



Leaseweb Canada

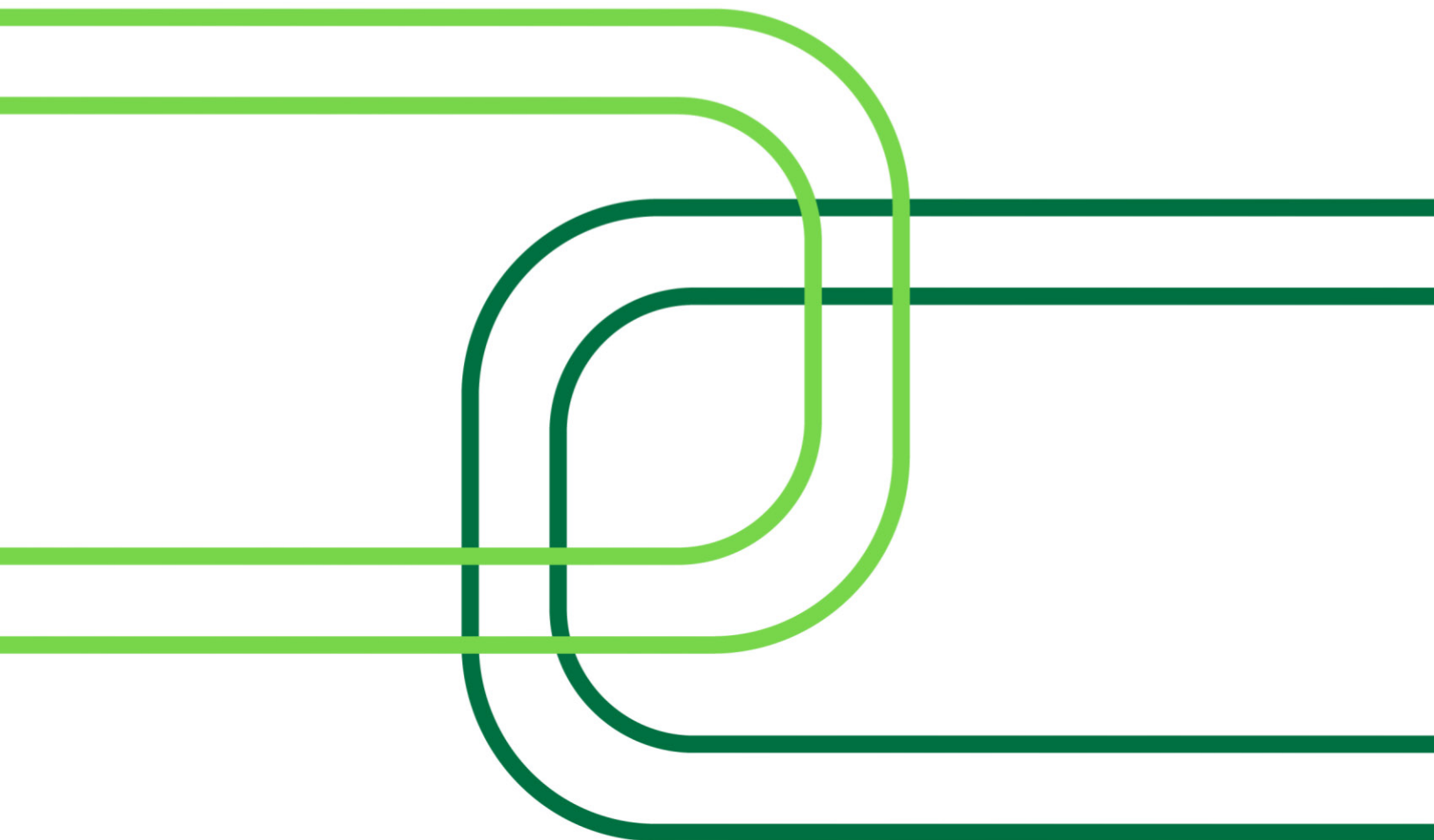
Colocation Data Center Services



SOC 2® Type 2 Report

For the Period

July 1, 2025 - June 30, 2026



Contents

Section 1: Independent Service Auditor's Report.....3

Section 2: Management’s Assertions8

Section 3: Leaseweb Canada’s Description of its Colocation Data Center Services.....11

 Overview12

 Scope of the System12

 Description of the Service Offerings Provided12

 Principal Service Commitments and System Requirements14

 Components of the System15

 Relevant Aspects of Internal Controls16

 Trust Services Criteria Determined to be Not Applicable23

 Complementary Subservice Organization Control Considerations.....23

Section 4: Trust Services Criteria, Related Controls, and Tests of Controls24

 Guidance Regarding Tests of Controls25

 Applicable Trust Services Criteria25

Section 1: Independent Service Auditor's Report





INDEPENDENT SERVICE AUDITOR'S REPORT ON A SOC 2 EXAMINATION

To the Management of:
Leaseweb Canada
20, Place du Commerce
Montreal, QC, H3E 1Z6, Canada

Scope

We have been engaged to report on Leaseweb Canada's accompanying description of its Colocation Data Center Services, including data center operations services provided by and controls operated by EvoSwitch, titled "Leaseweb Canada's Description of Its Colocation Data Center Services" throughout the period July 1, 2025 to June 30, 2026, (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)*, in AICPA, *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of Leaseweb Canada's controls, including the controls designed by Leaseweb Canada and operated by EvoSwitch, stated in the description throughout the period July 1, 2025 to June 30, 2026, to provide reasonable assurance that Leaseweb Canada's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)*, in AICPA, *Trust Services Criteria*.

EvoSwitch is an independent subservice organization providing data center operations services to Leaseweb Canada. The description includes those elements of the data center operations services provided to Leaseweb Canada and the controls designed by Leaseweb Canada and operated by EvoSwitch that are necessary for Leaseweb Canada to achieve its service commitments and system requirements based on the applicable trust services criteria.

Leaseweb Canada also uses a subservice organization to provide services outlined in Section 3 of the report. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Leaseweb Canada, to achieve Leaseweb Canada's service commitments and system requirements based on the applicable trust services criteria. The description presents Leaseweb Canada's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Leaseweb Canada's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

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

Subservice Organization's Responsibilities

EvoSwitch has provided the accompanying statement titled "EvoSwitch Management's Assertion" (EvoSwitch assertion) about the description and the controls stated therein. EvoSwitch is responsible for preparing the portion of the description related to the data center operations services provided to Leaseweb Canada and the EvoSwitch statement, including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; and implementing, operating, and documenting controls designed by Leaseweb Canada, which enable Leaseweb Canada to achieve its service commitments and system requirements.

Our Independence and Quality Control

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits and Reviews of Financial Statements, or Other Assurance or Related Services Engagements*, which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service Auditor's Responsibilities

Our responsibility, under this engagement, is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on the evidence we have obtained.

Our engagement was conducted in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information, set out in the CPA Canada Handbook – Assurance*. This standard requires that we plan and perform our engagement to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

A reasonable assurance engagement to report on the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.

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

Inherent Limitations

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

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

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

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4, "Trust Services Criteria, Related Controls, and Tests of Controls" of this report.

Opinion

In our opinion, in all material respects—

- a. The description presents Leaseweb Canada's Colocation Data Center Services that was designed and implemented throughout the period July 1, 2025 to June 30, 2026 in accordance with the description criteria.
- b. The controls stated in the description, including the controls designed by Leaseweb Canada and operated by EvoSwitch, were suitably designed throughout the period July 1, 2025 to June 30, 2026, to provide reasonable assurance that Leaseweb Canada's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period and if the subservice organization applied the complementary controls assumed in the design of Leaseweb Canada's controls throughout the period July 1, 2025 to June 30, 2026.
- c. The controls stated in the description including the controls designed by Leaseweb Canada and operated by EvoSwitch, operated effectively throughout the period July 1, 2025 to June 30, 2026, to provide reasonable assurance that Leaseweb Canada's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary

subservice organization controls assumed in the design of Leaseweb Canada's controls operated effectively throughout the period from July 1, 2025 to June 30, 2026.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Leaseweb Canada, user entities of Leaseweb Canada's Colocation Data Center Services during some or all of the period July 1, 2025 to June 30, 2026, business partners of Leaseweb Canada subject to risks arising from interactions with the Colocation Data Center Services, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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



Chartered Professional Accountants

Licensed Public Accountants

Toronto, Ontario

September 8, 2026

Section 2: Management's Assertions



Leaseweb Canada Management's Assertion

We have prepared the accompanying description of Leaseweb Canada's Colocation Data Center Services titled "Leaseweb Canada's Description of its Colocation Data Center Services" throughout the period July 1, 2025 to June 30, 2026 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)*, in AICPA, *Description Criteria* (description criteria). The description is intended to provide report users with information about the Colocation Data Center Services that may be useful when assessing the risks arising from interactions with Leaseweb Canada's system, particularly information about system controls that Leaseweb Canada has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)*, in AICPA, *Trust Services Criteria*.

Leaseweb Canada uses EvoSwitch to provide data center operations services. Leaseweb Canada's description includes a description of EvoSwitch's data center operations services used by Leaseweb Canada, including the controls of Leaseweb Canada and the controls designed by Leaseweb Canada and operated by EvoSwitch that are necessary, in combination with controls at Leaseweb Canada, for Leaseweb Canada to achieve its service commitments and system requirements based on the applicable trust services criteria. EvoSwitch's assertion is presented on page 10 in Section 2.

Leaseweb Canada also uses a subservice organization to provide services outlined in Section 3 of the report. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Leaseweb Canada, to achieve Leaseweb Canada's service commitments and system requirements based on the applicable trust services criteria. The description presents Leaseweb Canada's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Leaseweb Canada's controls. The description does not disclose the actual controls at the subservice organization.

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

- 1) The description presents Leaseweb Canada's Colocation Data Center Services that was designed and implemented throughout the period July 1, 2025 to June 30, 2026, in accordance with the description criteria.
- 2) The controls stated in the description, including the controls designed by Leaseweb Canada and operated by EvoSwitch, were suitably designed throughout the period July 1, 2025 to June 30, 2026, to provide reasonable assurance that Leaseweb Canada's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period and if the subservice organization applied the complementary controls assumed in the design of Leaseweb Canada's controls throughout that period.
- 3) The controls stated in the description, including the controls designed by Leaseweb Canada and operated by EvoSwitch, operated effectively throughout the period July 1, 2025 to June 30, 2026, to provide reasonable assurance that Leaseweb Canada's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Leaseweb Canada's controls operated effectively throughout that period.

EvoSwitch Management's Assertion

EvoSwitch provides data center operations services to Leaseweb Canada. The services provided by EvoSwitch are part of Leaseweb Canada's Colocation Data Center Services. We have prepared the portion of the accompanying description of Leaseweb Canada Colocation Data Center Services titled "Leaseweb Canada's Description of Its Colocation Data Center Services" throughout the period July 1, 2025 to June 30, 2026, (description) disclosing EvoSwitch's data center operations services provided to Leaseweb Canada based on the criteria for a description of a service organization's system in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)*, in AICPA, *Description Criteria* (description criteria). The description is intended to provide report users with information about Leaseweb Canada's Colocation Data Center Services that may be useful when assessing the risks arising from interactions with Leaseweb Canada's system, particularly information about system controls that Leaseweb Canada has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)*, in AICPA, *Trust Services Criteria*.

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

- 1) The description presents EvoSwitch's data center operations services made available to Leaseweb Canada throughout the period July 1, 2025 to June 30, 2026, in accordance with the description criteria.
- 2) EvoSwitch's controls stated in the description, which were designed by Leaseweb Canada, operated as described throughout the period July 1, 2025 to June 30, 2026, based on the applicable trust services criteria.

Section 3:

Leaseweb Canada's

Description of its

Colocation Data

Center Services



Overview

Leaseweb Canada provides the high-performance hosting infrastructure behind diverse organizations in more than 150 countries worldwide. We share the innovative spirit of our startup customers and the global footprint of our most established.

Scope of the System

The system description has been prepared to provide information on Leaseweb Canada’s control environment over its Colocation Data Center Services provided throughout the period of July 1, 2025 to June 30, 2026 in relation to the security and availability trust services categories.

Subservice Organizations

Leaseweb utilizes third-party providers (subservice organizations) to support the system. The subservice organizations and the services provided include:

Subservice Organization	Services Provided
EvoSwitch	Data Center Operations Services
Northwave	Managed Security Service Provider

The scope of this report includes control activities performed by Leaseweb Canada and EvoSwitch. It does not include the controls in place at the other subservice organization.

Significant Changes to the System

There were no significant changes to the system during the attestation period. Any changes to the service organization’s control activities or processes related to the system are included in Section 4, “Trust Services Criteria, Related Controls, and Tests of Controls”.

Significant Subsequent Events

There were no significant events subsequent to the attestation period and through the date of the report that would materially impact the system.

Identified System Incidents

No significant incidents have occurred related to the services provided to user entities during the review period.

Description of the Service Offerings Provided

Leaseweb Canada provides colocation data center services which includes data centers in the following locations:

- Nuns’ Island (MTL-01), 20 Place du Commerce, Nuns Island, Montreal, Canada
- Newman (MTL-02), 7207 Newman Blvd., LaSalle, Quebec, Canada

Leaseweb Canada's key-focus targets for customers are:

- High Performance - Dedicated server hardware and OpenStack cloud computing engineered to the highest performance standards.
- On Demand - Order servers online, deployed on demand in your choice of data center location, with the flexibility to scale when you need to.
- Custom Solutions - Custom solutions and support for private clouds, disaster recovery, business continuity and high availability.

Leaseweb Canada is primarily responsible for the following types of activities related to data center services at its data centers:

- Providing a safe, secure facility for customers. Related security requirements are supported by badge access systems, video surveillance cameras, and onsite 24/7/365 manned security and controls designed to ensure that only authorized individuals have access to the facility.
- Ensuring that networks and systems are available for use by customers, as defined by service level agreements (SLAs) agreed to in advance with the customer. Availability requirements are supported by an environmentally stable facility with uninterruptable power for the customers.
- Environmental controls and redundancy features must be periodically serviced and maintained to ensure effective operation.
- Resolving customer complaints, issues, and incidents on an as needed basis, or providing administrative services that customers require to maintain the availability and related security of their systems.
- Consistently applying an infrastructure change management process designed to ensure that only authorized, adequately planned, and supervised changes to the facility are performed.

Leaseweb Canada provides the following customer support services, which enhance the security and availability of the system by communicating related issues and requests with the customer. These services are primarily carried out by Network Operations Center (NOC) and Data Center Operations personnel.

- Responding to requests for support services.
- Responding to requests for changes (additions, modifications, and removals) to the customer's list of designated contacts. Requests for changes to customer contacts that have physical access are handled using this process.
- Responding to, and escalating, customer complaints and issues regarding the availability and / or related security of their services.
- Communicating changes, issues, and incidents to customers who have the potential to affect them.

Leaseweb Canada is not responsible for providing the following services for its colocation customers, unless these services are agreed to in advance under Leaseweb Canada's other service offerings (IP services, cloud services, hosting services, or hybridized services), which are not included within the scope of this report. Customers are responsible for performing these functions.

- Applying logical access security controls, including user authentication, password complexity requirements, password history requirements, password change procedures, account lockout procedures, and related procedures.

- Protecting and maintaining the network security of system resources (for example, secure VPN, configuration and use of firewalls and intrusion detection, and disabling of unneeded network services).
- Maintaining system components and configurations, including the application of change controls and procedures as necessary.
- Data encryption controls and the secure transfer of data through networks, including public, semi-private, and virtual private networks.
- Performing data backup procedures and data classification procedures as necessary.
- Protecting systems against infection by computer viruses, malicious codes, and unauthorized software.

Customers may choose to have Leaseweb Canada perform certain of these functions through Leaseweb Canada's other service offerings, which are not included within the scope of this report. Service offerings are subject to reasonable best efforts and are billable at the active rate at the time of purchase.

Principal Service Commitments and System Requirements

Leaseweb Canada's service commitments to customers for colocation services include providing physically secure and conditioned space for customer equipment.

- Leaseweb Canada must install and maintain security systems to control access to data centers and shared common space and provide customers with key cards or other such technology to access the facilities. Customers may access secured data centers 24 hours a day, 7 days a week, 365 days a year ("24/7/365") unless otherwise specified.
- Access to customer cages or cabinets must be limited to individuals authorized by the customer, except for instances where Leaseweb Canada personnel must access for maintenance or emergency purposes. Otherwise, consent must be obtained from the customer prior to Leaseweb Canada accessing their space. Leaseweb Canada must ensure that there is no unauthorized access.
- Leaseweb Canada must condition the data center to ensure that the power supply to customer equipment is uninterrupted, using a combination of UPS and backup generator systems. Uninterrupted cooling must be provided to customer space.
- For customers who have purchased and installed a redundant power solution, Leaseweb Canada must use commercially reasonable efforts to ensure that power will be available to the customer's cage, cabinet, rack, or suite 100% of the time except as part of scheduled maintenance or by request from the customer. In instances where customers do not have a redundant power solution, Leaseweb Canada must use commercially reasonable efforts to ensure that customers will not experience an event lasting more than 15 minutes except as part of scheduled maintenance or by request from the customer.
- Leaseweb Canada must use commercially reasonable efforts to ensure that the temperature in Leaseweb Canada's colocation areas will not fall below 65 degrees (18 Celsius) Fahrenheit or rise above 80 degrees (27 Celsius) Fahrenheit.
- Leaseweb Canada must use commercially reasonable efforts to ensure that humidity in Leaseweb Canada's colocation areas will not fall below 20% or rise above 80% relative humidity.
- In order to ensure these commitments are met and to ensure the safety of its data centers, Leaseweb Canada must regularly inspect and service power and cooling equipment.

Components of the System

System Boundaries

The system includes the people, processes, and technology that make up the infrastructure responsible for supporting Leaseweb Canada's colocation data center services system.

Infrastructure & Software

Leaseweb Canada's colocation data center services system includes the infrastructure that supports the physical access control systems, activity logging, and video monitoring. These systems are self-hosted by Leaseweb Canada on Windows and Linux servers and protected by firewalls and other logical access mechanisms.

People

Leaseweb Canada's and EvoSwitch's employees are organized into functional areas including Executives, Finance, Operations, and IT. Reporting lines are established and communicated to employees via the Company organization chart.

Processes, Policies, and Procedures

Leaseweb Canada IT policies and procedures are documented and are readily available to employees. The responsibility and accountability for changes and updates to these policies are assigned to appropriate IT management personnel. The information in these policies is reviewed on an annual basis by IT management.

Leaseweb Canada data center operational policies and procedures are documented in various ways and are readily available to employees and customers. The responsibility and accountability for developing and maintaining these policies, and changes and updates to these policies, are assigned to the appropriate data center employees. The information in these policies is reviewed on an annual basis by appropriate data center employees.

Each Leaseweb Canada data center has a specific Data Center Operations Manual kept in a binder and physically available for employees in case of an emergency. The Data Center Operations Manual is reviewed and approved by Data Center Operations management on an annual basis to ensure the information is up-to-date and accurate.

The Network Operations Center (NOC) uses its own internal wiki dedicated to its policies and procedures. Content is updated in real time on the wiki's webpage to ensure NOC employees are always aware of the newest policy or procedures. On an annual basis, NOC management performs a review of information on the NOC wiki's webpage to ensure the information is up-to-date and accurate. Leaseweb Canada personnel use a ticketing system to track incidents and customer requests. Incidents are escalated as necessary and tracked until resolution.

Each customer in Leaseweb Canada data centers is given Customer Service documentation. These documents include all necessary customer facing information and procedures to follow for many common questions/ requests, such as system availability issues and what to do when a possible security breach is identified, along with many other incident responses. The information in the Customer Service documents is reviewed on an annual basis by business unit management to ensure the information is up-to-date and accurate. Additionally, Leaseweb Canada customers connect to Leaseweb Canada via the Leaseweb Canada website and online customer portal. Leaseweb Canada's website hosts a detailed description of the data center services and the portal houses customer specific information and enables customers to

contact Leaseweb Canada directly through the system. This customer portal, along with ad hoc communication methods are used to ensure transparent communication with customers.

Data

Data, as defined by Leaseweb Canada includes:

Client Data

Leaseweb Canada does not manage client data or content. Clients are responsible for applying logical access security controls, network security controls, data encryption controls, and related procedures to protect their data, as well as performing data backup procedures and data classification procedures as necessary.

Data Managed by Leaseweb Canada

Listing of Customer Contacts – Leaseweb Canada maintains a listing of all customer contacts with approved access to the data center. The listing provides the privileges granted to each contact, including whether or not they have physical access, may request tech support, or add other contacts to the approved listing managed by Leaseweb Canada. Customers may request a report listing all individuals on this approved listing, as well as their privileges.

Physical Access Control System Lists and Key Badges – Leaseweb Canada maintains a listing of all individuals with physical access to the data center. This is managed using the Access Control System. Customers may request a report listing all individuals who have physical access to their cage or cabinet. Customers are responsible for periodically reviewing their access lists and for notifying Leaseweb Canada of terminated employees.

Physical Access Activity Logs – The Access Control System maintains records of all physical access attempts to the data center (both successful and unsuccessful). Temporary visitor and contractor logs are maintained by the Security Desk.

The system and procedures have been designed to secure sensitive data at all stages.

Relevant Aspects of Internal Controls

The security and availability trust services categories and applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. The controls supporting the applicable trust services criteria are included in Section 4 of this report.

Information and Communication Systems

Leaseweb Canada's management team is responsible for the detailed design and effective operation of the Company's internal controls. As part of this process, management communicates responsibilities and expectations to company personnel through both formal and informal means. Internal controls are evaluated by Internal Audit throughout the year as part of its internal audit reviews. Testing results and exceptions identified during the audits are reported to management on a consistent basis. Management ensures that any internal control deficiencies identified are addressed and communicates expected timelines for doing so.

Monitoring

Leaseweb Canada's management team, including support from Leaseweb Global's Internal Audit team, continuously monitors the effectiveness of the Company's system of internal controls through the performance of periodic and annual assessments of internal controls. Any deficiencies in the Company's system of internal controls are reported to management, assessed, and addressed. Management's consistent oversight of internal controls helps the Company identify deficiencies in the system, ensuring the adequacy of the process. Additionally, management has implemented security and availability monitoring controls in the form of periodic external inspections, metrics reviews, and incident monitoring.

There have not been any known instances of security breaches affecting customer equipment or data during the period under review. There have not been any instances of extensive service outages during the period under review.

Risk Assessment

Leaseweb Canada uses various methods to manage risks that could impact the Company's ability to deliver services to customers. Leaseweb Global performs an annual companywide risk assessment which includes each of the Leaseweb Canada data centers. Management assesses risks that inherently arise from the expansion of the business, whether organically or inorganically. This may include managing risks that are rooted in changes in personnel, technology, or the Company's operating environment. Management revisits these assessments annually to ensure these risks are appropriately mitigated.

Control Activities

Leaseweb Canada's commitment to competence includes management's determination of the levels of competence and expertise required for each position at the data center, ensuring highly technical and customer service focused data center employees. Leaseweb Canada provides 24/7/365 manned facilities with a host of security features designed to protect the customer's equipment and network connectivity. Leaseweb Canada controls ingress and egress using electronic keycard and / or biometric software. All cages and cabinets are securely locked, and Closed-Circuit Television (CCTV) cameras monitor and record activity within each facility.

Organizational Structure and Assignment of Authority and Responsibility

Leaseweb Canada has developed an organizational structure that adequately suits the nature and scope of its operations. The Company has developed organizational charts that internally convey employee reporting relationships, operational responsibilities, and the overall organizational hierarchy.

Human Resource Policies and Practices

Leaseweb Canada's human resource department has policies and established practices that govern the hiring, termination, evaluation, promotion, counseling, and compensation of current and prospective company employees. A documented set of human resource, operational, and financial policies and procedures, along with a complete list of internal controls are made available to applicable employees via the intranet. The Company has a written Code of Conduct that is communicated to and certified by all employees annually. The Code details the company's expectations regarding behavior, ethics, and business practices that every employee must abide by.

Detailed job descriptions and organizational charts convey the requirements for each position. Leaseweb Canada also facilitates employee development through annual evaluations, onsite training, and the allocation of funds for other relevant training. New hire policies include the requirement that background checks be performed on all new employees prior to commencing employment with Leaseweb Canada.

Newly hired data center employees receive training and are made aware of customer facing documents and other internal policies covering system security and availability. For terminated employees, Leaseweb Canada has a formal process for decommissioning access to data center facilities, company records and systems in a timely manner.

Security Staff

Responsibilities of security personnel include but are not limited to the following.

- Monitoring of Physical Security Systems
- Loss Prevention
- Internal Investigations
- Security Policies and Procedures Compliance

Security Control

All Leaseweb Canada data centers have Security and/or Leaseweb Canada/EvoSwitch data center personnel to control access, monitor security alarms, monitor CCTV camera surveillance, and support security-related operational activities 24/7/365. Security personnel and/or Leaseweb Canada on-duty engineers are onsite 24/7/365. The Security Control Desk performs the following.

- Real-time monitoring of data center door alarms
- Real-time monitoring of data center CCTV cameras
- Centralized security service and emergency dispatch communications for Security Staff, as well as for local fire departments, police departments, and other emergency response resources
- Electrical power support for continuous operation of communications, lighting, CCTV, intrusion detection, and alarm monitoring equipment in the event of utility power loss

Surveillance and Monitoring

Leaseweb Canada data centers employ a CCTV system to record and facilitate monitoring of the data center. Cameras are positioned to provide views of critical areas, including perimeter doors, main entrances and exits, shipping & receiving, and other areas of importance.

Leaseweb Canada and EvoSwitch personnel monitor the signals from the CCTV system. The desk is connected by secure cables to the cameras throughout the facility to permit both interior and exterior surveillance.

Cameras are recorded on site via digital video recorders 24/7/365. These visual records are retained for at least 90 days to provide details of activity at Leaseweb Canada data centers. Leaseweb Canada provides dedicated 24/7/365 continuous power supply (CPS) and standby emergency power via generator to support security systems.

Access Control

Leaseweb Canada employs a computerized Access Control System (ACS) to control physical access to the data centers. The ACS utilizes proximity card readers with pin codes or biometrics to control access into the data center floor, perimeter doors, shipping & receiving areas, storerooms, and other critical areas. Customers and employees (including contractors and security guards) must follow formal access request and approval processes before physical access to the data centers is granted. Additional access control features are as follows.

- Access to the data center and other restricted areas is specifically limited to authorized individuals.
- Leaseweb Canada access badges and / or biometrics are required to gain entry to critical areas.
- Vendors, Contractors, Visitors and non-data center employees must sign in at the security desk prior to entry into the data center. Leaseweb Canada personnel verifies log accuracy and reconciles log with ACS.
- Customers, Vendors, Contractors, and other Visitors must be sponsored by an Leaseweb Canada-approved host to gain access if not on the Customer-Approved List.
- It is mandatory that all Customers, Vendors, Contractors, and Visitors are in the possession of their government issued photo ID while visiting the data center and that the identification is shown to the physical security guard upon request.
- All Customers, Vendors, Contractors, and Visitors on the Customer-Approved List must check in with the Security Desk upon arrival with photo identification if they require the physical key to access cages. Those customers with badge cage access will have automatic access to their cages.
- Visitors and others not on the Customer-Approved List are escorted while in the data center and other critical areas.
- Guest access for approved Contractors is generally limited to particular areas where work is being performed.
- Employees with access to the data center are limited to those with a specific business need or job function.

Administrator access (add, modify, and delete users) in the ACS, is restricted to appropriate personnel based on job roles and responsibilities and reviewed during periodic access reviews. Data Center Management authorizes Administrator access to the keycard system based on the individual's job responsibilities.

The ACS is also used to monitor, notify, and log security alarms. The system monitors the following.

- Perimeter / external doors
- Restricted area doors
- Data center doors
- Shipping / receiving doors

The system is programmed to log all card reader activity. It also generates alarms for forced doors, propped doors, and denied card read attempts.

Visitor / Sales Tour Access

All Leaseweb Canada data center tours must be coordinated with an Leaseweb Canada or EvoSwitch representative. Tours of the data center and other restricted areas require an escort from an authorized Leaseweb Canada employee.

Customer Access

Each customer is permitted to designate individuals with access to Leaseweb Canada data centers via the Network Operations Center (NOC) and Data Center Operations. The customers make requests for access via email, phone call, or the online Customer Portal. Data Center Operations manages customers' respective Customer Access Lists (CALs) within the Facility Management application. Update access to the CAL is reviewed for appropriateness based on job responsibilities on an annual basis. Data center security has view access to the CALs and will only allow individuals listed on a Company's CAL access to the data center. The customer is responsible for requesting additions, modifications, or deletions to access. Upon notification of a customer employee termination or revocation of customer agreement, physical access to the data center is revoked. Customers are responsible for retaining a terminated employee's access badge and either destroying it or returning it to Leaseweb Canada and EvoSwitch security.

Customer equipment is segregated via locked cages or locked cabinets to ensure that customers can only access their own equipment.

Cages are secured via one of two possible means: Physical key or electronic badge reader.

1. Physical key - Keys are maintained by Leaseweb Canada security personnel or Leaseweb Canada onsite engineer. After the security personnel or Leaseweb Canada onsite engineer determine appropriate authority per the CAL, they escort the customer to the cage and unlock it for them; or
2. Badge reader access - access is controlled via the ACS, similar to that of data center access.

Cabinets are secured via one of two possible means: Physical key or combination lock.

1. Physical key - Keys are maintained by Leaseweb Canada security personnel and Leaseweb Canada onsite engineer. After the security personnel or Leaseweb Canada onsite engineer determine appropriate authority per the CAL, they escort the customer to the cabinet and unlock it for them; or
2. Combination lock - access is controlled via the use of a customer specific combination code.

Customers are responsible for ensuring their cage and cabinet(s) are properly locked before leaving the facility.

Employee and Security Guard Access to Data Center

Access to the data center is restricted to only those Leaseweb Canada employees with a legitimate business need. Access, if temporarily required for other employees whose job functions do not necessitate access to the data center on a day-to-day basis, is granted on a case-by-case basis by the data center manager, and these employees must be escorted by data center personnel. Physical access to the data center is revoked upon termination of Leaseweb Canada employees and security guards.

Contractor and Vendor Access to Data Center

Access to the data center is restricted to Contractors and Vendors with a legitimate business purpose. Access is granted with a daily temporary badge and logged with security. Data Center management will notify Security of an expected Contractor or Vendor, and if a Contractor or Vendor arrives unexpectedly, Security will contact Data Center Management to gain approval for temporary access. Temporary access cards are returned to security prior to leaving the facilities. If a temporary badge is not returned at the end of the day, it is disabled in the system by Security. Physical access to the data center is revoked upon completion of the contractors' and / or vendors' duties.

General Visitor Rules

- All visitors must be escorted at all times by an authorized host or employee.
- Leaseweb Canada data center regulations must be strictly followed at all times. Any individual (including Leaseweb Canada employees) not adhering to these rules will be escorted from the data center by staff and / or security.
- Badges must be displayed at all times within the facility.

Customer and Employee Access Review

Leaseweb Canada and EvoSwitch personnel perform audits to validate the appropriateness of access permissions in the Access Control System (ACS). The following audits are performed.

1. Customer access permissions in the ACS are validated against the Facilities Access list at least quarterly and discrepancies are investigated and remediated appropriately.
2. Employee, Contractor, and Security Guard access in the keycard system are reviewed for appropriateness at least quarterly.
3. Employees with access to add, modify, and delete users in the ACS are reviewed for appropriateness at least annually.

Logical and Network Protections for the Access Control System and Facility Management Application

Access to the network and applications is ID and password protected. Roles based access to applications and operating systems ensures privileges and authorizations associated with user accounts provide access to specific limited system functionality.

Password length and complexity requirements are established for the Leaseweb Canada internal network. Password settings for the keycard system are the same as for the internal network since the system uses single sign on.

Anti-virus software for network workstations and keycard system servers is installed and operating effectively. The Company has firewalls in place to limit access over the internet to the central keycard system application and database. Connections via VPN tunnel between company locations are protected using encryption. Connections to applications via the internet are protected using encryption.

Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to the appropriate business unit representative for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.

Monitoring Activities

Leaseweb Canada's data center operations consist of a strong physical infrastructure, including secure facilities featuring N+1 redundancy for both power and cooling at the MCO and MNE data centers, along with fire protection and system monitoring. The existing facility and environmental standards at the data centers are designed to ensure that uptime is maximized by providing redundancy to key facility and environmental systems.

Monitoring Environmental Conditions and Critical Work Authorizations

Data center environmental conditions are constantly monitored and reported via an automated Building Management System (BMS). Leaseweb Canada and EvoSwitch personnel monitor a BMS console which reports the real-time status of power, HVAC, temperature, and fire detection / suppression conditions. If

any issues or incidents with these environmental systems arise, the console displays an alert and/or e-mails data center personnel.

Leaseweb Canada has in place a Change Management process to ensure all scheduled maintenance and other data center implementations/modifications are documented and authorized to assure minimal impact to the customers. Threats that could impair the availability of data centers are identified and ranked by overall risk (determined by likelihood and impact) in the company's Business Continuity Plan.

Smoke / Fire Detection

The smoke and fire detection system in the data centers is comprised of smoke detectors and either a particulate sampling system or a very early smoke detection apparatus (VESDA) system that detects smoke during the very early stages of combustion. The smoke detection system is the first line of defense against fire in the facility. When smoke is detected by the system, an alarm is generated in the facility control room, and the BMS generates alerts to Leaseweb Canada and EvoSwitch employees.

The smoke detection system is inspected and serviced at least annually to ensure effective operation.

Fire Suppression

The fire suppression system consists of a pre-action dry pipe system. The pre-action dry pipe system is designed to keep water out of the sprinkler system plumbing in the data center areas during normal operations. If smoke and/or excessive heat is detected, and a sprinkler fusible head melts as a result, water is pumped into the sprinkler systems for the affected zone(s) only. The BMS continuously monitors and reports the status of the fire suppression system.

The fire suppression systems are inspected and serviced at least annually to ensure effective operation.

Clean agent fire extinguishers are also provided throughout the data center for accessibility in the event of a fire within the data center (or elsewhere in the building).

Fire extinguishers are inspected and serviced at least annually to ensure effective operation.

Heating, Ventilation, and Air Conditioning (HVAC)

Multiple HVAC units control both temperature and humidity within the data center and are configured in a redundant formation to ensure operation continues if a unit fails at the MCO and MNE data centers. Temperature and humidity are maintained to current SLA standards. The HVAC units are monitored by the BMS, and any alerts generated are sent to Leaseweb Canada and EvoSwitch personnel.

HVAC units are inspected and serviced at least annually to ensure effective operation.

Utility Power and Backup Power Systems

Data center power is provided by feeds from the local utility provider to support daily operations. The power is channeled into an uninterruptible power supply (UPS) system, which conditions the power to be supplied to data center equipment. The UPS system allows for customers to opt for redundant N+1 power feeds to their equipment at the MCO and MNE data centers. In the event of a utility power outage, the UPS system seamlessly draws backup power from a battery farm which will supply power for at least 15 to 20 minutes until diesel generators power up. Leaseweb Canada maintains a sufficient onsite fuel reserve, which gives the backup generators capability to power the data center for at least 48 hours.

Each of Leaseweb Canada's data centers maintain contracts with fuel companies for the delivery of fuel as needed.

The UPS systems and generators are inspected and serviced at least annually to ensure effective operation. The operating effectiveness of backup power systems are confirmed at least annually, through load bank testing and / or other methods.

Description of Controls Relevant to Availability

Automated alerts are in place to notify relevant parties for performance, security threats, changing resource utilization needs, unusual system activity and environmental threats. Tickets are created based on the alert and appropriate action is taken. Redundancy has been implemented for critical infrastructure components. Environmental protections are in place including Cooling systems, UPS & generator backups, redundant communication lines, smoke detectors and dry pipe sprinklers.

Daily full-system backups are performed using an automated system. Backups are monitored for failure and resolved.

There are business continuity and disaster recovery plans in place. These plans are tested annually.

Trust Services Criteria Determined to be Not Applicable

The disposal, transmission, movement, and removal of information & data is the responsibility of the client. Therefore, CC6.5 & CC6.7 are not applicable to Leaseweb Canada.

Trust Services Criteria and Related Controls

Leaseweb Canada’s applicable trust services criteria and their related controls are included in Section 4, “Trust Services Criteria, Related Controls, and Test of Controls,” to eliminate the redundancy that would result from listing them in this section and repeating them in Section 4. Although the trust services criteria and related controls are included in Section 4, they are, nevertheless, an integral part of Leaseweb Canada’s description of controls.

Complementary User Entity Control Considerations

Complementary user entity controls are not necessary to achieve the Company’s service commitments and system requirements based on the applicable trust services criteria.

Complementary Subservice Organization Controls

Leaseweb Canada’s controls related to the Colocation Data Center Services cover only a portion of overall internal control for each user entity of Leaseweb Canada. Complementary controls at the subservice organization are required to meet the applicable trust services criteria related to security and availability. Therefore, each user entity’s internal control for security and availability must be evaluated in conjunction with Leaseweb Canada’s controls described in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Complementary Subservice Organization Controls	Applicable TSC
Notification of Leaseweb Canada personnel of any incidents requiring action should be done timely.	CC7.1 – 7.3
Any changes made to security configurations should be tested and approved prior to implementation.	CC8.1

Section 4: Trust Services Criteria, Related Controls, and Tests of Controls



Guidance Regarding Tests of Controls

When using information produced by the service organization, we evaluated whether the information was sufficiently reliable for our purposes, including, as necessary, obtaining evidence about the completeness and accuracy of the information and evaluating whether the information was sufficiently precise and detailed for our purposes.

The types of tests that may have been performed in evaluating the effectiveness of controls include inquiry, observation, inspection and/or re-performance.

Applicable Trust Services Criteria

Category	Description
Security	Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.
Availability	Information and systems are available for operation and use to meet the entity's objectives.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
CC 1	Common Criteria Related to Control Environment	
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	
The Code of Conduct provides standards on conduct, integrity, and ethical values. The Code of Conduct is required to be acknowledged during onboarding and annually thereafter. The policy is available on the Company intranet.	Inspected the Code of Conduct to determine that the document outlines standards on conduct, integrity and ethical values and is available on the Company intranet. Inspected the Code of Conduct acknowledgements for a sample of newly hired employees to determine that new hires are required to acknowledge the policy upon hire. Inspected the Code of Conduct acknowledgements for a sample of existing employees to determine that employees are required to acknowledge the policy on an annual basis.	No exceptions noted.
An employment prescreening process is performed for new hires, which includes background, credit, and DMV checks (based on job requirements) being completed prior to hire.	Inspected prescreening documentation for a sample of new hires to determine that Human Resources ran background, credit, and/or DMV checks prior to hire.	No exceptions noted.
Leaseweb Canada has an annual objective setting process and employee evaluation process. During these periods, managers and employees discuss and assess expectations regarding performance; roles and responsibilities, including internal controls; ethics; integrity; and training needs. Human Resources tracks completion and results of the assessment procedure.	Inspected the performance evaluation template to determine that expectations regarding performance, ethics, integrity, and training needs were part of the objective setting and employee evaluation process. Inspected results of the most recently performed performance evaluation cycle to determine that Human Resources tracked completion and results of the annual assessment.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	
The Company has an independent Board of Directors with clear duties, responsibilities and purpose articulated in the Corporate Governance Guidelines. The Board of Directors provides management oversight responsibilities.	Inspected internal policies and Board of Director descriptions to determine that the Company has an independent Board of Directors with clear duties, responsibilities and purposes that provide management oversight responsibilities.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
CC 1	Common Criteria Related to Control Environment	
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	
The Company has an independent Board of Directors with clear duties, responsibilities and purpose articulated in the Corporate Governance Guidelines. The Board of Directors provides management oversight responsibilities.	Inspected internal policies and Board of Director descriptions to determine that the Company has an independent Board of Directors with clear duties, responsibilities and purposes that provide management oversight responsibilities.	No exceptions noted.
The Company has a formal corporate organizational structure appropriate for the size of the organization. Organizational charts are in place documenting reporting lines and responsibilities.	Inspected the corporate organizational chart to determine that the Company has a formal organizational structure that documents reporting lines and responsibilities.	No exceptions noted.
Role descriptions exist for all key positions, which define minimum requirements, experience requirements, and roles and responsibilities.	Inspected maintained job descriptions to determine that the minimum requirements, experience requirements, roles and responsibilities for internal control are defined for each position.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	
An employment prescreening process is performed for new hires, which includes background, credit, and DMV checks (based on job requirements) being completed prior to hire.	Inspected prescreening documentation for a sample of new hires to determine that Human Resources ran background, credit, and/or DMV checks prior to hire.	No exceptions noted.
Leaseweb Canada has an annual objective setting process and employee evaluation process. During these periods, managers and employees discuss and assess expectations regarding performance; roles and responsibilities, including internal controls; ethics; integrity; and training needs. Human Resources tracks completion and results of the assessment procedure.	Inspected the performance evaluation template to determine that expectations regarding performance, ethics, integrity, and training needs were part of the objective setting and employee evaluation process. Inspected results of the most recently performed performance evaluation cycle to determine that Human Resources tracked completion and results of the annual assessment.	No exceptions noted.
Internal Audit maintains an active listing of control owner assignments for each SOC 2 control activity. Control design and coverage is assessed at least annually by Internal Audit with the control owners.	Inspected the control owner assignment tracker to determine that Internal Audit maintains the tracker and updates after collaboration with the control owners at least annually.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
CC 1	Common Criteria Related to Control Environment	
All employees are required to complete security awareness training at least annually. Management tracks completion and results of the annual security training and follows-up on any users who have not completed by the assigned due date.	Inspected the security awareness training results from the period to determine that in-scope employees completed security awareness training.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	
Role descriptions exist for all key positions, which define minimum requirements, experience requirements, and roles and responsibilities.	Inspected maintained job descriptions to determine that the minimum requirements, experience requirements, roles and responsibilities for internal control are defined for each position.	No exceptions noted.
Leaseweb Canada has an annual objective setting process and employee evaluation process. During these periods, managers and employees discuss and assess expectations regarding performance; roles and responsibilities, including internal controls; ethics; integrity; and training needs. Human Resources tracks completion and results of the assessment procedure.	Inspected the performance evaluation template to determine that expectations regarding performance, ethics, integrity, and training needs were part of the objective setting and employee evaluation process. Inspected results of the most recently performed performance evaluation cycle to determine that Human Resources tracked completion and results of the annual assessment.	No exceptions noted.
Internal Audit maintains an active listing of control owner assignments for each SOC 2 control activity. Control design and coverage is assessed at least annually by Internal Audit with the control owners.	Inspected the control owner assignment tracker to determine that Internal Audit maintains the tracker and updates after collaboration with the control owners at least annually.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity		Test Results
CC 2	Common Criteria Related to Communication and Information	
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	
IT staff monitor critical/relevant systems for errors or exceeded thresholds. Errors are logged and alerts are generated to notify IT staff when conditions exceed defined thresholds.	Inspected network monitoring dashboards and system configurations to determine that IT staff monitor critical/relevant systems for errors and exceeded thresholds. Inspected the error log during the period to determine that errors were escalated and resolved when conditions exceeded defined thresholds.	No exceptions noted.
Company data center power and environmental conditions are monitored and reported via automated monitoring systems. Appropriate personnel receive and monitor alerts regarding the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	Inspected the BMS monitoring dashboards, system configurations, and alert logs from the period to determine that data center power and environmental conditions were monitored and reported via automated monitoring systems.	No exceptions noted.
Data center power and cooling capacity reports are prepared at least monthly to assist Data Center Operations management in maintaining, monitoring, and evaluating power and cooling capacity needs.	Inspected the data center power and cooling capacity reports for a sample of months to determine that data center power and cooling capacity reports were prepared to assist Data Center Operations management maintain, monitor, and evaluate power and cooling capacity needs.	No exceptions noted.
Management, with collaboration from Internal Audit, performs an annual risk assessment to identify internal and external risks, including those relevant to the industry, competition, IT infrastructure, cybersecurity, customer retention, capital investment, regulations, fraud, changes in the business model, changes in leadership, and other areas. The results of the assessment are communicated to management, and any deficiencies identified are tracked in a register through resolution.	Inspected the results of the most recent annual risk assessment to determine that internal and external risks are identified, assessed, and communicated to management. Inspected the maintained risk register to determine that identified internal and external risks and treatment activities were actively tracked until remediation.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity		Test Performed by the Service Auditor
CC 2	Common Criteria Related to Communication and Information	
Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to appropriate personnel for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.		Inspected network monitoring tool dashboards and configurations to determine that they are in place to detect unauthorized access to the network. Inspected alert logs from the period to determine that issues and incidents related to network security are escalated as necessary and tracked to resolution.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	
Each Company controlled data center has a detailed Data Center Operations Manual which is available to Data Center Operations personnel and includes emergency procedures, contact information, and data center equipment details, monitoring and/or maintenance requirements. Each Data Center Operations Manual is reviewed and approved by management as needed.		Inspected the Data Center Operations Manual for the Company data centers to determine that each had a Manual available to Data Center Operations personnel, procedures were documented, internal control requirements were specified, and the Manual was reviewed and approved by management as needed.
Management, with collaboration from Internal Audit, performs an annual risk assessment to identify internal and external risks, including those relevant to the industry, competition, IT infrastructure, cybersecurity, customer retention, capital investment, regulations, fraud, changes in the business model, changes in leadership, and other areas. The results of the assessment are communicated to management, and any deficiencies identified are tracked in a register through resolution.		Inspected the results of the most recent annual risk assessment to determine that internal and external risks are identified, assessed, and communicated to management. Inspected the maintained risk register to determine that identified internal and external risks and treatment activities were actively tracked until remediation.
Role descriptions exist for all key positions, which define minimum requirements, experience requirements, and roles and responsibilities.		Inspected maintained job descriptions to determine that the minimum requirements, experience requirements, roles and responsibilities for internal control are defined for each position.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
CC 2 Common Criteria Related to Communication and Information		
Leaseweb Canada has an annual objective setting process and employee evaluation process. During these periods, managers and employees discuss and assess expectations regarding performance; roles and responsibilities, including internal controls; ethics; integrity; and training needs. Human Resources tracks completion and results of the assessment procedure.	Inspected the performance evaluation template to determine that expectations regarding performance, ethics, integrity, and training needs were part of the objective setting and employee evaluation process. Inspected results of the most recently performed performance evaluation cycle to determine that Human Resources tracked completion and results of the annual assessment.	No exceptions noted.
The Company maintains policies and procedures pertaining to IT, including Information Security, Change Management, and other policies for operations and conduct. These are reviewed and approved by management as needed and available to employees on the internal Wiki	Inspected Company policies and procedures pertaining to Information Security, Change Management, and Incident Response to determine that they are maintained and approved by management. Inspected the internal Wiki to determine that Company policies and procedures are made available to employees.	No exceptions noted.
CC2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.		
The process for customers to inform the Company of system availability issues, possible security breaches, and other incidents is provided in the Customer Service documents and/or online customer webpage.	Inspected the customer web page and customer service documents to determine that the process to inform the Company of system availability issues, possible security breaches, and other incidents is provided.	No exceptions noted.
The Company has in place a Change Management process to ensure all scheduled maintenance and other data center implementations / modifications are properly documented and authorized to assure minimal impact to customers. For scheduled maintenance and other changes that have the potential to affect customer availability, customers are notified of the maintenance or change in advance.	Inspected the Company's Change Management process to determine that the Company has formalized procedures to ensure all scheduled maintenance and other data center implementations / modifications are properly documented and authorized to assure minimal impact to customers. Inspected documentation for a sample of data center maintenance and implementation events to determine that the changes followed the Change Management process, including obtaining formal authorization and communicating the change to customers, when necessary.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
CC 2	Common Criteria Related to Communication and Information	
The scope of services agreed to with new vendor service providers which could impact the security and availability of the Company data centers, as well as any compliance or security requirements and SLAs that the vendor must adhere to, are documented in contractual agreements with the vendor.	Inspected signed agreements with the population of new vendor service providers that could impact the security and availability of the Company data centers to determine that the scope of services and security requirements are documented.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
CC 3	Common Criteria Related to Risk Assessment	
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	
Management, with collaboration from Internal Audit, performs an annual risk assessment to identify internal and external risks, including those relevant to the industry, competition, IT infrastructure, cybersecurity, customer retention, capital investment, regulations, fraud, changes in the business model, changes in leadership, and other areas. The results of the assessment are communicated to management, and any deficiencies identified are tracked in a register through resolution.	Inspected the results of the most recent annual risk assessment to determine that internal and external risks are identified, assessed, and communicated to management. Inspected the maintained risk register to determine that identified internal and external risks and treatment activities were actively tracked until remediation.	No exceptions noted.
Leaseweb Canada has an annual objective setting process and employee evaluation process. During these periods, managers and employees discuss and assess expectations regarding performance; roles and responsibilities, including internal controls; ethics; integrity; and training needs. Human Resources tracks completion and results of the assessment procedure.	Inspected the performance evaluation template to determine that expectations regarding performance, ethics, integrity, and training needs were part of the objective setting and employee evaluation process. Inspected results of the most recently performed performance evaluation cycle to determine that Human Resources tracked completion and results of the annual assessment.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories			
Service Organization Control Activity		Test Performed by the Service Auditor	Test Results
CC 3	Common Criteria Related to Risk Assessment		
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		
Cybersecurity Risk Assessments are performed at least annually to assess risks and the controls in place to mitigate those risks. Risk items and related treatment plans are added to the risk register and tracked until remediation.		Inspected the results of the most recent Cybersecurity Risk Assessment to determine that the assessment is performed at least annually to identify risks and controls in place to mitigate them. Inspected the maintained risk register to determine that identified risks and treatment activities were actively tracked until remediation.	No exceptions noted.
Management, with collaboration from Internal Audit, performs an annual risk assessment to identify internal and external risks, including those relevant to the industry, competition, IT infrastructure, cybersecurity, customer retention, capital investment, regulations, fraud, changes in the business model, changes in leadership, and other areas. The results of the assessment are communicated to management, and any deficiencies identified are tracked in a register through resolution.		Inspected the results of the most recent annual risk assessment to determine that internal and external risks are identified, assessed, and communicated to management. Inspected the maintained risk register to determine that identified internal and external risks and treatment activities were actively tracked until remediation.	No exceptions noted.
Formalized vendor risk assessments are performed for new vendor service providers that could impact the security and availability of Leaseweb Canada data centers. Risks considered include, as applicable, (1) any access a vendor will have to facilities and data, including access to confidential or restricted data, (2) how Company data will be transmitted, processed, or stored by the vendor, (3) whether the vendor will share such data with other third parties, (4) whether the vendor will be given access to Company systems, and other risk factors.		Inspected vendor risk assessment documentation for the population of new vendor service providers that could impact the security and availability of Leaseweb Canada data centers to determine that the Company assessed the vendor based on their level of access and the scope of services performed.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
CC 3	Common Criteria Related to Risk Assessment	
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	
Management, with collaboration from Internal Audit, performs an annual risk assessment to identify internal and external risks, including those relevant to the industry, competition, IT infrastructure, cybersecurity, customer retention, capital investment, regulations, fraud, changes in the business model, changes in leadership, and other areas. The results of the assessment are communicated to management, and any deficiencies identified are tracked in a register through resolution.	Inspected the results of the most recent annual risk assessment to determine that internal and external risks are identified, assessed, and communicated to management. Inspected the maintained risk register to determine that identified internal and external risks and treatment activities were actively tracked until remediation.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	
Cybersecurity Risk Assessments are performed at least annually to assess risks and the controls in place to mitigate those risks. Risk items and related treatment plans are added to the risk register and tracked until remediation.	Inspected the results of the most recent Cybersecurity Risk Assessment to determine that the assessment is performed at least annually to identify risks and controls in place to mitigate them. Inspected the maintained risk register to determine that identified risks and treatment activities were actively tracked until remediation.	No exceptions noted.
Management, with collaboration from Internal Audit, performs an annual risk assessment to identify internal and external risks, including those relevant to the industry, competition, IT infrastructure, cybersecurity, customer retention, capital investment, regulations, fraud, changes in the business model, changes in leadership, and other areas. The results of the assessment are communicated to management, and any deficiencies identified are tracked in a register through resolution.	Inspected the results of the most recent annual risk assessment to determine that internal and external risks are identified, assessed, and communicated to management. Inspected the maintained risk register to determine that identified internal and external risks and treatment activities were actively tracked until remediation.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
CC 3	Common Criteria Related to Risk Assessment	
Formalized vendor risk assessments are performed for new vendor service providers that could impact the security and availability of Leaseweb Canada data centers. Risks considered include, as applicable, (1) any access a vendor will have to facilities and data, including access to confidential or restricted data, (2) how Company data will be transmitted, processed, or stored by the vendor, (3) whether the vendor will share such data with other third parties, (4) whether the vendor will be given access to Company systems, and other risk factors.	Inspected vendor risk assessment documentation for the population of new vendor service providers that could impact the security and availability of Leaseweb Canada data centers to determine that the Company assessed the vendor based on their level of access and the scope of services performed.	No exceptions noted.
Servers supporting the colocation data center services are scanned in real-time for vulnerabilities and misconfigurations. Patches are applied on a monthly basis to remediate identified issues.	Inspected scanning configurations to determine that servers supporting the colocation data center services are scanned in real-time for vulnerabilities and misconfigurations. Inspected patch tracking documentaion from the period to determine that patches are applied on a monthly basis to the servers supporting the colocation data center services.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
CC 4	Common Criteria Related to Monitoring Activities	
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	
Company data center power and environmental conditions are monitored and reported via automated monitoring systems. Appropriate personnel receive and monitor alerts regarding the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	Inspected the BMS monitoring dashboards, system configurations, and alert logs from the period to determine that data center power and environmental conditions were monitored and reported via automated monitoring systems.	No exceptions noted.
Appropriate personnel track data center power, environmental, and other incidents that may affect data center availability. Incidents are escalated as necessary and tracked until resolution.	Inspected the BMS monitoring and reporting system and event log to determine that appropriate personnel track data center power, environmental, and other incidents that may affect data center availability. Inspected the incident and availability log from the period to determine that incidents were tracked within through remediation.	No exceptions noted.
Data center power and cooling capacity reports are prepared at least monthly to assist Data Center Operations management in maintaining, monitoring, and evaluating power and cooling capacity needs.	Inspected the data center power and cooling capacity reports for a sample of months to determine that data center power and cooling capacity reports were prepared to assist Data Center Operations management maintain, monitor, and evaluate power and cooling capacity needs.	No exceptions noted.
A smoke detection system is installed in each in-scope data center to detect and alert data center personnel to the presence of a fire. Each critical smoke detection system is inspected and serviced at least annually to ensure effective operation.	Observed the smoke detection systems to determine that a smoke detection system was installed in each data center to detect and alert data center personnel to the presence of a fire. Inspected the most recent smoke detection system preventative maintenance reports for each in-scope data center to determine that the smoke detection systems are inspected and serviced at least annually to ensure effective operation.	No exceptions noted.
Multiple HVAC units control both temperature and humidity within each in-scope data center, delivering redundant HVAC service throughout the data center. HVAC units are inspected and serviced at least annually to ensure effective operation.	Observed the HVAC units within each data center to determine that multiple HVAC units were utilized to control both temperature and humidity. Inspected the HVAC preventative maintenance reports for each in-scope data center to determine that HVAC units are inspected and serviced at least annually to ensure effective operation.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
CC 4	Common Criteria Related to Monitoring Activities	
Redundant UPS systems are in place to provide temporary power in the event of a power failure and to mitigate the risk of power surges impacting infrastructure in each in-scope data center. UPS systems are inspected and serviced at least annually to ensure effective operation.	Observed the UPS systems within each data center to determine that redundant UPS systems were utilized to provide temporary power in the event of a power failure and mitigate the risk of power surges impacting the data center infrastructure. Inspected the UPS preventative maintenance reports for each in-scope data center to determine that UPS systems are inspected and serviced at least annually to ensure effective operation.	No exceptions noted.
Multiple diesel generators are in place to provide backup power in the event of a power outage at each in-scope data center. Generators are inspected and serviced at least annually to ensure effective operation.	Observed the diesel generator systems within each data center to determine that multiple diesel generators were utilized to provide backup power in the event of a power outage. Inspected the backup generators preventative maintenance reports for each in-scope data center to determine that the generators are inspected and serviced during the review period to ensure effective operation.	No exceptions noted.
The operating effectiveness of backup power systems at each in-scope data center are confirmed at least annually, through load bank testing and/or other methods.	Inspected the most recently performed backup power system test results for each in-scope data center to determine that the operating effectiveness of backup power systems were tested at least annually through load bank testing and/or other methods.	No exceptions noted.
Management, with collaboration from Internal Audit, performs an annual risk assessment to identify internal and external risks, including those relevant to the industry, competition, IT infrastructure, cybersecurity, customer retention, capital investment, regulations, fraud, changes in the business model, changes in leadership, and other areas. The results of the assessment are communicated to management, and any deficiencies identified are tracked in a register through resolution.	Inspected the results of the most recent annual risk assessment to determine that internal and external risks are identified, assessed, and communicated to management. Inspected the maintained risk register to determine that identified internal and external risks and treatment activities were actively tracked until remediation.	No exceptions noted.
Access to in-scope systems is reviewed at least annually by management to help ensure that access is commensurate with job responsibilities.	Inspected the most recently performed in-scope system user access reviews to determine access is reviewed at least annually by management to help ensure that access is commensurate with job responsibilities.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
CC 4	Common Criteria Related to Monitoring Activities	
Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to appropriate personnel for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.	Inspected network monitoring tool dashboards and configurations to determine that they are in place to detect unauthorized access to the network. Inspected alert logs from the period to determine that issues and incidents related to network security are escalated as necessary and tracked to resolution.	No exceptions noted.
Servers supporting the colocation data center services are scanned in real-time for vulnerabilities and misconfigurations. Patches are applied on a monthly basis to remediate identified issues.	Inspected scanning configurations to determine that servers supporting the colocation data center services are scanned in real-time for vulnerabilities and misconfigurations. Inspected patch tracking documentaion from the period to determine that patches are applied on a monthly basis to the servers supporting the colocation data center services.	No exceptions noted.
User access to add, modify, and delete users in the Company's keycard system is reviewed for appropriateness based on job responsibilities on an annual basis.	Inspected the review of users with access to add, modify, and delete users in the Company's keycard system to determine that the users are reviewed for appropriateness based on job responsibilities on an annual basis.	No exceptions noted.
The Company employs 24 hour video surveillance to monitor all entrances, exits, and other sensitive areas of its data centers. The video surveillance footage is retained for at least 90 days.	Observed video surveillance cameras at entrances, exits, and other sensitive areas to determine that entrances, exits, and sensitive areas of each in-scope data center were monitored. Inspected historical surveillance video footage to determine that recordings were retained for at least 90 days at each Company data center.	No exceptions noted.
Company data centers are monitored 24/7/365 by security equipment such as cameras, data center access management, data center personnel or facilities personnel.	Observed the security desk at each Company to determine that data centers were monitored 24/7/365 by security equipment such as cameras, data center access management, and Company personnel. Inspected the on-call schedule to determine that personnel are made available 24/7/365 to respond to incidents affecting the data centers.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
CC 4	Common Criteria Related to Monitoring Activities	
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	
Appropriate personnel track data center power, environmental, and other incidents that may affect data center availability. Incidents are escalated as necessary and tracked until resolution.	Inspected the BMS monitoring and reporting system and event log to determine that appropriate personnel track data center power, environmental, and other incidents that may affect data center availability. Inspected the incident and availability log from the period to determine that incidents were tracked within through remediation.	No exceptions noted.
Management, with collaboration from Internal Audit, performs an annual risk assessment to identify internal and external risks, including those relevant to the industry, competition, IT infrastructure, cybersecurity, customer retention, capital investment, regulations, fraud, changes in the business model, changes in leadership, and other areas. The results of the assessment are communicated to management, and any deficiencies identified are tracked in a register through resolution.	Inspected the results of the most recent annual risk assessment to determine that internal and external risks are identified, assessed, and communicated to management. Inspected the maintained risk register to determine that identified internal and external risks and treatment activities were actively tracked until remediation.	No exceptions noted.
Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to appropriate personnel for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.	Inspected network monitoring tool dashboards and configurations to determine that they are in place to detect unauthorized access to the network. Inspected alert logs from the period to determine that issues and incidents related to network security are escalated as necessary and tracked to resolution.	No exceptions noted.
Servers supporting the colocation data center services are scanned in real-time for vulnerabilities and misconfigurations. Patches are applied on a monthly basis to remediate identified issues.	Inspected scanning configurations to determine that servers supporting the colocation data center services are scanned in real-time for vulnerabilities and misconfigurations. Inspected patch tracking documentation from the period to determine that patches are applied on a monthly basis to the servers supporting the colocation data center services.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
CC 5	Common Criteria Related to Control Activities	
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	
Cybersecurity Risk Assessments are performed at least annually to assess risks and the controls in place to mitigate those risks. Risk items and related treatment plans are added to the risk register and tracked until remediation.	Inspected the results of the most recent Cybersecurity Risk Assessment to determine that the assessment is performed at least annually to identify risks and controls in place to mitigate them. Inspected the maintained risk register to determine that identified risks and treatment activities were actively tracked until remediation.	No exceptions noted.
Management, with collaboration from Internal Audit, performs an annual risk assessment to identify internal and external risks, including those relevant to the industry, competition, IT infrastructure, cybersecurity, customer retention, capital investment, regulations, fraud, changes in the business model, changes in leadership, and other areas. The results of the assessment are communicated to management, and any deficiencies identified are tracked in a register through resolution.	Inspected the results of the most recent annual risk assessment to determine that internal and external risks are identified, assessed, and communicated to management. Inspected the maintained risk register to determine that identified internal and external risks and treatment activities were actively tracked until remediation.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	
Cybersecurity Risk Assessments are performed at least annually to assess risks and the controls in place to mitigate those risks. Risk items and related treatment plans are added to the risk register and tracked until remediation.	Inspected the results of the most recent Cybersecurity Risk Assessment to determine that the assessment is performed at least annually to identify risks and controls in place to mitigate them. Inspected the maintained risk register to determine that identified risks and treatment activities were actively tracked until remediation.	No exceptions noted.
Management, with collaboration from Internal Audit, performs an annual risk assessment to identify internal and external risks, including those relevant to the industry, competition, IT infrastructure, cybersecurity, customer retention, capital investment, regulations, fraud, changes in the business model, changes in leadership, and other areas. The results of the assessment are communicated to management, and any deficiencies identified are tracked in a register through resolution.	Inspected the results of the most recent annual risk assessment to determine that internal and external risks are identified, assessed, and communicated to management. Inspected the maintained risk register to determine that identified internal and external risks and treatment activities were actively tracked until remediation.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
CC 5	Common Criteria Related to Control Activities	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	
Each Company controlled data center has a detailed Data Center Operations Manual which is available to Data Center Operations personnel and includes emergency procedures, contact information, and data center equipment details, monitoring and/or maintenance requirements. Each Data Center Operations Manual is reviewed and approved by management as needed.	Inspected the Data Center Operations Manual for the Company data centers to determine that each had a Manual available to Data Center Operations personnel, procedures were documented, internal control requirements were specified, and the Manual was reviewed and approved by management as needed.	No exceptions noted.
An employment prescreening process is performed for new hires, which includes background, credit, and DMV checks (based on job requirements) being completed prior to hire.	Inspected prescreening documentation for a sample of new hires to determine that Human Resources ran background, credit, and/or DMV checks prior to hire.	No exceptions noted.
Leaseweb Canada has an annual objective setting process and employee evaluation process. During these periods, managers and employees discuss and assess expectations regarding performance; roles and responsibilities, including internal controls; ethics; integrity; and training needs. Human Resources tracks completion and results of the assessment procedure.	Inspected the performance evaluation template to determine that expectations regarding performance, ethics, integrity, and training needs were part of the objective setting and employee evaluation process. Inspected results of the most recently performed performance evaluation cycle to determine that Human Resources tracked completion and results of the annual assessment.	No exceptions noted.
The Company maintains policies and procedures pertaining to IT, including Information Security, Change Management, and other policies for operations and conduct. These are reviewed and approved by management as needed and available to employees on the internal Wiki	Inspected Company policies and procedures pertaining to Information Security, Change Management, and Incident Response to determine that they are maintained and approved by management. Inspected the internal Wiki to determine that Company policies and procedures are made available to employees.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories			
Service Organization Control Activity		Test Performed by the Service Auditor	Test Results
CC 6	Common Criteria Related to Logical and Physical Access Controls		
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
	Roles based access to applications ensures privileges and authorizations associated with user accounts provide access to specific limited system functionality.	Inspected the user access listings for the in-scope systems to determine that privileges and authorizations were assigned based on the users' roles.	No exceptions noted.
	Access to the network and in-scope systems is restricted by requiring passwords or other system specific authentication control protocols. Password length, complexity, change, and account lockout requirements are established for systems in accordance with company policy. In instances where system limitations prevent implementation, policy exemptions are documented.	Observed login screens for the network and applications to determine user authentication was required to access the system and applications. Inspected the Password Policy and network and application password and account lockout settings to determine that the systems were configured to enforce minimum password length, complexity, periodic password rotation, and account lockout requirements in accordance with policy.	No exceptions noted.
	The Company has firewalls in place to limit access over the internet for internal corporate networks.	Inspected the network diagrams and firewall rules for the in-scope data centers to determine that firewalls were in place to limit access over the internet to corporate networks.	No exceptions noted.
	Connections via VPN tunnel between Company locations are protected using encryption. Connections to applications via the Internet are protected using encryption. VPN connections for user workstations outside the network require two factor authentication.	Inspected VPN configurations to determine that connections between Company locations and connections to internal applications via the Internet are protected using encryption. Inspected the configuration for the remote access VPN to determine that VPN connections for user workstations outside the network require two factor authentication.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
	Access to the network and in-scope systems is properly approved by Human Resources, management, and/or authorized system owner.	Inspected access provisioning documentation for a sample of new hires to determine that access to the network and in-scope systems is properly approved by Human Resources, management, and/or authorized system owner and is appropriate based on job responsibilities.	No exceptions noted.
	Terminated employee system access is removed by IT in accordance with Company policy.	Inspected access removal documentation for a sample of terminated employees to determine that access to the network and in-scope systems is removed in accordance with Company policy.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
CC 6	Common Criteria Related to Logical and Physical Access Controls	
Access to in-scope systems is reviewed at least annually by management to help ensure that access is commensurate with job responsibilities.	Inspected the most recently performed in-scope system user access reviews to determine access is reviewed at least annually by management to help ensure that access is commensurate with job responsibilities.	No exceptions noted.
User access to add, modify, and delete users in the Company's keycard system is reviewed for appropriateness based on job responsibilities on an annual basis.	Inspected the review of users with access to add, modify, and delete users in the Company's keycard system to determine that the users are reviewed for appropriateness based on job responsibilities on an annual basis.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
Access to the network and in-scope systems is properly approved by Human Resources, management, and/or authorized system owner.	Inspected access provisioning documentation for a sample of new hires to determine that access to the network and in-scope systems is properly approved by Human Resources, management, and/or authorized system owner and is appropriate based on job responsibilities.	No exceptions noted.
Terminated employee system access is removed by IT in accordance with Company policy.	Inspected access removal documentation for a sample of terminated employees to determine that access to the network and in-scope systems is removed in accordance with Company policy.	No exceptions noted.
Roles based access to applications ensures privileges and authorizations associated with user accounts provide access to specific limited system functionality.	Inspected the user access listings for the in-scope systems to determine that privileges and authorizations were assigned based on the users' roles.	No exceptions noted.
Access to in-scope systems is reviewed at least annually by management to help ensure that access is commensurate with job responsibilities.	Inspected the most recently performed in-scope system user access reviews to determine access is reviewed at least annually by management to help ensure that access is commensurate with job responsibilities.	No exceptions noted.
User access to add, modify, and delete users in the Company's keycard system is reviewed for appropriateness based on job responsibilities on an annual basis.	Inspected the review of users with access to add, modify, and delete users in the Company's keycard system to determine that the users are reviewed for appropriateness based on job responsibilities on an annual basis.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
CC 6	Common Criteria Related to Logical and Physical Access Controls	
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	
In order to gain physical access to Company data centers, individuals must be validated via a combination of key card and/or biometric technology.	Observed successful and unsuccessful attempts to gain physical access to each data center to determine that employees and customers must be validated by keycard and/or biometric technology.	No exceptions noted.
Customer equipment in Company data centers is segregated via locked cages or locked cabinets to ensure that customers can only access their own equipment. Lock mechanisms are combination, badge reader, or physical key.	Observed the location of customer equipment within the in-scope data centers to determine that the equipment is segregated via locked cages or cabinets using a combination lock, badge reader, or physical key that is only accessible by customers.	No exceptions noted.
For employees and customers that are given permanent physical access badges to Company data centers, access is properly approved during the onboarding process.	Inspected access provisioning documentation for the population of new customers with access to the in-scope data centers to determine that access is properly approved during the onboarding process. Inspected access provisioning documentation for the population of new employees with access to the in-scope data centers to determine that access is properly approved during the onboarding process.	No exceptions noted.
Visitor and contractor access to Company data centers is logged at the entrance via a tablet device. Customers can register in advance for their visit with Customer Care, or onsite with a Company representative. Proper identification is provided to visitors and / or personnel.	Observed the visitor and contractor check-in process at the in-scope data centers to determine that access is logged at the entrance via a tablet device. Observed the badges provided to visitors and contractors to determine that the identification is unique and clearly distinguishable from permanent access badges.	No exceptions noted.
Quarterly audits are performed to validate the appropriateness of all employee and customer physical access to Leaseweb Canada data centers. Any necessary actions are documented and performed.	Inspected the results of quarterly physical access audits for a sample of quarters to determine that the audits were performed to validate the appropriateness of employee and customer physical access to the data centers, and any necessary actions are documented and performed.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories			
Service Organization Control Activity		Test Performed by the Service Auditor	Test Results
CC 6	Common Criteria Related to Logical and Physical Access Controls		
Physical access to Company data centers is revoked in accordance with Company policy for terminated employees and customers with permanent physical access badges.		Inspected access removal documentation for the population of terminated employees with access to in-scope data centers to determine that removal of access to Company data centers is performed in accordance with Company policy. Inspected access removal documentation for the population of terminated customers to determine that removal of access to Company data centers is performed in accordance with Company policy.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity’s objectives.		
The disposal of data is the responsibility of the client. Therefore, this criterion is not applicable.			
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
Employees have the capability to report potential phishing attempts and other issues to appropriate personnel. Information is provided via email to both alert and help educate employees when potential security issues are observed.		Inspected email reporting configurations to determine that employees have the capability to report potential phishing attempts and other issues to appropriate personnel. Inspected the security awareness training results from the period to determine that each in-scope employee completed security awareness training to help educate employees on potential security issues.	No exceptions noted.
The Company has firewalls in place to limit access over the internet for internal corporate networks.		Inspected the network diagrams and firewall rules for the in-scope data centers to determine that firewalls were in place to limit access over the internet to corporate networks.	No exceptions noted.
Connections via VPN tunnel between Company locations are protected using encryption. Connections to applications via the Internet are protected using encryption. VPN connections for user workstations outside the network require two factor authentication.		Inspected VPN configurations to determine that connections between Company locations and connections to internal applications via the Internet are protected using encryption. Inspected the configuration for the remote access VPN to determine that VPN connections for user workstations outside the network require two factor authentication.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories			
Service Organization Control Activity		Test Performed by the Service Auditor	Test Results
CC 6	Common Criteria Related to Logical and Physical Access Controls		
Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to appropriate personnel for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.		Inspected network monitoring tool dashboards and configurations to determine that they are in place to detect unauthorized access to the network. Inspected alert logs from the period to determine that issues and incidents related to network security are escalated as necessary and tracked to resolution.	No exceptions noted.
Antivirus software is used on in scope workstations and servers and configured to accept automatic software updates and periodically scan for malware. In instances where system limitations prevent implementation, policy exemptions are documented.		Inspected antivirus configurations and asset exports to determine that antivirus software is installed on in scope workstations and servers. Inspected the antivirus settings to determine that antivirus software was configured to accept automatic updates and periodically scan for malware.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		
The disposal of data is the responsibility of the client. Therefore, this criterion is not applicable.			
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
Changes to the in-scope systems monitoring the security and availability of the data centers must be reviewed and approved by the Change Advisory Board (CAB) and/or IT management before being implemented. Approvals and testing plans, if applicable, are documented within the ticketing system.		Inspected change tickets for the population of changes made to the in-scope systems monitoring the security and availability of the data centers to determine that they were reviewed and approved by the CAB and/or IT management and included testing plans within the ticket.	No exceptions noted.
Access to in-scope systems is reviewed at least annually by management to help ensure that access is commensurate with job responsibilities.		Inspected the most recently performed in-scope system user access reviews to determine access is reviewed at least annually by management to help ensure that access is commensurate with job responsibilities.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
CC 6	Common Criteria Related to Logical and Physical Access Controls	
Servers supporting the colocation data center services are scanned in real-time for vulnerabilities and misconfigurations. Patches are applied on a monthly basis to remediate identified issues.	Inspected scanning configurations to determine that servers supporting the colocation data center services are scanned in real-time for vulnerabilities and misconfigurations. Inspected patch tracking documentaion from the period to determine that patches are applied on a monthly basis to the servers supporting the colocation data center services.	No exceptions noted.
Antivirus software is used on in scope workstations and servers and configured to accept automatic software updates and periodically scan for malware. In instances where system limitations prevent implementation, policy exemptions are documented.	Inspected antivirus configurations and asset exports to determine that antivirus software is installed on in scope workstations and servers. Inspected the antivirus settings to determine that antivirus software was configured to accept automatic updates and periodically scan for malware.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories			
Service Organization Control Activity		Test Performed by the Service Auditor	Test Results
CC 7	Common Criteria Related to System Operations		
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		
Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to appropriate personnel for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.		Inspected network monitoring tool dashboards and configurations to determine that they are in place to detect unauthorized access to the network. Inspected alert logs from the period to determine that issues and incidents related to network security are escalated as necessary and tracked to resolution.	No exceptions noted.
Servers supporting the colocation data center services are scanned in real-time for vulnerabilities and misconfigurations. Patches are applied on a monthly basis to remediate identified issues.		Inspected scanning configurations to determine that servers supporting the colocation data center services are scanned in real-time for vulnerabilities and misconfigurations. Inspected patch tracking documentaion from the period to determine that patches are applied on a monthly basis to the servers supporting the colocation data center services.	No exceptions noted.
Antivirus software is used on in scope workstations and servers and configured to accept automatic software updates and periodically scan for malware. In instances where system limitations prevent implementation, policy exemptions are documented.		Inspected antivirus configurations and asset exports to determine that antivirus software is installed on in scope workstations and servers. Inspected the antivirus settings to determine that antivirus software was configured to accept automatic updates and periodically scan for malware.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity’s ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
Company data center power and environmental conditions are monitored and reported via automated monitoring systems. Appropriate personnel receive and monitor alerts regarding the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.		Inspected the BMS monitoring dashboards, system configurations, and alert logs from the period to determine that data center power and environmental conditions were monitored and reported via automated monitoring systems.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity		Test Results
CC 7	Common Criteria Related to System Operations	
Appropriate personnel track data center power, environmental, and other incidents that may affect data center availability. Incidents are escalated as necessary and tracked until resolution.	Inspected the BMS monitoring and reporting system and event log to determine that appropriate personnel track data center power, environmental, and other incidents that may affect data center availability. Inspected the incident and availability log from the period to determine that incidents were tracked within through remediation.	No exceptions noted.
Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to appropriate personnel for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.	Inspected network monitoring tool dashboards and configurations to determine that they are in place to detect unauthorized access to the network. Inspected alert logs from the period to determine that issues and incidents related to network security are escalated as necessary and tracked to resolution.	No exceptions noted.
Servers supporting the colocation data center services are scanned in real-time for vulnerabilities and misconfigurations. Patches are applied on a monthly basis to remediate identified issues.	Inspected scanning configurations to determine that servers supporting the colocation data center services are scanned in real-time for vulnerabilities and misconfigurations. Inspected patch tracking documentation from the period to determine that patches are applied on a monthly basis to the servers supporting the colocation data center services.	No exceptions noted.
Antivirus software is used on in scope workstations and servers and configured to accept automatic software updates and periodically scan for malware. In instances where system limitations prevent implementation, policy exemptions are documented.	Inspected antivirus configurations and asset exports to determine that antivirus software is installed on in scope workstations and servers. Inspected the antivirus settings to determine that antivirus software was configured to accept automatic updates and periodically scan for malware.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	
Significant incidents affecting data center physical security and/or availability are analyzed to identify the root cause. Recovery actions are taken as applicable and corrective action plans are put into place, as necessary, to prevent, detect and respond to future incidents.	Inspected the incident and availability log from the period to determine that there were no significant incidents affecting data center physical security and/or availability during the period.	Control not tested. The circumstances that warrant the operation of the control did not occur during the period.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
CC 7	Common Criteria Related to System Operations	
Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to appropriate personnel for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.	Inspected network monitoring tool dashboards and configurations to determine that they are in place to detect unauthorized access to the network. Inspected alert logs from the period to determine that issues and incidents related to network security are escalated as necessary and tracked to resolution.	No exceptions noted.
Cybersecurity incidents are analyzed to identify the root cause. Recovery actions are taken as applicable, corrective action plans are put into place and the incident response plan and recovery procedures are updated as necessary to prevent, detect and respond to future cybersecurity incidents.	Inspected MDR report logs during the period to determine that there were no security events that rose to the level of a cybersecurity incident during the period.	Control not tested. The circumstances that warrant the operation of the control did not occur during the period.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	
Significant incidents affecting data center physical security and/or availability are analyzed to identify the root cause. Recovery actions are taken as applicable and corrective action plans are put into place, as necessary, to prevent, detect and respond to future incidents.	Inspected the incident and availability log from the period to determine that there were no significant incidents affecting data center physical security and/or availability during the period.	Control not tested. The circumstances that warrant the operation of the control did not occur during the period.
Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to appropriate personnel for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.	Inspected network monitoring tool dashboards and configurations to determine that they are in place to detect unauthorized access to the network. Inspected alert logs from the period to determine that issues and incidents related to network security are escalated as necessary and tracked to resolution.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
CC 7 Common Criteria Related to System Operations		
Cybersecurity incidents are analyzed to identify the root cause. Recovery actions are taken as applicable, corrective action plans are put into place and the incident response plan and recovery procedures are updated as necessary to prevent, detect and respond to future cybersecurity incidents.	Inspected MDR report logs during the period to determine that there were no security events that rose to the level of a cybersecurity incident during the period.	Control not tested. The circumstances that warrant the operation of the control did not occur during the period.
A Global Incident Management process is documented and in place. This is reviewed and approved by management as needed and is available to employees on the internal Wiki.	Inspected the Global Incident Management Process to determine that it was documented, reviewed and approved by management as needed, and made available to employees on the internal Wiki.	No exceptions noted.
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.		
The company's Business Continuity Plan (BCP) is reviewed and updated as needed. As part of the BCP, threats that could impair the availability of data centers are identified and ranked by overall risk (determined by likelihood and impact). Annual testing of the BCP is conducted and updates to the Plan are considered based on test results.	Inspected the BCP to determine that the BCP considered environmental threats that could impair data center availability, risks were ranked, and the BCP was reviewed and updated as needed. Inspected documentation to determine that the Company updates the BCP based on lessons learned from BCP tests results and other material events.	No exceptions noted.
Significant incidents affecting data center physical security and/or availability are analyzed to identify the root cause. Recovery actions are taken as applicable and corrective action plans are put into place, as necessary, to prevent, detect and respond to future incidents.	Inspected the incident and availability log from the period to determine that there were no significant incidents affecting data center physical security and/or availability during the period.	Control not tested. The circumstances that warrant the operation of the control did not occur during the period.
Cybersecurity incidents are analyzed to identify the root cause. Recovery actions are taken as applicable, corrective action plans are put into place and the incident response plan and recovery procedures are updated as necessary to prevent, detect and respond to future cybersecurity incidents.	Inspected MDR report logs during the period to determine that there were no security events that rose to the level of a cybersecurity incident during the period.	Control not tested. The circumstances that warrant the operation of the control did not occur during the period.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity		Test Results
CC 8	Common Criteria Related to Change Management	
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	
Changes to the in-scope systems monitoring the security and availability of the data centers must be reviewed and approved by the Change Advisory Board (CAB) and/or IT management before being implemented. Approvals and testing plans, if applicable, are documented within the ticketing system.	Inspected change tickets for the population of changes made to the in-scope systems monitoring the security and availability of the data centers to determine that they were reviewed and approved by the CAB and/or IT management and included testing plans within the ticket.	No exceptions noted.
The Company has in place a Change Management process to ensure all scheduled maintenance and other data center implementations / modifications are properly documented and authorized to assure minimal impact to customers. For scheduled maintenance and other changes that have the potential to affect customer availability, customers are notified of the maintenance or change in advance.	Inspected the Company's Change Management process to determine that the Company has formalized procedures to ensure all scheduled maintenance and other data center implementations / modifications are properly documented and authorized to assure minimal impact to customers. Inspected documentation for a sample of data center maintenance and implementation events to determine that the changes followed the Change Management process, including obtaining formal authorization and communicating the change to customers, when necessary.	No exceptions noted.
The Company maintains policies and procedures pertaining to IT, including Information Security, Change Management, and other policies for operations and conduct. These are reviewed and approved by management as needed and available to employees on the internal Wiki	Inspected Company policies and procedures pertaining to Information Security, Change Management, and Incident Response to determine that they are maintained and approved by management. Inspected the internal Wiki to determine that Company policies and procedures are made available to employees.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
CC 9	Common Criteria Related to Risk Mitigation	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	
The company's Business Continuity Plan (BCP) is reviewed and updated as needed. As part of the BCP, threats that could impair the availability of data centers are identified and ranked by overall risk (determined by likelihood and impact). Annual testing of the BCP is conducted and updates to the Plan are considered based on test results.	Inspected the BCP to determine that the BCP considered environmental threats that could impair data center availability, risks were ranked, and the BCP was reviewed and updated as needed. Inspected documentation to determine that the Company updates the BCP based on lessons learned from BCP tests results and other material events.	No exceptions noted.
Insurance policies are obtained to offset the financial impact of loss events that would potentially impair the company in achieving its objectives. Property/casualty insurance is obtained for the Company flagship data centers and cybersecurity insurance is obtained for the company as a whole.	Inspected the general liability insurance to determine y insurance was obtained for the Company's flagship data centers. Inspected the cybersecurity insurance policy to determine that cybersecurity insurance was obtained for the Company as a whole.	No exceptions noted.
A Global Incident Management process is documented and in place. This is reviewed and approved by management as needed and is available to employees on the internal Wiki.	Inspected the Global Incident Management Process to determine that it was documented, reviewed and approved by management as needed, and made available to employees on the internal Wiki.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	
Attestation reports for all vendor service providers that could affect the security and availability of the Company data centers are reviewed at least annually by management.	Inspected the attestation report review for the vendor service provider that could affect the security and availability of the Company data centers to determine that the reviews are conducted at least annually.	No exceptions noted.
The scope of services agreed to with new vendor service providers which could impact the security and availability of the Company data centers, as well as any compliance or security requirements and SLAs that the vendor must adhere to, are documented in contractual agreements with the vendor.	Inspected signed agreements with the population of new vendor service providers that could impact the security and availability of the Company data centers to determine that the scope of services and security requirements are documented.	No exceptions noted.

Common Criteria to All In-Scope Trust Services Categories		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
CC 9	Common Criteria Related to Risk Mitigation	
Formalized vendor risk assessments are performed for new vendor service providers that could impact the security and availability of Leaseweb Canada data centers. Risks considered include, as applicable, (1) any access a vendor will have to facilities and data, including access to confidential or restricted data, (2) how Company data will be transmitted, processed, or stored by the vendor, (3) whether the vendor will share such data with other third parties, (4) whether the vendor will be given access to Company systems, and other risk factors.	Inspected vendor risk assessment documentation for the population of new vendor service providers that could impact the security and availability of Leaseweb Canada data centers to determine that the Company assessed the vendor based on their level of access and the scope of services performed.	No exceptions noted.

Availability Criteria		
Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
A	Additional Criteria for Availability	
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	
Data center power and cooling capacity reports are prepared at least monthly to assist Data Center Operations management in maintaining, monitoring, and evaluating power and cooling capacity needs.	Inspected the data center power and cooling capacity reports for a sample of months to determine that data center power and cooling capacity reports were prepared to assist Data Center Operations management maintain, monitor, and evaluate power and cooling capacity needs.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	
Backups on in-scope systems monitoring the security and availability of the data centers are performed according to the defined backup schedule.	Inspected backup configurations and logs for in-scope systems to determine that backups are performed in accordance with the defined backup schedule.	No exceptions noted.
Restoration testing is performed at least annually to test the integrity of critical infrastructure backups.	Inspected the most recently performed backup restoration test results to determine that the test was performed at least annually to test the integrity of critical infrastructure backups.	No exceptions noted.

Availability Criteria		
Service Organization Control Activity		Test Results
A	Additional Criteria for Availability	
The company's Business Continuity Plan (BCP) is reviewed and updated as needed. As part of the BCP, threats that could impair the availability of data centers are identified and ranked by overall risk (determined by likelihood and impact). Annual testing of the BCP is conducted and updates to the Plan are considered based on test results.	Inspected the BCP to determine that the BCP considered environmental threats that could impair data center availability, risks were ranked, and the BCP was reviewed and updated as needed. Inspected documentation to determine that the Company updates the BCP based on lessons learned from BCP tests results and other material events.	No exceptions noted.
Each Company controlled data center has a detailed Data Center Operations Manual which is available to Data Center Operations personnel and includes emergency procedures, contact information, and data center equipment details, monitoring and/or maintenance requirements. Each Data Center Operations Manual is reviewed and approved by management as needed.	Inspected the Data Center Operations Manual for the Company data centers to determine that each had a Manual available to Data Center Operations personnel, procedures were documented, internal control requirements were specified, and the Manual was reviewed and approved by management as needed.	No exceptions noted.
Company data center power and environmental conditions are monitored and reported via automated monitoring systems. Appropriate personnel receive and monitor alerts regarding the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	Inspected the BMS monitoring dashboards, system configurations, and alert logs from the period to determine that data center power and environmental conditions were monitored and reported via automated monitoring systems.	No exceptions noted.
Appropriate personnel track data center power, environmental, and other incidents that may affect data center availability. Incidents are escalated as necessary and tracked until resolution.	Inspected the BMS monitoring and reporting system and event log to determine that appropriate personnel track data center power, environmental, and other incidents that may affect data center availability. Inspected the incident and availability log from the period to determine that incidents were tracked within through remediation.	No exceptions noted.
Significant incidents affecting data center physical security and/or availability are analyzed to identify the root cause. Recovery actions are taken as applicable and corrective action plans are put into place, as necessary, to prevent, detect and respond to future incidents.	Inspected the incident and availability log from the period to determine that there were no significant incidents affecting data center physical security and/or availability during the period.	Control not tested. The circumstances that warrant the operation of the control did not occur during the period.

Availability Criteria		
Service Organization Control Activity		Test Results
A	Additional Criteria for Availability	
A smoke detection system is installed in each in-scope data center to detect and alert data center personnel to the presence of a fire. Each critical smoke detection system is inspected and serviced at least annually to ensure effective operation.	Observed the smoke detection systems to determine that a smoke detection system was installed in each data center to detect and alert data center personnel to the presence of a fire. Inspected the most recent smoke detection system preventative maintenance reports for each in-scope data center to determine that the smoke detection systems are inspected and serviced at least annually to ensure effective operation.	No exceptions noted.
Each in-scope data center is protected from the risk of fire by a pre-action, dry pipe sprinkler fire suppression system, as well as fire extinguishers located throughout the data center. Each critical pre-action, dry pipe sprinkler fire suppression system is inspected and serviced at least annually, and fire extinguishers are inspected and serviced at least annually, to ensure effective operation.	Observed the pre-action, dry pipe sprinkler fire suppression systems and fire extinguishers in-place at the in-scope data centers to determine the data centers were protected against risk of fire. Inspected the fire suppression system and fire extinguisher maintenance reports for each in-scope data center to determine that the data centers' fire suppression systems and fire extinguishers are serviced at least annually to ensure effective operation.	No exceptions noted.
Multiple HVAC units control both temperature and humidity within each in-scope data center, delivering redundant HVAC service throughout the data center. HVAC units are inspected and serviced at least annually to ensure effective operation.	Observed the HVAC units within each data center to determine that multiple HVAC units were utilized to control both temperature and humidity. Inspected the HVAC preventative maintenance reports for each in-scope data center to determine that HVAC units are inspected and serviced at least annually to ensure effective operation.	No exceptions noted.
Redundant UPS systems are in place to provide temporary power in the event of a power failure and to mitigate the risk of power surges impacting infrastructure in each in-scope data center. UPS systems are inspected and serviced at least annually to ensure effective operation.	Observed the UPS systems within each data center to determine that redundant UPS systems were utilized to provide temporary power in the event of a power failure and mitigate the risk of power surges impacting the data center infrastructure. Inspected the UPS preventative maintenance reports for each in-scope data center to determine that UPS systems are inspected and serviced at least annually to ensure effective operation.	No exceptions noted.

Availability Criteria		
Service Organization Control Activity		Test Results
A	Additional Criteria for Availability	
Multiple diesel generators are in place to provide backup power in the event of a power outage at each in-scope data center. Generators are inspected and serviced at least annually to ensure effective operation.	Observed the diesel generator systems within each data center to determine that multiple diesel generators were utilized to provide backup power in the event of a power outage. Inspected the backup generators preventative maintenance reports for each in-scope data center to determine that the generators are inspected and serviced during the review period to ensure effective operation.	No exceptions noted.
The operating effectiveness of backup power systems at each in-scope data center are confirmed at least annually, through load bank testing and/or other methods.	Inspected the most recently performed backup power system test results for each in-scope data center to determine that the operating effectiveness of backup power systems were tested at least annually through load bank testing and/or other methods.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	
Restoration testing is performed at least annually to test the integrity of critical infrastructure backups.	Inspected the most recently performed backup restoration test results to determine that the test was performed at least annually to test the integrity of critical infrastructure backups.	No exceptions noted.
The company's Business Continuity Plan (BCP) is reviewed and updated as needed. As part of the BCP, threats that could impair the availability of data centers are identified and ranked by overall risk (determined by likelihood and impact). Annual testing of the BCP is conducted and updates to the Plan are considered based on test results.	Inspected the BCP to determine that the BCP considered environmental threats that could impair data center availability, risks were ranked, and the BCP was reviewed and updated as needed. Inspected documentation to determine that the Company updates the BCP based on lessons learned from BCP tests results and other material events.	No exceptions noted.
The operating effectiveness of backup power systems at each in-scope data center are confirmed at least annually, through load bank testing and/or other methods.	Inspected the most recently performed backup power system test results for each in-scope data center to determine that the operating effectiveness of backup power systems were tested at least annually through load bank testing and/or other methods.	No exceptions noted.



GLOBAL

For a complete listing of our member firms,
please visit: www.uhy.com/our-locations

866-993-6723

info@uhy-us.com

Audit | Tax | Advisor | Consulting

An independent member of UHY International