.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
C1.4	The entity obtains confidentiality commitments that are consistent with the entity's confidentiality system requirements from vendors and other third parties whose products and services are part of the system and have access to confidential information.	VPN users are authenticated via multifactor authentication.	Security and confidentiality commitments regarding the system are included in related party and vendor specific service level agreements.	No exceptions noted.
C1.5	Compliance with the entity's confidentiality commitments and system requirements by vendors and others third parties whose products and services are part of the system is assessed on a periodic and as-needed basis, and corrective action is taken, if necessary.	Related party and vendor systems are subject to review as part of the vendor risk management process.	Inspected the company website and the contract for a sample of vendors to determine that security and confidentiality commitments regarding the system were included in related party and vendor specific service level agreements.	No exceptions noted.
			Inspected the most recently completed vendor risk assessment to determine that related party and vendor systems were subject to review as part of the vendor risk management process.	No exceptions noted.



C1.0	CONFIDENTIALITY CRITERIA			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.8	The entity disposes of confidential information to meet the entity's confidentiality commitments and system requirements.	Confidential information is maintained in locations restricted to those authorized to access.	Inspected the network, database and application administrator user listings to determine that confidential information was maintained in locations restricted to those authorized to access.	No exceptions noted.
		The entity establishes written policies related to the disposal of the confidential information it maintains.	Inspected the data retention and disposal policy to determine that the entity established written policies related to the disposal of the confidential information it maintained.	No exceptions noted.
		The entity purges confidential data stored on backup tapes and backup drives, per a defined schedule.	Inspected the data retention and disposal policy to determine that the entity purged confidential data stored on backup tapes and backup drives, per a defined schedule.	No exceptions noted.