TeraGo Networks

End to End Data.

NETWORK | DATA | VOICE | CLOUD

TeraGo Networks, Inc.
Service Organization Controls 2 (AT101), Type 2 Report

DESCRIPTION OF SYSTEM, SUITABILITY OF DESIGN AND OPERATING EFFECTIVENESS FOR THE

HYBRID CLOUD HOSTING AND COLOCATION SYSTEM

RELEVANT TO SECURITY AND AVAILABILITY

For the Period of February 1, 2016 to January 31, 2017

auditwerx
A DIVISION OF CARR, RIGGS & INGRAM, LLC
AUDITWERX.COM

TABLE OF CONTENTS

SECTION 1: INDEPENDENT SERVICE AUDITORS’ REPORT

auditwerx
A DIVISION OF CARR, RIGGS & INGRAM CAPITAL, LLC

Auditwerx
3000 Bayport Drive
Suite 500
Tampa, FL 33607
866.446.4038 office
727.499.6867 fax
AUDITWERX.COM

INDEPENDENT SERVICE AUDITORS' REPORT

To the Management of TeraGo Networks, Inc.:

We have examined the description in Section 3 titled "Description of TeraGo Networks, Inc.'s Hybrid Cloud Hosting and Colocation System" (the "description") at the Mississauga Data Centre, Kelowna GigaCentre, Downtown Vancouver Data Centre, Toronto North Data Centre and Vancouver "The Vault" Data Centre facilities based on the criteria set forth in paragraph 1.26 of the AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®) (the "description criteria) and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the Security and Availability principles set forth in TSP Section 100, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, throughout the period February 1, 2016 to January 31, 2017.

TeraGo's Responsibilities

In Section 2, TeraGo Networks, Inc. ("TeraGo" or "Company") has provided its assertion titled "TeraGo's Assertion" about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. TeraGo is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; identifying the risks that would prevent the applicable trust services criteria from being met; designing, implementing, and documenting the controls to meet the applicable trust services criteria; and specifying the controls that meet the applicable trust services criteria and stating them in the description.

Auditwerx's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria if the controls operated effectively throughout the period February 1, 2016 to January 31, 2017.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria involves—

- evaluating and performing procedures to obtain evidence about whether the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period February 1, 2016 to January 31, 2017.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed and operating effectively.
- testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met.
- evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization in its assertion.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

The information in Section 5, "Other Information Provided by TeraGo Networks, Inc." that describes TeraGo's response to exceptions identified during testing, is presented by management of TeraGo to provide additional information and is not a part of TeraGo's description of its Hybrid Cloud Hosting and Colocation System made available to user entities during the period February 1, 2016 to January 31, 2017. TeraGo's response to the exception has not been subjected to the procedures applied in the examination of the description of the Hybrid Cloud Hosting and Colocation System and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the Hybrid Cloud Hosting and Colocation System and, accordingly, we express no opinion on it.

Opinion

In our opinion, except for the matters described in the preceding paragraphs, based on the description criteria identified in TeraGo's assertion and the applicable trust services criteria, in all material respects,

a. the description fairly presents the TeraGo Hybrid Cloud Hosting and Colocation System that was designed and implemented throughout the period February 1, 2016 to January 31, 2017.
b. the controls of TeraGo stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period February 1, 2016 to January 31, 2017.
c. the controls tested operated effectively to provide reasonable assurance that the applicable trust service criteria were met throughout the period February 1, 2016 to January 31, 2017.

Description of the Tests of Controls

The specific controls we tested, the tests we performed, and the results of our tests are listed in Section 4 "Information provided by Auditwerx."

Restricted Use

This report is intended solely for the information and use of TeraGo; user entities of the TeraGo Hybrid Cloud Hosting and Colocation System throughout the period February 1, 2016 to January 31, 2017; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

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

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

Auditwerx, LLC

Auditwerx, LLC, a Division of Carr, Riggs & Ingram Capital, LLC
Tampa, Florida

April 10, 2017

SECTION 2: TERAGO'S ASSERTION

TERAGO'S ASSERTION

We have prepared the description titled "Description of TeraGo Networks, Inc. Hybrid Cloud Hosting and Colocation System" (the "description") at the Mississauga Data Centre, Kelowna GigaCentre, Downtown Vancouver Data Centre, and Toronto North Data Centre and Vancouver "The Vault" Data Centre facilities based on the criteria for a description of a service organization's system identified in *paragraph 1.26 of the AICPA Guide, Reporting on Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (description criteria). The description is intended to provide users with information about the Hybrid Cloud Hosting and Colocation System, particularly system controls intended to meet the criteria for the security and availability principles set forth in *TSP 100, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services principles), throughout the period February 1, 2016 to January 31, 2017. We confirm, to the best of our knowledge and belief, that—

1) The description fairly presents the system throughout the period February 1, 2016 to January 31, 2017.

   a) The description contains the following information:

      i) The types of services provided.

      ii) The components of the system used to provide the services, which are as follows:

         (1) *Infrastructure.* The physical structures, IT and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).

         (2) *Software.* The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).

         (3) *People.* The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).

         (4) *Processes.* The automated and manual procedures.

         (5) *Data.* Transaction streams, files, databases, tables, and output used or processed by a system.

      iii) The boundaries or aspects of the system covered by the description.

      iv) For information provided to, or received from, subservice organizations, and other parties—

         (1) how the information is provided or received and the role of the subservice organizations and other parties.

(2) the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

v) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

(1) Complementary user entity controls contemplated in the design of the service organization's system.

(2) When the inclusive method is used to present a subservice organization, controls at the subservice organization.

vi) If the service organization presents the subservice organization using the carve-out method—

(1) the nature of the services provided by the subservice organization.

(2) each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.

vii) Any applicable trust services criteria that are not addressed by a control and the reasons.

viii) In the case of a Type 2 report, relevant details of changes to the service organization's system during the period covered by the description.

b) The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that each individual report user may consider important to its own particular needs.

2) The controls stated in the description, except for those noted below, were suitably designed throughout the period February 1, 2016 to January 31, 2017 to meet the applicable trust services criteria.

3) The controls stated in the description operated effectively throughout the period February 1, 2016 to January 31, 2017 to meet the applicable trust services criteria.

By: /S/ Anthony Scalzo

Anthony Scalzo
Director, IT and Cloud Services
April 10, 2017

SECTION 3: DESCRIPTION OF TERAGO’S HYBRID CLOUD HOSTING AND COLOCATION SYSTEM

DESCRIPTION OF TERAGO NETWORKS, INC.'S HYBRID CLOUD HOSTING AND COLOCATION SERVICES SYSTEM

COMPANY OVERVIEW

TeraGo Networks, Inc. ("TeraGo" or "Company") (TSX:TGO) is a facilities based communications provider, utilizing a variety of technologies to provide services to businesses across Canada, which include High Speed Internet, Voice Services, Data Networking, and Internet Redundancy as well as colocation and cloud services. TeraGo manages facilities nationwide for colocation as well as providing cloud services allowing clients to operate hybrid solutions should they desire. TeraGo provides colocation and disaster recovery services to businesses, government establishments, and technology service providers.

TeraGo offers a cost effective and secure location for those looking to expand their data centre capacity or outsource existing data centre services. TeraGo operational teams have expertise in data centre design, advanced networking and data centre management. The climate controlled, biometric secure server environments are an ideal location for companies looking to store their online business needs. TeraGo Data Centres are home to a variety of global clients, including Fortune 100 companies, public sector organizations and government agencies. The Data Centre facilities provide enterprises with secure, resilient wholesale colocation and disaster recovery solutions. The Company provides rack and floor space, electrical power, environmental control and a connection to the Internet. Users have the option manage their own equipment, utilize cloud services, or create a hybrid solution.

PRODUCTS AND SERVICES OVERVIEW

Server Services

This category of services provides server and storage capacity in highly customizable, highly scalable packages. These services are considered server outsourcing, as TeraGo owns and manages the computing assets and charges on a subscription basis for use of the resources.

Server Services are delivered under three models:

- Dedicated Servers – a physical device is dedicated to one customer.
- Virtual Servers – virtual operating environments, running on the same physical hardware that is shared by multiple customers.
- Cloud Servers – virtual environments running on a dynamic physical infrastructure (scalable array of devices) shared by multiple customers.

Virtual Servers offers more flexibility and cost-effectiveness than Dedicated Servers, while Cloud Servers offer more than both Virtual and Dedicated. The Legacy Internet Service Provider business falls primarily in the Dedicated and Virtual Server categories, although some Legacy customers are moving to Cloud services. Cloud services are considered the future mainstream computing delivery model in the ICT industry and are at the core of TeraGo's offering strategy.

Colocation Solutions

TeraGo offers colocation (or co-location) solutions provide clients reliable data centre solutions for enterprises of all sizes. Clients can utilize TeraGo's flexible colocation solutions including shared cabinets, private cabinets, private cages, and private colocation suites. The data centre environment operates in a carrier neutral colocation environment, providing clients multiple carrier solutions via the Managed-Meet-Me-Rooms (carrier point of presence). Features include:

- Single cabinet or dedicated, customized cage / suite tailored to meet client specific power and cooling requirements.
- Shared Racks offering provides enterprises server colocation solution for infrastructure 1U or more. Bundled with other data centre services such as Remote Hands and multi-homed network access and redundant power and infrastructure provides a complete turn-key data centre solution for enterprises.
- For Private Racks TeraGo offers enterprises seeking full 42U private cabinet colocation can take advantage of TeraGo's cost effective colocation starter packs provide 42U cabinets, redundant power and managed or carrier neutral network access. Enterprises who require additional services for their colocation environments can utilize TeraGo's technical team to assist in providing a vast array of support services including: logistics support, smart hands, and consulting services.
- Customizable options including: private cooling and power, private CCTV Feeds and biometric access systems provide a turnkey colocation solution for organizations seeking to collocate in a TeraGo data centre.

SYSTEM DESCRIPTION

TeraGo's system description covers the Data Centre System, which includes colocation services at the Mississauga Data Centre, Kelowna GigaCentre, Downtown Vancouver Data Centre, Toronto North Data Centre, and Vancouver "The Vault" Data Centre facilities.

The system is comprised of the following components:

a. Infrastructure (facilities, equipment, and networks)
b. Software (overview, key components, applications, and utilities)
c. People (functional areas, operators, users, and managers)
d. Procedures (automated, manual procedures involved in the operation of the system)
e. Data (transaction streams, files, databases, and tables)

The following sections of this description define each of these five components above that comprise the entire system.

Infrastructure

The following describes the infrastructure for each location:

Mississauga Data Centre, Ontario

A Tier 3 capable facility, located in Mississauga is equipped with 2N power, cooling and connectivity infrastructure, providing high levels of reliability and support. Also one of the locations for the hybrid cloud environments and back up location for the Kelowna GigaCentre.

Power

- Up to 4.8 MW total power available with full redundancy
- Clean power supplied by double conversion UPS
- 2N back-up power infrastructure, from two municipal diverse hydro substations dedicated to the complex
- Ten 600 kVa generators
- A/B power pre-configured in every cabinet

Cooling Systems

- Raised floor warm aisle, cold aisle configuration
- 2N Cooling Infrastructure
  - Chilled water towers and closed glycol loop
  - Independent air-cooled rooftop cooling units
  - 14 30-tonne CRAC units, supporting 1470 kVa

Fire Suppression

- Pre-action suppression system
- FM-200 fire suppression system
- Complex outfitted with proper fire and smoke alarm system

Security

- Multi-factor access authentication
- 24/7 video monitoring and manned security
- 24/7 monitoring by Network Operations Centre
- Security professional at complex main entrance
- Secure loading dock area

Kelowna GigaCentre, British Columbia

Kelowna's seismically stable geographic location, temperate climate and minimal probability of both natural and man-made events present a very low risk profile. Kelowna advantages include abundant diverse fiber networks and reliable hydroelectric power. The second of the two locations for the hybrid cloud environments and back up location for the Mississauga Data Centre.

Power

- 6MW power
- Redundant power & cooling infrastructure
- Powered by 'Green' hydro energy

Cooling & Fire Suppression

- Free cooling chillers and advantageous climate
- Cold aisle containment
- In-row coolers, backed by UPS

Connectivity

- Up to 10Gbs network capacity
- Carrier neutral access
- Redundant fiber into building from diverse carriers

Security & Monitoring

- Among the lowest risk locations in North America
- Secured and Monitored 24x7x365 with alarms, cameras, biometric access points and man traps
- Staff on-site 24×7

Toronto North Data Centre, Ontario

Located in Vaughan, Ontario, the North Toronto facility is located minutes away from Pearson International Airport (YYZ) and downtown Toronto, with easy access to all major highways.

Power

- Up to 1 MW total available power
- Clean power supplied by double conversion UPS
- A / B power available
- Generators located on site

Cooling & Fire Suppression

- Commercial-grade modular system
- Raised floor cooling
- Very Early Smoke Detection Apparatus (VESDA)
- Zoned pre-action dry pipe sprinkler system

Connectivity

- Carrier-neutral facility
- Fully-redundant and diverse fibre core fed from multiple providers including wireless backhaul

Security & Monitoring

- Multi-factor access authentication
- 24/7 video monitoring on facility perimeter
- 24/7 monitoring by Network Operations Centre
- Secure and private loading dock

The Vault – Vancouver Data Centre, British Columbia

The location was originally built for the Bank of Canada, to store gold bullion. Situated in downtown Vancouver, the facility is close to multiple SkyTrain stations, major driving routes, and the Vancouver International Airport.

Power

- 600 KW total available power
- Clean power supplied by double conversion UPS
- Two independent power feeds from separate grids
- Electrical sub-station separated from building power grid
- A/B power available in every cabinet

Cooling & Fire Suppression

- Chilled water system
- In-row APC cooling system
- Waterless, Inergen fire suppression system
- Very Early Smoke Detection Apparatus (VESDA)

Connectivity

- Carrier-neutral facility
- Fully-redundant and diverse fibre core fed by from multiple providers
- Access to TeraGo's fibre ring in downtown Vancouver – connecting their data centres and the Vancouver Telco Hotel (555 West Hastings St.)

Security & Monitoring

- Multi-factor access authentication
- 24/7 CCTV & access control monitoring
- 24/7 monitoring by Network Operations Centre
- Complex designed to withstand seismic activities

Downtown Vancouver Data Centre, British Columbia

Located in downtown Vancouver, the Downtown Vancouver data centre is strategically located in a pre-eminent property in the business district, within close proximity to several SkyTrain stations, major driving routes, and the Vancouver International Airport. Additionally, this data centre is only blocks away from their Vault facility location.

Power

- 600 KW power
- Clean power supplied by double conversion UPS
- A/B power available in every cabinet

Cooling & Fire Suppression

- Raised floor warm aisle, cold aisle configuration on data centre floor
- Waterless, FM-200 fire suppression system
- Zoned pre-action dry pipe sprinkler system

Connectivity

- Carrier neutral access
- Fully-Redundant and diverse fiber core fed from multiple providers
- Access to TeraGo's fibre ring in downtown Vancouver – connecting to their data centres the Vancouver Telco Hotel (555 West Hastings St.)

Security & Monitoring

- Multi-factor access authentication
- 24/7 manned security at building entrance
- 24/7 CCTV & Access Control monitoring by Network Operations Centre (NOC)

Software

With the exception of software applications utilized to the monitoring of TeraGo physical security access controls, environmental security controls and communications infrastructure, TeraGo does not provide software applications utilized by its clients, software applications are the responsibility of clients subscribing to TeraGo colocation services.

People

See Roles and Responsibilities for the Company organization chart.

Policies and Procedures

Policies

TeraGo maintains a suite of comprehensive policies designed to provide both management's stated direction (policy) and staff working practices (procedures). These documents are distributed to all new hires by human resources (HR).

Policies address the reasons for security; the rules and procedures required to achieve security; and the personnel and roles who work to enforce the security policies. The exact details of the policy are presented elsewhere. The following table lists an example of the policy documents that have been adopted by TeraGo.

Policies	Description
Acceptable Use Policy for Employees Acceptable Use Policy for Clients Software Policy	Policies governing how computing resources may be used
Confidentiality & Non-Disclosure Agreement Electronic Messaging	Policies related to the creation, exposure and disposal of data, both corporate and client
Security Policy Administrative Access Control Role Based Security	Policies that cover the security of network attached resources and the network infrastructure that serves these resources
Change Management	Rules and procedures covering actions that affect the ongoing maintenance and availability of a secure infrastructure
Telecommuting Policy Encryption	Policies covering the security of Information Technology assets

Procedures

Information Security

The Company has an approved policy that enables the implementation of information security appropriate to the complexity of the Company's IT environment. The information security policy is detailed in the employee handbook. The policy includes within its scope all aspects of the IT environment relevant to financial reporting applications and data (e.g., application security, operation system security, infrastructure security, acceptable systems use). The policy is communicated to all relevant users.

The handbook is provided to all new employees upon hiring and is available to all current employees through the intranet site. The policies described in the handbook include: acceptable use, software, electronic messaging, and email signature.

TeraGo's network consists of host and remote central office digital switches and loop carriers interconnected with copper and fiber facilities. The outside plan infrastructure connect the customer with the core network consists of a mix of fiber optic and copper facilities. There is a fully integrated communications network that consists of IP routers, Ethernet switches, and switches capable of handling voice, data, and dedicated circuits.

Security is critical to the physical network, computer operating systems, and application programs. Each area offers its own set of security issues and risks. The Company has implemented a comprehensive security program that offers a high level of protection corresponding with the value of the assets. The information security program provides reasonable protection against unauthorized access, disclosure, modification, or destruction, as well as to assure the availability, integrity, usability, authenticity, and confidentiality of information. This applies to all systems that manage or store data.

Human Resource Policies and Practices

HR policies and practices are documented in the employee handbook. The policies include controls for hiring, training, evaluating, promoting, and compensating employees. All prospective employees and contractors are subject to screening procedures, which allow the Company to avoid hiring candidates, who are not suitable for the position or who are of poor moral character. Employees will be required to acknowledge all company policies and procedures.

The Company provides access to relevant systems such as WHMCS (Web Hosting Billing and Automation System), Solarwinds, Navision, and other in scope systems only for those employees that require access for a valid business purpose. The IT director controls the granting and removal of system access rights (segregation of duties). There is no default access provided to any system upon hiring. When a new employee is hired, the employee's manager will establish if the user requires access a particular system or program. Upon receipt of an approved request form for access from the hiring manager by the HR department, an email is sent to the IT support team requesting that the appropriate system access be established. Requests outside the standard role definitions must be approved at the VP level. Similar to the process for new hires, a request for any changes in the level of access to the in-scope applications must be approved by the employee's manager prior to the implementation of changes in access by IT. When the IT department receives the new request form, the employee's profile will be modeled based on an employee with a similar role.

When an employee has been terminated or resigns, as part of the exit process, the HR specialist will forward an email to the IT support team who will suspend/remove their access rights immediately. In certain cases (e.g. for terminations) this removal may occur prior to the employee receiving notification of termination.

Access change requests for new employees or changes in job functions/requirements require approval of a department manager prior to IT granting access. IT will not grant access without such approval notification. The department managers review the requests for appropriateness based on the employee's job description. HR procedures for employee leaving the company (termination/ resignation) require that IT be notified on a timely basis to revoke the person's system access. The HR director reviews that this notification occurs as part of review of the exit package. IT revokes access on a timely basis.

Super User Identification

The Company maintains super-user identifications that serve as domain administrator user accounts. These accounts have the ability to manipulate the level of access for users of in-scope applications, therefore provide/restrict additional functions. Access to these super-user accounts is restricted to IT department.

Acceptable Use Policy

An Acceptable Use Policy was developed to guide staff on the appropriate use of Company computers, information systems, and adherence to security policies.

Non-Disclosure and Confidentiality Agreement

Employees, Contractors and Clients must sign a non-disclosure agreement as acknowledgment not to disclose proprietary or confidential information, including client information, to unauthorized parties.

Disciplinary Process

A Disciplinary Process has been developed to remediate future employee violations of the data centre security policies.

Infrastructure Change

An Infrastructure Change management policy and procedures to document and approve changes to the data centre infrastructure has been developed and implemented and will be tested for operating effectiveness in subsequent audits.

Data

Access to data is limited to authorized personnel in accordance with the Company's security policies. IT is also responsible for the overall availability of data, including system backups, monitoring of data processing and file transmissions as well as identifying and resolving problems. The data TeraGo obtains is usually sensitive to each client. It contains login, server, network, and application information for the client.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT, INFORMATION AND COMMUNICATION, AND MONITORING

CONTROL ENVIRONMENT

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. The control environment has a pervasive influence on the structure of business activities, establishment of objectives, and assessment of risks. It influences control activities, information and communication systems, and monitoring procedures. The control environment is influenced by an entity's history and managerial culture. Effectively controlled entities strive to have competent personnel, instill an enterprise-wide attitude of integrity and control consciousness, and set a positive corporate direction. These entities establish appropriate controls that foster shared values and teamwork in pursuit of the organization's objectives.

Control environment elements include the following, and the extent to which each element is addressed at TeraGo is described below:

- Management Controls, Philosophy, and Operating Style
- Integrity and Ethical Values
- Organizational Structure
- Assignment of Authority and Responsibility
- Standard Operating Controls
- Risk Management
- Monitoring

Management Controls, Philosophy, and Operating Style

Management is responsible for directing and controlling operations; establishing, communicating, and monitoring control policies and procedures; and setting the tone for the organization. Importance is placed on accuracy and integrity, maintaining written and updated procedures, security and privacy, and establishing and maintaining sound internal controls over all functional aspects of operations.

Management's philosophy and operating style affect the way TeraGo is managed, including the kinds of business risks accepted. TeraGo places a great deal of importance on working to ensure that the integrity of processing is a primary focus and that controls are maximized to mitigate risk in daily operations. Management and specific teams are structured to ensure the highest level of integrity and efficiency in customer support and transaction processing.

Formal job descriptions and regular departmental/divisional meetings and staff interactions ensure communication of organizational values, ethics, and behavior standards. Personnel operate under TeraGo's policies and procedures, including confidentiality agreements and security policies. Periodic training is conducted to communicate regulations and the importance of privacy and security. Management is committed to being aware of regulatory and economic changes that impact lines of business and monitoring customer base for trends, changes, and anomalies.

Competence should reflect the knowledge and skills needed to accomplish tasks that define an individual's job. Through consideration of an entity's objectives and the strategies and plans for achievement of those objectives, management must determine how well these tasks need to be accomplished. Management has identified the competence levels for particular jobs and translated those levels into requisite knowledge and skills.

Integrity and Ethical Values

Maintaining a climate that demands integrity and ethical values is critical to the establishment and maintenance of an effectively controlled organization. The effectiveness of internal controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. TeraGo has programs and policies designed to promote and ensure integrity and ethical values in its environment.

TeraGo desires to maintain a safe, pleasant, and cooperative working environment and expects employees to have high standards of performance, integrity, productivity, and professionalism. TeraGo has developed professional conduct policies that set forth policies of importance to all employees relating to ethics, values, and conduct. All employees are expected to know and adhere to these standards, as well as to generally accepted norms of conduct and courtesy at all times. While managers are responsible for understanding, communicating, and enforcing Company policies, this does not override or diminish an employee's individual responsibility to be aware of and adhere to these policies. Violations of these policies or other forms of misconduct may lead to disciplinary or corrective action up to and including dismissal.

Standards of Conduct

TeraGo has implemented standards of conduct to guide all employee and contractor behavior. Management monitors behavior closely, and exceptions to these standards lead to immediate corrective action as defined by HR policies and procedures. Any employee found to have violated TeraGo's ethics policy may be subject to disciplinary action, up to and including termination of employment.

Commitment to Competence

TeraGo has formal job descriptions that define roles and responsibilities and the experience and background required to perform jobs in a professional and competent fashion. TeraGo determines the knowledge and skills needed to perform job duties and responsibilities and hires for that skill set and job requirement. Management monitors and formally evaluates employee and contractor performance on a periodic basis to determine that performance meets or exceeds TeraGo's standards.

Organizational Structure

TeraGo's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Significant aspects of establishing a relevant organizational structure include defining key areas of authority and responsibility and establishing appropriate lines of reporting. Significant cross-training between management positions and between staff positions exists to help ensure smooth operations and maintenance of controls during staff or management absence.

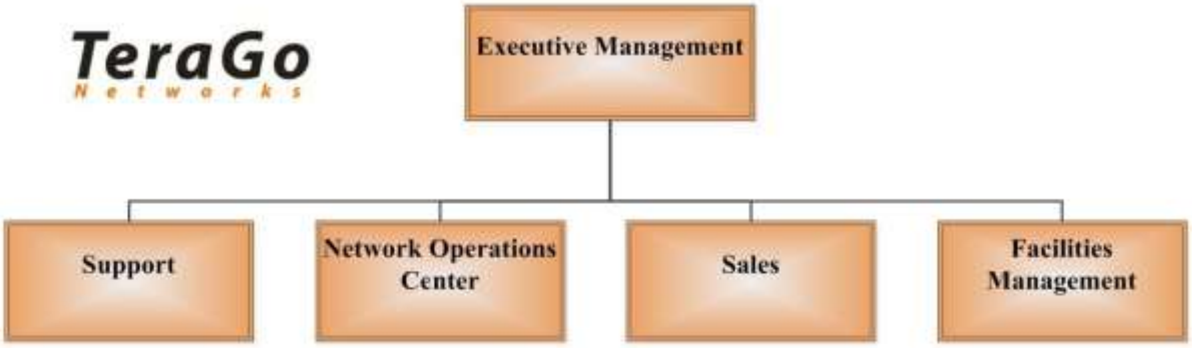
Assignment of Authority and Responsibility

The extent to which individuals recognize that they are held accountable influences the control environment. This holds true for everyone who has ultimate responsibility for activities within an entity, including the internal control system. This includes assignment of authority and responsibility for operating activities, and establishment of reporting relationships and authorization protocols. TeraGo's management encourages individuals and teams to use initiative in addressing issues and resolving problems. Policies describing appropriate business practices, knowledge and experience of key personnel, and available resources are provided to employees in order to assist them in carrying out their duties.

TeraGo is led by its CEO who has delegated to a team of Managers with the skills and experience necessary to carry out their assignments. Such assignments commonly relate to achieving corporate objectives, oversight of operating functions, and any compliance with applicable regulatory requirements. Open dialogue and individual initiative are encouraged as fundamental parts of TeraGo's goal to deliver client service.

Roles and Responsibilities

The following organizational chart depicts TeraGo's corporate structure.



Standard Operating Controls

TeraGo's management provides guidance to employees regarding expected levels of integrity, ethical behavior, and competence. Such practices relate to hiring, orientation, training, evaluation, counseling, promotion, compensation, and remedial actions. TeraGo has hiring practices that are designed to help ensure that new employees are qualified for their job responsibilities.

TeraGo invests significant resources in employee development by providing on-the-job training and other learning opportunities. New employees participate in an orientation program that acquaints them with TeraGo's organization, functions, values, products, and selected policies. Thereafter, development activities include providing more challenging assignments, job rotation, training programs, seminars, and continuing education programs. Additionally, employees are provided with measurable objectives and are subject to periodic performance reviews to help ensure competence. Managers give each of their employees at least one formal written performance appraisal per year.

Customer Experience and Service Delivery

The Customer Experience and Service Delivery Group is made up of three technical teams: Account Success Managers (ASMs), Technical Operations Team and the Network Operations Centre.

The ASM team is made up of customer experience specialists whose primary focus is to act as a communications conduit and customer advocate between the client and TeraGo. The ASM team is managed by the Manager of Client Success.

The Technical Operations team consists of subject matter specialists. These team members are responsible for implementation, configuration, management, and maintenance of systems relating to IT and Cloud Services, in addition to being points of escalation for the Network Operations Centre. This team is overseen by the Manager of IT.

The Network Operations Centre is made up from a multi-tier technical support team.

Their Priorities are to react appropriately to all inbound support requests and/or alerts and to escalate as needed. This technical team is overseen by the Director of Operations. These teams overlap to encourage mentorship and cross training as well as to ensure technical support matters have an unobstructed technical support escalation path.

RISK ASSESSMENT

Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to the achievement of Company objectives and forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.

Management is proactive in identifying the risks that threaten client commitments. Risk assessment efforts include analyses of threats, probabilities of occurrence, potential business impacts, and associated mitigation plans. Risk mitigation strategies include prevention and elimination through the implementation of internal controls and transference of risk through insurance policies.

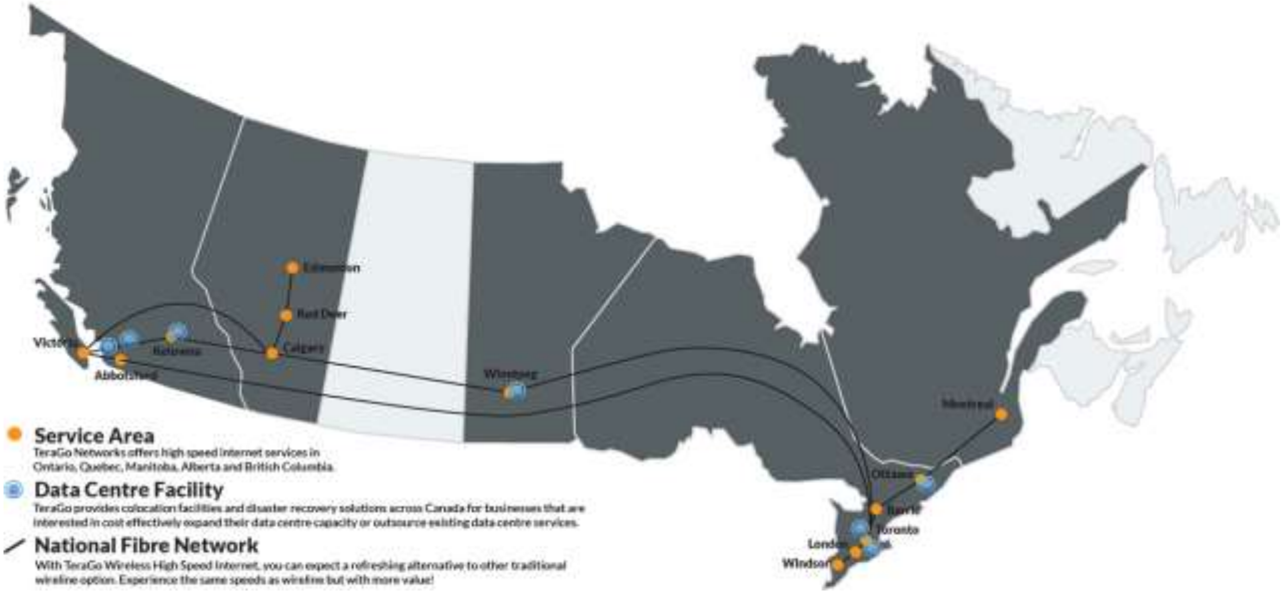
INFORMATION AND COMMUNICATION

TeraGo uses a variety of methods for communication to ensure that significant events and issues are conveyed in a timely manner and that staff understand their role and responsibility over services and controls. These methods include the following: new hire training, ongoing security awareness training, employee handbooks, policy and process updates, weekly departmental meetings summarizing events and changes, use of email and instant messaging to communicate time-sensitive information, and the documentation and storage of historical data in internal repositories for business and support activities. TeraGo maintains systems that manage the flow of information and facilitate communication with its customers.

TeraGo facilities utilize diverse fiber uplinks from diverse carriers leveraged through our parent organization TeraGo Networks, who operate a national fiber network with diverse paths. TeraGo's access network leverages international peering using connections to internet exchange points in Seattle (SIX) and Toronto (TorIX), as well as local connectivity through major Canadian providers using geographically-diverse peering locations. The links feed into fully meshed 10gbps core routing infrastructure using the Cisco Data Centre 3.0 topology model utilized by the TeraGo Data Centre facilities.

This configuration increases reliability, while at the same time providing the flexibility necessary to overcome localized Internet bottlenecks that can affect overall performance. The geographic separation provides lower cross-country round trip times, access to prime peering relationships, and east-west diversity for increased resiliency against major events.

TeraGo Data Centre facilities are carrier neutral and allow for connection to any network provider, as well as offer access and WAN connectivity using the TeraGo network in order to provide multiple internet options and reliable service availability.


Edmonton
Red Deer
Calgary
Victoria
Kelowna
Abbotsford
Winnipeg
Montreal
Ottawa
Barrie
Toronto
London
Windsor
● Service Area
TeraGo Networks offers high speed internet services in Ontario, Quebec, Manitoba, Alberta and British Columbia.
● Data Centre Facility
TeraGo provides colocation facilities and disaster recovery solutions across Canada for businesses that are interested in cost effectively expand their data centre capacity or outsource existing data centre services.
National Fibre Network
With TeraGo Wireless High Speed Internet, you can expect a refreshing alternative to other traditional wireline option. Experience the same speeds as wireline but with more value!

Core Network Description

TeraGo utilizes Cisco Nexus devices to ensure maximum uptime and optimum performance for network traffic in TeraGo Data Centre Facilities.

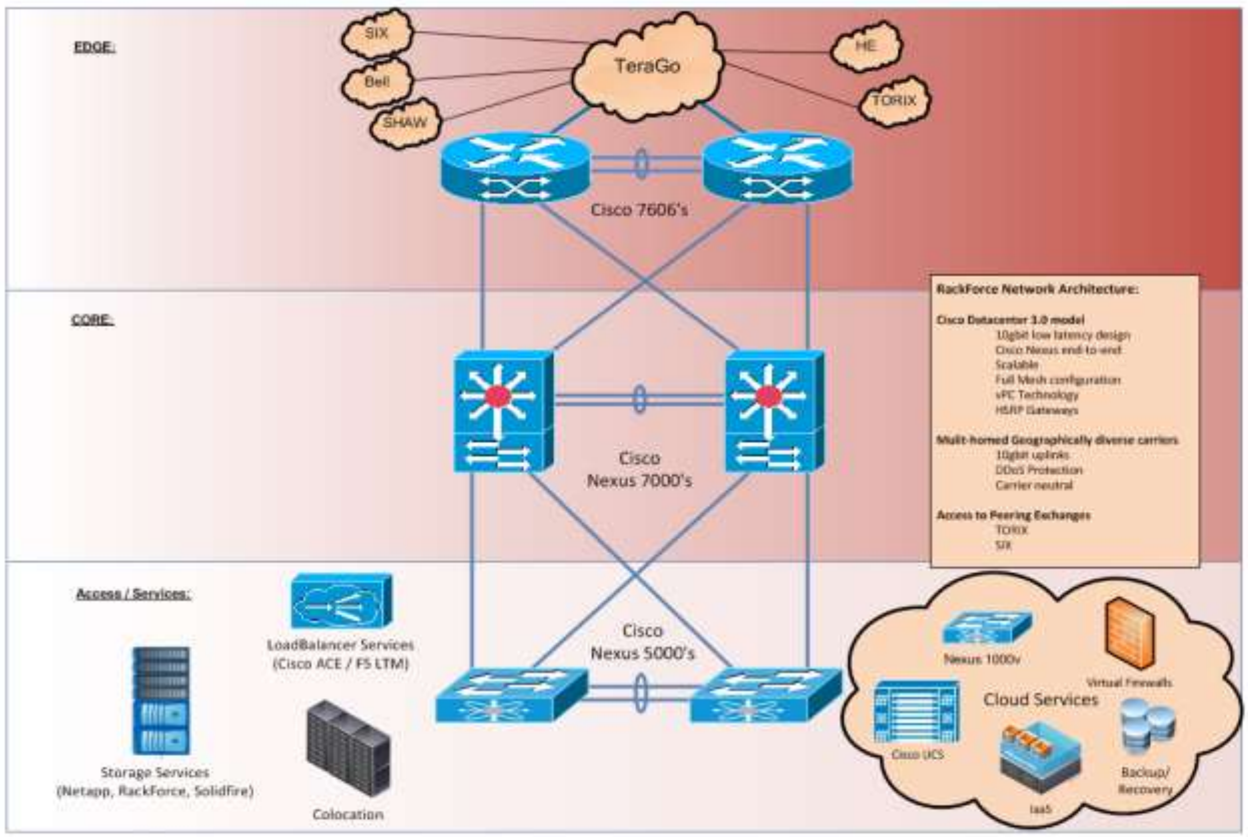
Dedicated customer Virtual Local Area Networks (VLAN) are used to logically segment customers on the TeraGo network into different broadcast domains so that packets are only switched between ports that are designated on the same VLAN. Firewalls protecting customers from the public network and from the Internet are implemented when selected. Managed network options are available to be configured, and managed by experienced Internet security specialists.

Firewalls are configured with Access Control Lists (ACL) which prevent access to private internal Internet protocol (IP) addresses and deny access to all non-administrative ports. All non-administrative ports are closed by default. Administrative activity by TeraGo staff on customer servers is restricted and controlled through the use of vendor accounts. Accessing the vendor account by TeraGo staff must be authorized by the customer administrator.

TeraGo staff access to customer servers is restricted and controlled through the use of vendor accounts. Accessing the vendor account by TeraGo staff must be authorized by the customer administrator.

Network Diagram

Network Architecture



Physical Security

Data Centre Physical Security

The facility main entrance is secured with a mantrap using both a proximity card and biometric access control system (ACS) to gain entry into the facility. All other exterior entrances are secured using a proximity cards and biometric ACS. The facility is configured with multiple security zones used to segment the interior spaces with varying degrees of sensitivity. All guests are enrolled into the badge ACS and issued a temporary badge with limited access. Data centre personnel are required to display their identity badges at all times when onsite at the TeraGo facility.

Mantraps and two-factor authentication are used to gain access to data centre areas. The system uses electromechanical locks controlled by biometric authentication and key-cards. Pre-authorized customers are given unescorted access to their specific area within the data centre. Only authorized TeraGo personnel have access to high security data centre areas. The system is administered by TeraGo onsite security personnel.

Closed circuit video surveillance has been installed at all critical areas within the data centre. Entry attempts at any door within the facility are recorded providing a video log with each access attempt. Security personnel can select any entry event and view the recorded image taken at the time the event occurred. All customer equipment is located in secured, locked pods. Facility is alarmed and monitored with offsite alarm monitoring services.

Data Centre Power

The data centre is equipped with Uninterruptible Power Supplies (UPS) to mitigate the risk of short-term utility power failures and fluctuations. The UPS power subsystems are N+1 redundant with instantaneous failover in the event of a primary power failure. Customers may select dual path power from independent N+1 UPS systems providing them 2 (N+1) resiliency. The UPS systems are inspected on a regular basis. The data centre facility is also equipped with diesel generators to mitigate the risk of long-term utility power failures and fluctuations. The generators configuration are also N+1 and are tested regularly and maintained to provide assurance of appropriate operability.

Data Centre Cooling

The data centre features N+1 redundant heating ventilation air conditioning (HVAC) units which provide consistent temperature and humidity within the raised floor areas. Cooling mechanisms include either Computer Room Air Conditioning (CRAC) units or in-row coolers. Closed loop glycol or water systems have been constructed with redundant, rotating coolant pumps. Water sensors are placed throughout the facilities and around critical coolant lines to ensure early detection of moisture. Regular inspections of the HVAC units and all components are performed by TeraGo personnel as well as third-party vendors.

Data Centre Fire Detection and Suppression

Detection sensors are installed in the ceiling of the data centre areas. Fire detection equipment is monitored remotely 24x7x365. Suppression devices include handheld extinguishers and a fixed double lockout dry pipe sprinkler system. Fire detection and suppression features include:

- Smoke sensors
- Heat sensors
- Remote 24x7x365 monitoring
- Handheld fire extinguishers
- Fixed double lock-out dry pipe sprinkler system

Data Centre Environmental Monitoring and Support

Manned 24x7x365, the Network Operations Centre (NOC) monitors all HVAC, fire suppression, and security systems onsite by specially trained personnel. Additionally, critical airflows, temperature, humidity, power consumption by individual customer, early warning fire identification and suppression systems, generators, chillers, CRAC units, in-row coolers, and all security systems are monitored in real-time from the NOC.

Monitoring policies and procedures are utilized for addressing issues relating to outages of critical services or other issues needing immediate action. These procedures vary based on the severity level of the problem. TeraGo support teams receive customer problem reports, and utilize an online problem tracking and reporting system to assist in the following:

- Logging the problem report (ticketing)
- Ticket tracking
- Routing and documenting all actions through problem resolution

Network Perimeter Security

The following are complementary types of network security perimeter devices used by the Company on its network to defend Internet-accessible systems:

- Firewall
- Demilitarized Zone (DMZ)
- Network Address Translation (NAT)
- Intrusion Detection System (IDS)
- Virtual Private Network (VPN)

Firewall

TeraGo utilizes firewalls at the perimeter of its network to protect against threats from the Internet. The firewalls protect TeraGo's local area network (LAN) from the WAN environment. The firewalls are also used for VPN management for gateway-to-gateway connections as well as gateway-to-user connections.

The firewall devices provide user and application policy enforcement, multi-vector attack protection, and secure connectivity services through a wide range of security and networking services in a unified threat management platform including:

- Advanced application-aware firewall services
- Site-to-site and remote access IPSec VPN connectivity
- Intelligent networking services
- Flexible management solutions

DMZ

Network computers exposed to the Internet can subject the entire network to hacker attacks. This can lead to compromised data, viruses, and other types of malicious acts that could damage TeraGo's credibility and operations.

A DMZ has been established to isolate TeraGo computers from the Internet. A DMZ is a small network of computers exposed to the external world (Internet). Identifiable security incidents occurring on the DMZ are evaluated, and steps are taken to mitigate those issues and further reduce the risk of breaches of the DMZ.

NAT

TeraGo uses the technique of NAT on the main Internet firewall to provide hidden Internet addresses to internal Company computers. This effectively mitigates the possibility of external sources finding the addresses of internal Company computers.

NAT allows computers on a private network to access the Internet through an intermediary called the Network Address Translator. The Network Address Translator examines all packets destined for the Internet, removes the private IP address from the IP header, substitutes the address of the NAT public interface, and forwards it to the destination. When the resource at the destination IP address responds to the request, the Network Address Translator receives it, checks its internal table to see which client the packet belongs to, and forwards it to the proper client.

IDS

An Intrusion Detection System (IDS) detects unwanted manipulations to computer systems, mainly through the Internet. The manipulations may take the form of attacks by hackers.

An Intrusion Detection System (IDS) is used to detect many types of malicious network traffic and computer usage that cannot be detected by a conventional firewall. This includes network attacks against vulnerable services; data-driven attacks on applications; host-based attacks such as privilege escalation, unauthorized logins, and access to sensitive files; and malware (viruses, Trojan horses, and worms). An Intrusion Detection System (IDS) is composed of several components:

- Sensors that generate security events
- A console to monitor events, alerts, and control the sensors
- A central engine that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received

VPN

Virtual Private Networking is used to provide secure, encrypted communication between a network and a remote host or other remote networks over the public Internet. VPNs allow the establishment of an encrypted tunnel that protects the flow of network traffic from eavesdroppers.

VPN is used to allow remote users to access the Company's internal network. Users authenticate with the VPN concentrator and then authenticate with the Windows domain to gain access to network resources. Three levels of access rights are implemented based on the type of users accessing the network. Strong VPN authentication and encryption protocols are in use.

Computer Operations

Systems Monitoring

TeraGo's Information Technology (IT) Team regularly monitors the customer-hosted network for capacity, performance, and hardware failure. Overall database health and capacity planning are monitored daily to ensure the system will meet the needs of TeraGo's clients. IT monitors security access violations, including server logs and reports.

Monitoring policies and procedures are utilized for addressing issues relating to outages of critical services or other issues needing immediate action. These procedures vary based on the defined severity level of the problem.

TeraGo engineers use several monitoring tools to identify and provide alerts to the following conditions:

- A managed system has exceeded a predefined performance or load threshold.
- A managed system has suffered an error condition.
- A managed system has detected a hardware element that is expected to fail in the near future.
- A managed system is no longer in communication with the monitoring infrastructure.
- A managed system has entered a condition previously specified by Company engineers as operating outside of a threshold.

Patch Deployment

TeraGo takes a proactive approach to patch management. TeraGo engineers regularly monitor various Web sites, message boards, and mailing lists where advanced notification of bug and related patches is often disclosed prior to public announcement by the vendor. This allows TeraGo to plan ahead for upcoming patches.

TeraGo engineers consider each patch carefully and independently to determine if it is necessary to deploy it within the production environment. In many cases, the vulnerability being addressed by the patch has been mitigated through any number of other countermeasures already in place such as firewalls, the intrusion prevention system, or an aspect of their hardening process. In these cases, patches may be deferred until they are included in a future service pack. If TeraGo engineers decide that the patch is necessary and should be deployed, the patch is tested. Once the patch has been thoroughly tested, it is approved for deployment in the production environment.

Logical Access

Access to resources and data is granted to individuals based on their job responsibilities. New user accounts are established only upon receipt of properly authorized requests. The Company Security Officer (CSO) or the Alternate Company Security Officer (ACSO) are the security administrators and are responsible for ensuring adherence to the security policies that address logical access control procedures.

Unique user IDs and passwords are assigned to each individual user. Password rules are established according to the TeraGo's security policy, which requires a minimum of alphanumeric characters with password complexity requirements. Passwords are systematically required to be changed periodically. The system administrator sets the user's initial password. The user is required to change the password at first logon.

Individual access capabilities are removed immediately by IT upon the notification of termination of employment, change of responsibilities, or termination of a contract with a client that uses the system. System security access levels are periodically reviewed by IT to ensure individual access rights are appropriate based on job information.

User accounts and access rights are managed on the domain controllers employing the Internet-standard Kerberos network authentication protocol to authenticate both the client and the network, and to protect against the possibility of unauthorized users impersonating a server to enter the network.

Database software maintains their respective client databases. The databases are only accessible through the software application and are protected from unauthorized access. No direct network access is granted to this software or the servers that it runs on to anyone other than those granted by IT management.

Data Backup and Restore

Backup

TeraGo has implemented various backup methods as part of its production operations. TeraGo has a multi-layered strategy for protecting critical data files to meet client requirements. This strategy includes using an online storage management backup system where targeted files are backed up to a SAN. A predefined number of copies of backed up files are stored on this online SAN device per the client’s retention agreements. Backup files are then replicated over a secured Layer 2 Network connection to a SAN at TeraGo's offsite facility. Using an automated process, backup jobs are run using a backup utility whereby the target files are identified in predefined backup jobs. The backup system is monitored by the IT department.

Restore

Restore testing is performed through the course of normal operations and as part of periodic testing. It involves restoring files from the online storage management system, where predefined iterations of files exist based on client retention agreements. This dramatically increase the mean time to recovery (MTTR) by reducing the time needed to restore system data.

Infrastructure Change Management

TeraGo has a formal change management process in place to ensure only authorized updates and changes are implemented to customer systems and production networks. Controls are in place to properly authorize, test, and implement changes. TeraGo has developed a change ticket process whereby no changes to the infrastructure or production systems can take place without the proper approval and scheduling. Change tickets dealing with operational changes typically originate from internal staff and frontline support staff. Once logged in the issue tracking system change tickets are routed to the appropriate technical group for assessment and approval. Once approved, the work is put on the calendar to be carried out by a qualified technician.

MONITORING

TeraGo's management performs monitoring activities as part of normal business operations to assess the quality of the internal control environment. Management performs regular reviews of tasks assigned to their teams. Monitoring activities are used to initiate corrective action through team meetings, client conference calls, and informal notifications. Corrective actions are taken as required to correct deviations from company policy and procedures. Tasks that are not addressed in a timely manner are manually escalated and resolved.

TRUST SERVICES CRITERIA AND RELATED CONTROLS

TeraGo's trust services criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them here in Section 3 and repeating them in Section 4. Although the trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of TeraGo's description of controls.

USER CONTROL CONSIDERATIONS

TeraGo's applications are designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report.

This section describes additional controls that should be in operation at user organizations to complement the controls at the Company for Colocation services. User auditors should consider whether or not the following controls have been placed in operation at the user organizations:

- User entities are responsible for requesting and authorizing changes that would impact their systems located in the data centre facilities.
- User entities are responsible for administrating and monitoring all aspects of logical security over their servers and systems located in the data centre facilities.
- User entities are responsible for ensuring that system maintenance on their servers and applications located at the data centre facilities is appropriate for their needs.
- User entities are responsible for ensuring backups, changing backup media and monitoring the availability and recovery of their systems located at the data centre facility is appropriate for their needs.

- User entities are responsible for informing TeraGo of any regulatory issues that may affect the services provided by TeraGo; however, TeraGo may not be able to accommodate the regulatory issues.
- User entities are responsible for establishing a development and test environment to test and validate patches, upgrades, and modifications of customer maintained applications or content.
- User entities are responsible for understanding and complying with their contractual obligations to TeraGo.
- User entities are responsible for maintaining their own system of record.
- User entities are responsible for ensuring critical application processes, queues, and resources are monitored to aid application availability.
- User entities are responsible for responding to alert notifications as needed.
- User entities are responsible for ensuring changes to IT infrastructure are appropriate.
- User entities are responsible for notifying TeraGo, in a timely manner, when changes are made to technical, billing, or administrative contract information.
- User entities are responsible for developing their own disaster recovery and business continuity plans that address their inability to access or utilize TeraGo's services.
- User entities are responsible for determining whether TeraGo's security infrastructure is appropriate for its need, and for notifying TeraGo of any requested modifications, which TeraGo will negotiate with the user entity to determine whether requested modifications are possible and at what cost.
- User entities are responsible for the confidentiality and integrity of data maintained on their internal systems.
- User entities are responsible for notifying TeraGo of new, termination, or transfer of employees in a timely manner.
- User entities are responsible for providing and maintaining a list of employees authorized to request or remove access to the TeraGo data centre facilities.
- User entities are responsible for ensuring the confidentiality of any user accounts and passwords assigned to them to access the TeraGo data centre facilities.
- User organizations are responsible for controls to comply with the operating instructions of the Company's products and applications.
- User organizations are responsible for controls to ensure that user organizations adopt strong operating system and application password management procedures, including using passwords that cannot be easily compromised and require to change on a regular basis.
- User organizations are responsible for controls to dictate the use of encryption.
- User organizations are responsible for controls for maintaining the telecommunications infrastructure between itself and its users.

- User organizations are responsible for malicious code management on their servers and systems.

This section describes additional controls that should be in operation at user organizations to complement the controls at the Company for Hybrid Cloud Services. User auditors should consider whether or not the following controls have been placed in operation at the user organizations:

- Controls are in place for user organizations to ensure compliance with contractual requirements.
- Controls are in place to ensure that user organizations adopt strong operating system and application password management procedures, including using passwords that cannot be easily compromised and require to change on a regular basis.
- Controls are in place to provide reasonable assurance of the compatibility of software not provided by TeraGo.
- Controls to provide reasonable assurance that the customer has procedures in place for developing, maintaining, and testing their own business continuity plans (BCP).
- Controls to provide reasonable assurance that TeraGo is notified in advance of any equipment or other shipments they will be sending or receiving.
- Controls to provide reasonable assurance of the transmission and receipt of information not provided by TeraGo.
- Controls to provide reasonable assurance, in conjunction with advice from TeraGo personnel, for the customer to communicate their IP connectivity needs to permit TeraGo personnel to design managed firewall solutions. Customers are responsible for communicating changes in these needs in a timely manner to permit timely changes in firewall configurations.
- Controls to provide reasonable assurance that data is backed up or contracting with TeraGo to perform these services.
- Controls for approving the telecommunications infrastructure between itself and TeraGo.

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Processing of transactions for customers by TeraGo covers only a portion of the overall internal control structure of each customer. TeraGo's products and services were not designed to be the only control component in the internal control environment. Additional control procedures are required to be implemented at the customer level. It is not feasible for all of the control objectives relating to the processing of transactions to be completely achieved by TeraGo. Therefore, each customer's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

SECTION 4: INFORMATION PROVIDED BY AUDITWERX

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
Criteria Common to All Security Principles				
CC1.0	***Common Criteria Related to Organization and Management***			
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security and availability	TeraGo has an organizational structure is in place to establish and communicate key areas of authority, responsibility, and appropriate lines of reporting; the organizational structure is reviewed and updated periodically, but not less than annually.	Inspected the current TeraGo organizational chart to verify that reporting lines and levels of authority and responsibility appeared to be appropriate based on position titles and that the organizational chart was up-to-date and reviewed annually.	No exceptions noted.
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relates to security and availability.	The Company Security Manual (CSM) establishes the Company Security Officers and Alternate Company Security Officers (CSO/ACSO) and the responsibilities of the CSO and ACSO.	Inspected the Company Security Manual to verify that CSO and ACSO roles and responsibilities were established and assigned per the CSM.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
		The roles and responsibilities of key TeraGo managers are defined in written job descriptions, which include duties, such as the proper oversight, management, and monitoring of security activities; job descriptions are reviewed or updated periodically, but not less than annually.	Inspected the job descriptions of TeraGo's key managers to verify that the roles and responsibilities were defined sufficiently to include duties, such as proper oversight, management, and monitoring activities and that the job description were up-to-date and reviewed during the examination period.	No exceptions noted.
			Inspected job descriptions posted on the intranet to verify that the written job descriptions were available to TeraGo managers and their supervisors.	No exceptions noted.
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining and monitoring the system affecting the of security and availability and provides resources necessary for personnel to fulfill their responsibilities.	Job requirements are documented in the job descriptions and the candidates' ability to meet these requirements are evaluated as part of the hiring and transfer evaluation processes.	Inspected the qualification assessment for a sample of employees hired or transferred during the examination period to verify that the qualifications of prospective employees were evaluated during the hiring or transfer process.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
		Management establishes skills and continued training, and monitors completion of security awareness training programs at least annually.	Inspected security awareness training materials/agenda to verify training courses are available to personnel.	No exceptions noted.
			Inspected the attendance roster/test results for a sample of employees to verify that management monitored training at least annually.	No exceptions noted.
		During its ongoing and periodic business planning and budgeting process, management evaluates the need for additional tools and resources in order to achieve business objectives.	Inspected copy of the Cloud Hosting Services (CHS) Service Level Objectives quarterly meeting minutes and noted documented discussion of operational planning.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to security and availability.	TeraGo maintains established policies and procedures, which outline operating practices and business conduct for employees. Policies and procedures are reviewed periodically (but not less than annually), updated when needed and communicated to employees with employees acknowledgements received for the Employee Handbook, Code of Conduct and Information Security Policy upon hire. The policies and procedures include the following: • Code of Conduct • Employee Handbook • Information Security ○ Acceptable Use ○ Remote Access ○ Removable Media ○ Data Classification ○ Backup & Recovery ○ Change Control ○ Company Security Manual ○ Incident Response	Inspected the Company's most recent versions of the policies and procedures listed below, noting the documents were reviewed and included items such as: • Code of Conduct • Employee Handbook • Information Security ○ Acceptable Use ○ Remote Access ○ Removable Media ○ Data Classification ○ Backup & Recovery ○ Change Control ○ Company Security Manual ○ Incident Response	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC1.4 Cont.		Management ensures employees are subject to a criminal and financial trust background check during the hiring process.	Inspected the criminal background check results for a sample of employees hired during the examination period to verify that each employee was subject to a criminal background check as part of the hiring process.	**Exceptions noted:** Two of the 7 new hires sampled did not undergo background checks within the examination period.
CC2.0	***Common Criteria Related to Communications***			
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the result of system operation.	The TeraGo service description is available to system users via the TeraGo website.	Inspected the system description published on the TeraGo website to verify that the system description was communicated to system users via the TeraGo website.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC2.2	The entity's security commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal system users to enable them to carry out their responsibilities.	Commitments regarding the system are included in the TeraGo Service Level Agreement (SLA).	Inspected the SLA published on the TeraGo website to verify that commitments regarding the system were communicated to system users via the Service Level Agreement published on the TeraGo website.	No exceptions noted.

Ref #	Criteria	Description of TeraGo’s Controls	Tests of Controls Performed	Testing Results
CC2.2 Cont.		TeraGo maintains established policies and procedures, which outline operating practices and business conduct for employees. Policies and procedures are reviewed periodically (but not less than annually), updated when needed and communicated to employees with employees acknowledgements received for the Employee Handbook, Code of Conduct and Information Security Policy upon hire. The policies and procedures include the following: • Code of Conduct • Employee Handbook • Information Security ○ Acceptable Use ○ Remote Access ○ Removable Media ○ Data Classification ○ Backup & Recovery ○ Change Control ○ Company Security Manual ○ Incident Response	Inspected the Company’s most recent versions of the policies and procedures listed below, noting the documents were reviewed and included items such as: • Code of Conduct • Employee Handbook • Information Security ○ Acceptable Use ○ Remote Access ○ Removable Media ○ Data Classification ○ Backup & Recovery ○ Change Control ○ Company Security Manual ○ Incident Response	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	Policy and procedures documents for significant processes that address system requirements are available on the TeraGo internal network	Inspected the policies and procedures published on the TeraGo internal network to verify that policies and procedures were in place for significant processes and communicated to internal system users.	No exceptions noted.
		Customer responsibilities are available to authorized external users of the system via the TeraGo SLA.	Inspected the SLA published on the TeraGo website to verify that customer responsibilities regarding the system were communicated to system users via the SLA published on the TeraGo website.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls relevant to the security and availability of the system is provided to personnel to carry out their responsibilities.	TeraGo maintains established policies and procedures, which outline operating practices and business conduct for employees. Policies and procedures are reviewed periodically (but not less than annually), updated when needed and communicated to employees with employees acknowledgements received for the Employee Handbook, Code of Conduct and Information Security Policy upon hire. The policies and procedures include the following: • Code of Conduct • Employee Handbook • Information Security ○ Acceptable Use ○ Remote Access ○ Removable Media ○ Data Classification ○ Backup & Recovery ○ Change Control ○ Company Security Manual ○ Incident Response	Inspected the Company's most recent versions of the policies and procedures listed below, noting the documents were reviewed and included items such as: • Code of Conduct • Employee Handbook • Information Security ○ Acceptable Use ○ Remote Access ○ Removable Media ○ Data Classification ○ Backup & Recovery ○ Change Control ○ Company Security Manual ○ Incident Response ○	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC2.5	Internal and external system users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel.	Policy and procedures documents for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints and the process for handling complaints, are published and made available on the TeraGo internal network drive.	Inspected the Incident Response Plan published on the TeraGo internal network to verify that policies and procedures related to incident response were in place and communicated to internal system users.	No exceptions noted.
		Customer responsibilities, which include the responsibility for reporting operational failures, incidents, problems, concerns and complaints, and the process for doing so, are described in system documentation.	Inspected the SLA published on the TeraGo website to verify that customer responsibilities regarding the system were communicated to system users via the SLA published on the TeraGo website.	No exceptions noted.
CC2.6	System changes that affect internal and external system user responsibilities or the entity's commitments and requirements relevant to security and availability are communicated to those users in a timely manner.	Changes made to systems are communicated and confirmed with customers through ongoing communications mechanisms by customer support personnel via email.	Inspected the communication mechanism utilized to facilitate system change notifications to external system users.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC2.6 Cont.		The system change calendar that describes changes to be implemented and is published on the TeraGo internal network drive.	Inspected the system change calendar to verify that the system change calendar was published on the internal network drive and was available to internal system users.	No exceptions noted.
		Major changes to roles and responsibilities and changes to key personnel are communicated to affected internal and external system users via email by the client support team.	Inspected email communication for a sample of new hires and terminations to verify that internal system users were notified of any changes in roles and responsibilities by the client support team.	No exceptions noted.
			Inspected the communications sent to external system users for major changes in roles to key personnel to verify that external system users were notified major changes in the roles and responsibilities of key personnel.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC3.0	***Common Criteria Related to Risk Management and the Design and Implementation of Controls***			
CC3.1	The entity (1) identifies potential threats that would impair system security commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system); (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies); (4) identifies and assesses changes (for examples, environmental, regulatory and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control; and (5) reassesses and revises as necessary, risk assessments and mitigation strategies based on the identified changes.	A master list of the entity's system components, which accounts for IT asset additions and removals, is maintained for management's use.	Inspected the IT asset records to verify that the IT asset records were current.	No exceptions noted.
		Management performs an annual enterprise-wide risk assessment (ERA), which is reviewed and approved by the Board of Directors to identify: • changes to business objectives • commitments and requirements • internal operations • external factors that threaten the achievement of business objectives • update the potential threats to system objectives • identified risks are rated using a risk evaluation process • ratings are reviewed by management • evaluates the effectiveness of controls and mitigation strategies • mitigation plans	Inspected TeraGo's annual risk assessment and verified that the identified attributes were addressed.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC3.2	The entity designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy, reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities and updates the controls as necessary.	Disaster Recovery Plan (DRP) is documented and tested annually.	Inspected the DRP and the results of DRP testing to verify that the DRP was documented and was tested annually.	No exceptions noted.
		Internal vulnerability scans are performed annually and the frequency is adjusted as required to meet ongoing and changing commitments and requirements.	Inspected the vulnerability scan results to verify that an internal vulnerability scan was performed annually.	No exceptions noted.
		If applicable, remediation plans are established based upon the severity level of any deficiencies identified during vulnerability scans.	Inspected the remediation plan established based upon severity level of deficiencies identified during vulnerability scan to verify deficiencies are followed up and resolved.	No exceptions noted.
CC4.0	***Common Criteria Related to Monitoring of Controls***			
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	IT operations monitor system performance, security threats, changing resource utilization needs, and unusual system activity to identify, log and report potential security breaches and incidents.	Inspected the monitoring system in place and inquired of IT management to validate systems were monitored for the period.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
		Incidents are logged and alerts are generated to notify IT staff when conditions exceed defined threshold settings	Inspected the monitoring system alert log to verify it was configured to generate alerts to IT when conditions exceed threshold settings.	No exceptions noted.
		Identified incidents are tracked in a ticketing system and reported to appropriate personnel for resolution.	Inspected tickets for a sample of incidents to verify that monitoring alerts were evaluated and countermeasures were implemented.	No exceptions noted.
CC5.0	***Common Criteria Related to Logical and Physical Access Controls***			
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability.	Established entity standards exist for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration standards, and standardized access control lists.	Inspected hardening standards to verify that a standard exists for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration standards, and standardized access control lists.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC5.1 Cont.			Inspected a listing of server deployed during the examination period and verified in active directory that the servers were joined to the domain.	No exceptions noted.
		Application controls match each user ID to an Active Directory group and restrict output to approved user IDs.	Inspected the domain Active Directory group's configuration to verify that each user ID was matched to a single account and output was restricted to an approved user ID.	No exceptions noted.
		Infrastructure components and software are configured to use the shared sign-on functionality when available; systems not using the single sign-on functionality are required to be implemented with separate user ID and password submission.	Inspected configuration to verify single sign-on functionality was implemented where available.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC5.1 Cont.		VPN connections are utilized over public networks for encrypting sensitive information and management limits the remote access to authorized individuals (i.e., employees, vendors, or customers).	Inspected the VPN settings to verify that VPN rules control remote access and encryption is enabled.	No exceptions noted.
			Inspected the list of personnel with VPN access and inquired with management to verify that the access was authorized.	No exceptions noted.
			Inspected the system-generated list of VPN administrators and inquired of management to verify their access was authorized.	No exceptions noted.
		Administrator access to the network is restricted to authorized personnel.	Inspected the list of domain administrators and inquired with management to verify whether administrator access to systems was authorized.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC5.2	New internal and external system users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials, and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security and availability. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	New or modified access to the network, systems and software is timely granted or changed after the completion of an access request form that is authorized by appropriate individuals.	Inspected the completed access request form and user access rights for a sample of new system users to verify that the request was authorized by a supervisor or manager and granted appropriately.	No exceptions noted.
			There were no access modifications for existing users changing job roles; therefore, no testing performed.	No testing performed.
		A human resources representative notifies security administrators of resignations or terminations of employees or consultants resulting in the person's logon ID being disabled and/or the password reset.	Inspected the current access rights for a sample of terminated employees to verify their network and application security access was updated and access was removed.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC5.3	Internal and external system users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security and availability.	The Company has established standards for infrastructure and software hardening and software configuration, which includes the requirements for implementation of access control software, entity configuration standards, and standardized access control lists.	Inspected hardening standards to verify that a standard exists for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration standards, and standardized access control lists.	No exceptions noted.
			Inspected a listing of server deployed during the examination period and verified in active directory that the servers were joined to the domain.	No exceptions noted.
		Infrastructure components and software are configured to use the single sign-on functionality when available; systems not using the single sign-on functionality are required to be implemented with separate user ID and password submission.	Inspected domain user group configurations to verify single sign-on functionality was implemented where available.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC5.3 Cont.		Password complexity standards are established to enforce control over the network passwords.	Inspected the system security-layer password parameter settings for the network to verify that passwords complied with the TeraGo Password Management Policy.	No exceptions noted.
		Administrative accounts are set up, and the user administration function is segregated for managing privileged accounts.	Inspected the list of domain administrators and inquired with management to verify whether administrator access to systems was authorized.	No exceptions noted.
CC5.4	Access to data, software, functions, and other IT resources is authorized and modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security and availability.	New or modified access to the network, systems and software is timely granted or changed after the completion of an access request form that is authorized by appropriate individuals.	Inspected the completed access request form and user access rights for a sample of new system users to verify that the request was authorized by a supervisor or manager and granted appropriately.	No exceptions noted.
			There were no access modifications for existing users changing job roles; therefore, no testing performed.	No testing performed.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
		Roles are reviewed and updated by management and the risk and controls group on an annual basis. Access change requests resulting from the review are submitted to the security group via a change request record.	Inspected the service ticket for management's annual user control review, noting that appropriate individuals were monitoring and, if necessary, changing user access on a routine basis.	No exceptions noted.
CC5.5	Physical access to facilities housing the system (for example, data centres, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security and availability.	An ID card-based physical access control system has been implemented within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities.	Observed during testing that the KantechID card access control system has been implemented at the perimeter of facilities, as well as at the entry and exit points of sensitive areas.	No exceptions noted.
		In addition to ID-Card, finger print identification is required at both the entrance to the facility and at the entrance to the data centre.	Observed while onsite that finger prints identification was required to gain access to data centre facilities.	No exceptions noted.
		Employees are required to wear ID badges at all times in the facility.	Observed employees to determine that employees were required to wear ID badges at all times in the facility.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC5.5 Cont.		Motion detectors as well as door and window contacts are in place as security measure against unauthorized physical access to the data centres.	Observed during testing that motion detectors and door and window contacts are in place to prevent unauthorized access to the data centres.	No exceptions noted.
		Mantraps are utilized at the TeraGo facility to control physical access to sensitive areas.	Observed physical access to sensitive areas of the TeraGo facility to verify that mantraps were in place for control of access to sensitive facilities.	No exceptions noted.
		Visitors are required to sign a visitor log at the main entrance upon arrival and departure and are accompanied by an employee during their visit.	Inspected the visitor log to verify that visitors were required to sign in and accompanied by an employee.	No exceptions noted.
		The sharing of access badges and tailgating are prohibited by policy.	Inspected the Information Security Policy to verify that the sharing of access badges and tailgating is prohibited.	No exceptions noted.
CC5.6	Logical access security measures have been implemented to protect against security and availability threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.	A firewall is in place to control network traffic and prevent unauthorized traffic from passing between the internal and external networks.	Inspected the firewall configuration to verify that a firewall was in place to control network traffic and prevent unauthorized traffic from passing between the internal and external networks.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
			Inspected the system-generated list of firewall administrators and inquired of management to verify their access was authorized.	No exceptions noted.
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes, and is protected during transmission, movement, or removal enabling the entity to meet its commitments and requirements as they relate to security and availability.	VPN connections are utilized over public networks for encrypting sensitive information and management limits the remote access to authorized individuals (i.e., employees, vendors, or customers).	Inspected the VPN settings to verify that VPN rules control remote access and encryption is enabled.	No exceptions noted.
			Inspected the list of personnel with VPN access and inquired with management to verify that the access was authorized.	No exceptions noted.
			Inspected the system-generated list of VPN administrators and inquired of management to verify their access was authorized.	No exceptions noted.
		TeraGo has a client use secure web application to enter orders securely and review status and reports.	Inspected the web application software in use to verify whether security protocol (Hypertext Transport Protocol Secure) was enabled.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC5.7 Cont.			Observed the secure web application to verify that a username and password was required for access.	No exceptions noted.
			Inspected the secure sockets layer (SSL) configuration of the web server to verify that secure communication tunnels were in place for file transfers requiring encryption to the TeraGo's web servers using SSL encryption.	No exceptions noted.
		TeraGo provides secure file transfer capabilities to secure connections for the file transfer process.	Inspected the SFTP configuration to verify that a SFTP server was utilized for encrypted file transfers of confidential client data files.	No exceptions noted.
		Backup media is encrypted during creation.	Inspected the backup configuration or database configuration to verify the backups are encrypted.	No exceptions noted.
			Inspected the historical backup log to verify the backups were encrypted.	No exceptions noted.

Ref #	Criteria	Description of TeraGo’s Controls	Tests of Controls Performed	Testing Results
		Laptops are encrypted when assigned to owners.	Inspected laptop encryption configuration for a sample of laptops deployed.	No exceptions noted.
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s commitments and system requirements as they relate to security and availability.	Anti-virus software is installed and configured on all production servers and workstations to automatically scan and update virus definitions on a daily basis.	Inspected the anti-virus software configuration on production systems and workstations to verify that anti-virus software was configured to automatically scan and update virus definitions on a daily basis.	No exceptions noted.
			Inspected the system-generated list of anti-virus administrators and inquired of management to verify their access was authorized.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC6.0	***Common Criteria Related to System Operations***			
CC6.1	Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored and evaluated and countermeasures are designed, implemented and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity, confidentiality and privacy.	IT operations monitors critical/relevant systems for errors. Errors are logged and alerts are generated to notify IT staff when conditions exceed defined threshold settings.	Inspected the monitoring system in place and inquired of IT management to validate systems were monitored for the period.	No exceptions noted.
			Inspected the monitoring system alert log to verify it was configured to generate alerts to IT when conditions exceed threshold settings.	No exceptions noted.
		Internal vulnerability scans are performed annually and the frequency is adjusted as required to meet ongoing and changing commitments and requirements.	Inspected the vulnerability scan results to verify that an internal vulnerability scan was performed annually.	No exceptions noted.
		Incidents are logged and alerts are generated to notify IT staff when conditions exceed defined threshold settings.	Inspected the monitoring system alert log to verify it was configured to generate alerts to IT when conditions exceed threshold settings.	No exceptions noted.
		If applicable, remediation plans are established based upon the severity level of any deficiencies identified during vulnerability scans.	Inspected the remediation plan established based upon severity level of deficiencies identified.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
		A backup process is in place to perform daily system configuration backups. Backup jobs are monitored and notification alerts are sent to designated IT staff.	Inspected the configuration of the backup software used to verify that backups of system configurations were scheduled to run to provide daily backups and has logging and alerts features enabled.	No exceptions noted.
CC6.2	Security and availability incidents, including logical and physical security breaches, failures and identified vulnerabilities are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.	TeraGo has an Incident Response Plan in place with defined protocols for resolving and escalating reported events.	Inspected the incident management policies to verify that policies were in place that identify protocols for resolving and escalating reported events.	No exceptions noted.
		Identified incidents are tracked in a ticketing system and reported to appropriate personnel for resolution.	Inspected tickets for a sample of incidents to verify that monitoring alerts were evaluated and countermeasures were implemented.	No exceptions noted.

Ref #	Criteria	Description of TeraGo’s Controls	Tests of Controls Performed	Testing Results
CC7.0	***Common Criteria Related to Change Management***			
CC7.1	The entity’s commitments and system requirements as they relate to security are addressed, during the system development lifecycle including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	The Change Control Policy addresses system requirements and the potential effect of changes on security commitments throughout the change management process.	Inspected the Change Control Policy to verify that it addressed security commitments and system requirements.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security.	Management performs an annual enterprise-wide risk assessment (ERA), which is reviewed and approved by the Board of Directors to identify: • changes to business objectives • commitments and requirements • internal operations • external factors that threaten the achievement of business objectives • update the potential threats to system objectives • identified risks are rated using a risk evaluation process • ratings are reviewed by management • evaluates the effectiveness of controls and mitigation strategies • mitigation plans	Inspected TeraGo's annual risk assessment and verified that the identified attributes were addressed.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC7.2 Cont.		TeraGo maintains established policies and procedures, which outline operating practices and business conduct for employees. Policies and procedures are reviewed periodically (but not less than annually), updated when needed and communicated to employees with employees acknowledgements received for the Employee Handbook, Code of Conduct and Information Security Policy upon hire. The policies and procedures include the following: • Code of Conduct • Employee Handbook • Information Security ○ Acceptable Use ○ Remote Access ○ Removable Media ○ Data Classification ○ Backup & Recovery ○ Change Control ○ Company Security Manual ○ Incident Response	Inspected the Company's most recent versions of the policies and procedures listed below, noting the documents were reviewed and included items such as: • Code of Conduct • Employee Handbook • Information Security ○ Acceptable Use ○ Remote Access ○ Removable Media ○ Data Classification ○ Backup & Recovery ○ Change Control ○ Company Security Manual ○ Incident Response	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security and availability.	For major incidents, a root cause analysis is prepared and reviewed by operations management; based on the root-cause analysis, change requests are prepared and the entity's risk management process and relevant risk management data is updated to reflect the planned incident and problem resolution.	Inspected the root cause analysis for a sample of high severity incidents to verify they were prepared and reviewed by operations management.	No exceptions noted.
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented in accordance to meet the entity's security and availability commitments and system requirements.	Management authorizes and approves the implementation of new and changes to existing systems according to approved policies.	Inspected the documentation of the implementation for a sample of new and changes to existing systems to verify they are authorized by management for development.	No exceptions noted.
			Inspected the documentation of the implementation for a sample of new and changes to existing systems to verify they are approved by management for migration to production.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC7.4 Cont.		Functional and detailed designs are prepared for other than minor changes. Functional designs are reviewed and approved by the application or infrastructure and software owner and detailed designs are approved by the director of development for the application and the change advisory board prior to work commencing on the requested change or development project.	Inspected the documentation of the implementation for a sample of major new and changes to existing systems to verify that they include functional and detailed designs and were approved.	No exceptions noted.
		The Company tests changes to systems, applications, and databases in a segregated environment prior to system implementation.	Inspected the documentation of the implementation for a sample of changes to verify they were tested prior to system implementation.	No exceptions noted.
		Code review or walkthrough is required for high impact changes that meet established criteria (that mandate code reviews and walkthroughs) and these are performed by a peer programmer that does not have responsibility for the change.	Inspected the documentation of the implementation for a sample of changes to verify code review was performed by a peer programmer that does not have responsibility for the change.	No exception noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC7.4 Cont.		System changes, other than those pre-approved require the approval of management prior to implementation.	Inspected a sample of change management tickets to verify that changes other than pre-approved system changes were approved by management.	No exceptions noted.
		Changes are reviewed and approved by the change advisory board (CAB) prior to implementation.	Inspected the documentation of the implementation for a sample of changes to verify approval by the change advisory board prior to implementation.	No exceptions noted.
		Separate environments are used for development, testing, and production. Developers do not have the ability to make changes to software in testing or production.	Inspected the system documentation to verify that there are segregated environments for testing, development, and production.	No exceptions noted.
			Inspected user access rights to verify that non-IT personnel with access to move changes to production did not have access to development.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
CC7.4 Cont.		A turnover process that includes verification of operation and back out steps is used for system changes.	Inspected the documentation of the implementation for a sample of changes to verify that a turnover process and back out steps were used, if necessary.	No exceptions noted.
		Post implementation procedures that are designed to verify the operation of system changes are performed for one week after the implementation for other than minor changes, and results are shared with users and customers as required to meet commitments and requirements.	Inspected the documentation of the implementation for samples of changes to verify that post implementation procedures were performed.	No exceptions noted.
		The change management process has defined the following roles and assignments: • Authorization of change requests—owner or business unit manager • Development—application design and support department • Testing—quality assurance department • Implementation—software change management group	Inspected the documentation of the implementation for a sample of changes to verify that SDLC gates were met by separate individuals.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
A1.0	***Additional Criteria for Availability***			
A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet availability commitments and requirements.	IT operations monitor system performance, security threats, changing resource utilization needs, and unusual system activity to identify, log and report potential security breaches and incidents.	Inspected the monitoring system in place and inquired of IT management to validate systems were monitored for the period.	No exceptions noted.
		Incidents are logged and alerts are generated to notify IT staff when conditions exceed defined threshold settings	Inspected the monitoring system alert log to verify it was configured to generate alerts to IT when conditions exceed threshold settings.	No exceptions noted.
		Redundancy has been implemented for critical infrastructure components.	Inspected the configuration of critical infrastructure components to verify that redundancy had been implemented.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
A1.1 Cont.		Processing capacity is monitored on an ongoing basis.	Inspected the Nimsoft monitoring software configuration used by TeraGo to monitor the infrastructure processing capacity and usage reports to verify that TeraGo maintained, monitored, and evaluated capacity demand in order to meet availability commitments.	No exceptions noted.
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.	Environmental protections have been installed including the following: • Cooling systems • Battery and natural gas generator backup in the event of power failure • Redundant communications lines • Water leak detectors • Smoke detectors	Observed environmental protections to verify they were installed.	No exceptions noted.
		A backup process is in place to perform daily system configuration backups. Backup jobs are monitored and notification alerts are sent to designated IT staff.	Inspected the configuration of the backup software used to verify that backups of system configurations were scheduled to run to provide daily backups and has logging and alerts features enabled.	No exceptions noted.

Ref #	Criteria	Description of TeraGo's Controls	Tests of Controls Performed	Testing Results
A1.3	Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.	The TeraGo DRP is documented and tested annually.	Inspected the DRP and the results of DRP testing to verify that the DRP was documented and was tested annually.	No exceptions noted.

SECTION 5: OTHER INFORMATION PROVIDED BY TERAGO NETWORKS, INC.

Management's Response to Exception at CC1.4:

A change in HR personnel created a delay in criminal record checks as the account ownership had to be transitioned to the new head of HR. This was not noticed until the checklist item came up at the next new hire, and account ownership change started to take place at that time, this plus the delay in processing did not allow the criminal records checks for the exceptions to be completed within the audit period.