Statement on Standards for Attestation Engagements (SSAE) 16
Service Organization Control (SOC) 1 Type II Report

Report of Independent Auditors on Controls Placed in Operations and Tests of Operating Effectiveness

For the period from March 1, 2013 to February 28, 2014

THIS REPORT IS CONFIDENTIAL INFORMATION

TierPoint's existing clients and their independent service auditors are authorized to view this report.

Any person other than a TierPoint client who wishes to view this report must first sign a TierPoint approved non-disclosure and access agreement.

If you receive this report in error, please notify the sender and destroy this document without copying or disclosing it.

Table of Contents

HOLTZMAN PARTNERS

AUDIT · TAX · ADVISORY

Section I – Report of Independent Service Auditor

To the Executive Management Team,
TierPoint, LLC

We have examined TierPoint, LLC's (TierPoint or the Company) description of certain General Information Technology procedures pertaining to its Dallas Texas Datacenter for the period from March 1, 2013 to February 28, 2014 (the description) and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. The description (which is contained in Section III) indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of TierPoint's controls are suitably designed and operating effectively. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

In Section II of this report, TierPoint has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve specified control objectives. TierPoint is responsible for preparing this description and for its completeness, accuracy and method of presentation and providing the services covered by the description. TierPoint is also responsible for specifying control objectives (including identifying the risks that threaten the achievement of the control objectives) and designing, implementing, and documenting controls to achieve these control objectives.

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives specified by management based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives during the period from March 1, 2013 to February 28, 2014.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

HOLTZMAN PARTNERS

AUDIT · TAX · ADVISORY

In our opinion, in all material respects, based on the criteria described in TierPoint's Assertion in Section II of this report: a) the description fairly presents certain General Information Technology procedures of the Company pertaining to its Dallas Texas Datacenter for the period from March 1, 2013 to February 28, 2014; b) the controls described by TierPoint were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the controls operated effectively during the period from March 1, 2013 to February 28, 2014 and user entities applied the complementary user entity controls contemplated in the design of TierPoint's controls for the period from March 1, 2013 to February 28, 2014; and c) the controls tested, which together with the complementary user-entity controls referred to in this report (if operating effectively) were those necessary to provide reasonable assurance that the control objectives were met and operated effectively during the period from March 1, 2013 to February 28, 2014.

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the specified control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

This report is intended solely for the information and use of TierPoint, user entities of TierPoint's Dallas Texas Datacenter for some or all of the period from March 1, 2013 to February 28, 2014, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Holtzman Partners, LLP

April 7, 2014

Section II – TierPoint's Assertion

We have prepared the description of certain General Information Technology procedures of TierPoint pertaining to our Dallas Texas Datacenter for the period from March 1, 2013 to February 28, 2014 (the description) for user entities and their auditors who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when obtaining an understanding of user entities' information and communication systems relevant to financial reporting. We confirm to the best of our knowledge and belief that:

a) the description fairly presents certain General Information Technology procedures pertaining to our Dallas Texas Datacenter made available to user entities for the period from March 1, 2013 to February 28, 2014 for processing their transactions. The criteria used in making this assertion included evaluating whether the description:
    i. presents how the procedures made available to user entities were designed and implemented to process relevant transactions, including (1) the classes of transactions processed; (2) the manual and automated procedures by which those transactions are initiated, authorized, recorded, processed, corrected (as necessary) and transferred to the reports presented to user entities; (3) the related accounting records, supporting information and specific accounts used to initiate, authorize, record, process, and report transactions (including the correction of incorrect information and how information is transferred to the reports provided to user entities of the system); (4) how the certain General Information Technology procedures pertaining to our Dallas Texas Datacenter capture and address significant events and conditions (other than transactions); (5) the process used to prepare reports or other information provided to user entities; (6) specified control objectives and controls designed to achieve those objectives; and (7) other aspects of our control environment, risk management process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities.
    ii. does not omit or distort information relevant to the scope of certain General Information Technology procedures pertaining to our Dallas Texas Datacenter, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities and the independent auditors of those user entities, and may not, therefore, include every aspect of the General Information Technology procedures pertaining to our Dallas Texas Datacenter that each individual user entity and its auditor may consider important in its own particular environment.
b) the description includes relevant details of changes to certain General Information Technology procedures pertaining to our Dallas Texas Datacenter for the period from March 1, 2013 to February 28, 2014.
c) the controls listed in Section IV of this report were suitably designed and operated effectively during the period from March 1, 2013 to February 28, 2014 to achieve the specified control objectives based on the following criteria:
    i. the risks that threaten the achievement of the control objectives have been identified.
    ii. the controls would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives from being achieved.
    iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

We welcome any questions or comments from our clients regarding the assertions described above.

Carl Milloshewski
Compliance Manager
April 7, 2014

Section III –TierPoint's Description of the System

Overview of Operations

Cequel Data Centers, LLC was established in 2010 and is a portfolio company of Thompson Street Capital Partners, Charterhouse Group, and Cequel III which owns and operates a number of Datacenters throughout the US under the TierPoint brand name. TierPoint facilities are located in Baltimore, MD, Dallas, TX, Oklahoma City, OK, Seattle, WA, Spokane, WA and Tulsa, OK. The scope of this report only includes the Dallas, TX facility and does not extend to the other facilities or the services offered by those facilities.

The Dallas, TX facility offers 68,000 square feet of environmentally controlled and secure Datacenter space that is professionally staffed around the clock, 365 days a year. Through a premium, multi-homed network and high density power, TierPoint offers reliable service and availability of customer data, applications and equipment. The Company serves customers in the Dallas/Fort Worth area, across the country and around the globe.

Overview of Internal Controls

Control Environment

A company's control environment reflects the overall attitude, awareness and actions of management, employees, and others concerning the importance of controls and the emphasis given to controls in its policies, procedures, methods and organizational structure. The control environment of the Company originates with the Executive Management Team (EMT).

The EMT consists of the CEO, CFO and General Manager. This team is responsible for establishing the overall vision of the Company and meets quarterly to discuss operational and service issues.

The competence of Company employees is the basis for a strong control environment. As such, formal policies and procedures have been developed and outlined in the Company's Employee Handbook covering critical aspects of employment. The Company's Employee Handbook includes a section on "Employee Conduct" which serves as a guide to ethical behavior for all employees. The Employee Handbook covers areas of business conduct, conflicts of interest and ethics when working with clients, vendors, the public and other employees. During the new hire orientation, employees are required to acknowledge that they have read and understand the components of the Employee Handbook.

Management has implemented a division of roles and responsibilities which provides a basis for segregation of duties within the Company. This segregation of duties is further enforced through the physical and logical access controls at the Datacenter.

The Company's EMT believes employees and clients are best served by a management team that is highly involved in the operations of the Company while giving employees the authority they need to properly serve clients. Management at all levels is encouraged to address developing issues and risks proactively in order to minimize their impact on the Company and its clients.

Risk Management

A Company's risk assessment process is its identification, analysis and management of risks relevant to user organizations. The Company recognizes risk management is a critical component of its operations and is at the core of its Dallas Texas Datacenter.

Daily activities at the Datacenter are focused on mitigating risk from internal and external factors. Much of the risk mitigation is incorporated into their design with additional risk mitigation being considered in the daily operation and established procedures at the facilities. The EMT meets quarterly at which time critical projects, client implementations and the impact of new service offerings on the integrity of the Datacenter facilities are discussed. If any problem areas are identified, the resolution process is developed and necessary changes are implemented.

Clients are required to enter into a Master Services Agreement with the Company prior to the initiation of services which contains limits of liability, indemnification and other legal protections for the Company. The Company will also enter into contracts with its vendors which specify the vendor's obligations and liability for non-performance. For critical services, the Company maintains relationships with multiple vendors to limit exposure for failure to perform. Management monitors compliance against the terms of these contracts in their normal operations.

Measures to address these and other risks have resulted in the development of standardized policies and procedures.

Information and Communication

Information and communication systems support the identification, capture and exchange of information in a form and timeframe that enable people to carry out their responsibilities. The information system consists of the procedures, whether automated or manual, and records established to initiate, record, process and report a company's transactions (as well as events and conditions) and to maintain accountability for the related assets, liabilities and equity. The quality of system-generated information affects management's ability to make appropriate decisions in controlling company activities.

In addition to an Employee Handbook, TierPoint maintains several security-related policies which provide guidance and best practice information on securing data, assets, and other sensitive information. As necessary, management reviews and issues a revised Employee Handbook and security-related policies and these are distributed to all employees. During the new hire orientation, employees are required to acknowledge that they have read and understand the Employee Handbook.

Control Activities

Control activities are policies and procedures that help ensure management directives are carried out and necessary actions are taken to address risks in order to achieve the Company's objectives. Control activities, whether automated or manual, have various objectives and are applied at various organizational and functional levels.

TierPoint's EMT is responsible for directing and controlling operations and establishing, communicating, and monitoring control policies and procedures. TierPoint maintains sound internal controls and holds high expectations for the integrity and ethical values of its personnel. Organizational values and behavioral standards are communicated to all personnel via Company-wide emails, the Employee Handbook and in periodic meetings.

Specific control activities are provided in the General Information Technology Process section below and in *Section IV – Information Provided by the Independent Service Auditor.*

Monitoring

Monitoring is a critical aspect of internal control in the evaluation of whether controls are operating as intended and whether they are modified as appropriate for changes in conditions. The Company's management monitors the quality of internal control performance as a normal part of their activities. Employees use electronic problem tracking systems to monitor both internal and client related issues.

Exceptions to normal or scheduled availability due to hardware, software or procedural problems are logged, reported and resolved daily. In addition, the Company generates monthly capacity reports that summarize important operational information around Power Distribution Units, Uninterruptible Power Supplies, Fuel, the Service Entrance, etc. Management reviews these reports and action is taken as necessary.

Certain General Information Technology Procedures

***Note**: Parenthetical references have been included in the following narrative as a cross-reference to the applicable control activities included in Section IV of this report.*

Organization and Administration

***Control Objective #1 –** Controls provide reasonable assurance that the organization follows a structured hiring process, promotes appropriate employee behavior and segregates responsibilities within the organization.*

Although TierPoint has a relatively flat organizational structure, separate organizational segments have been established to create efficiencies to ensure that clients receive top level service and to provide for adequate segregation of duties. These assertions are strengthened by the creation of a division of roles and responsibilities for its personnel. Organizational charts are in place to communicate key areas of responsibility and appropriate lines of reporting. **(1.1)** The Company's primary departments include the following:

- Network Operations Center (NOC) – responsible for supporting the technical needs of clients and logical security of the Datacenter
- Facilities – responsible for maintaining the physical operation and environmental controls of the Datacenter.
- Sales – responsible for the sales process and ensuring new clients sign a Master Services Agreement.

Management has established an Employee Handbook which includes sections on Employment Policies, Employee Conduct, Compensation Policies, Operations Policies and Employee Benefits. **(1.2)** Prior to hiring, background checks are obtained for potential employees which are performed by an external third-party. **(1.3)** Upon hiring, employees are issued the Employee Handbook and are required to sign a Handbook Acknowledgement form verifying that they have received, read and agreed to abide by the terms of this Handbook. **(1.4)** These forms are retained in the employees' personnel files.

Physical Security and Environmental Safeguards

***Control Objective #2 –** Controls provide reasonable assurance that physical access to the Datacenter facility is restricted to authorized personnel and sufficient measures are in place and maintained for protection of these items from environmental hazards.*

The Company maintains policies and procedures for Physical Security in and around the Datacenter. **(2.1)** A Shipping and Receiving policy is also maintained to provide guidance for the secure temporary storage of customer packages and equipment. **(2.2)** As necessary, management reviews and issues revised policies and they are distributed to all employees at that time. NOC personnel walk through the facility every four hours to confirm that cabinets and cages are locked. **(2.3)** Automated Helpdesk Tickets are emailed to NOC personnel to remind them of the walkthrough and these Tickets are closed once the walkthrough has been completed. **(2.4)**

The Datacenter facility maintains continuous on site security. Over 140 security cameras cover the exterior, interior, and Datacenter floor. Recorded video is retained for at least 90 days. **(2.5)** Access to the facility is restricted to authorized personnel (i.e. Company employees, clients, etc.) through the use of a proximity card access system. **(2.6)** Authorized personnel are provided with proximity cards which are assigned access according to their requirements. **(2.7)** Datacenter access for new TierPoint employees is authorized by TierPoint management. **(2.8)** Client access to the Datacenter is restricted to authorized individuals on client access lists. **(2.9)** Changes (additions or removals) to these lists may only be requested by the primary client contact (or client designee) and client requests and approvals are documented in a Helpdesk Ticket. **(2.10)** Other third party access (i.e. contractors, etc.) is authorized by TierPoint management. **(2.11)** Individuals without authorized access must sign in at the front desk and be escorted by an individual with authorized access. **(2.12)** Access for terminated TierPoint employees is revoked upon their termination. **(2.13)**

TierPoint utilizes a variety of environmental controls at the Datacenter. Multiple redundant Computer Room Air Conditioners (CRAC's) are in place to maintain a constant temperature and humidity level. **(2.14)** The Datacenter is equipped with multiple High Sensitivity Smoke Detection (HSSD) sensors which continuously monitor the air throughout the facility. **(2.15)** Chemical fire extinguishers are located prominently throughout the facility. **(2.16)** The fire suppression system in the facility is a Dual Interlock, Dry Pipe, Pre-Action sprinkler system. **(2.17)** Temperature, humidity, fire, and smoke detection and action systems are maintained on an annual basis to help ensure that they are operating properly. **(2.18)**

The power systems at the Datacenters have been designed to run uninterrupted in the event of a power outage. Conditioned UPS (Uninterruptible Power Supply) units are utilized to supply power for short term power issues and these units are monitored real-time to help ensure that they are healthy and can be used in the event of an issue. **(2.19)** In the event of an extended power outage, on-site diesel generators are in place to generate power for the facility until power is restored. **(2.20)**

Logical Security

Control Objective #3 – *Controls provide reasonable assurance that logical access to the network systems and devices is restricted to authorized individuals.*

The Company's clients retain full administrative rights over their environment at the Datacenter through remote access to their servers. This access allows them to make changes to their servers as needed, including uploading content, configuring software and security settings, adding or removing local users and changing passwords. Clients may also elect to utilize dedicated firewalls to restrict this administrative access and limit the possibility of disruptions from unauthorized users.

The following are the logical access procedures utilized by the Company for its environment:

User Access Management

The Company utilizes Active Directory as a central point of verification for access to its network and user ID and password requirements have been established for TierPoint servers and network devices. **(3.1)** Password parameters for servers and network devices are in compliance with documented standards including minimum length, complexity, and age requirements. **(3.2)** Passwords to shared accounts for the network, servers and devices are stored in an in-house developed password management tool. **(3.3)** Access to the password tool is restricted to current NOC personnel, the General Manager and the Director of Facilities. **(3.4)** Passwords stored in the tool are encrypted to enhance the security of the data. **(3.5)**

Administrative access to the Company's network and servers is restricted to current NOC personnel, the General Manager and the Director of Facilities. **(3.6)** NOC personnel are responsible for security administration, including adding, changing and removing users to/from Company systems. An encrypted Virtual Private Network (VPN) is utilized to grant remote access. **(3.7)** Access to the VPN is restricted to TierPoint employees. **(3.8)** Access to the network, servers and devices is removed upon termination of a TierPoint employee. **(3.9)**

Network Management

NOC personnel are responsible for monitoring and maintaining the Company's internal network. Various network security policies and procedures are documented to include Encryption, Acceptable Use, Anti-virus, Password, Remote Access, and Server Security. **(3.10)** Network diagrams are documented to detail the connections between communications equipment. **(3.11)** Virus protection software is installed on NOC workstations and is scheduled to scan on a weekly basis. **(3.12)**

Service Management

Control Objective #4 – *Controls provide reasonable assurance that service incidents are tracked, recorded, and resolved.*

Network Trouble Escalation procedures are documented to ensure rapid resolution of issues to the network, server or device impacted. **(4.1)** Servers, devices and the network are monitored for DDoS attacks and abnormal network traffic. **(4.2)**. Events that are captured in the network monitoring system result in Tickets (within the Helpdesk System) being either automatically or manually generated. **(4.3)** The NOC escalates and triages events to ensure that proper personnel are alerted and that issues are resolved quickly. Once an event has been addressed and resolved, the Ticket is updated and closed. **(4.4)**

Complementary User Entity Control Considerations

The processing of transactions performed by the Company for user entities (clients) and the controls of the Company cover only a portion of the overall internal control environment. It is not feasible for control objectives relating to the processing of transactions to be solely achieved by the Company. Therefore, each user entity's internal control environment must be evaluated in conjunction with the Company's controls and testing summarized in *Section IV - Information Provided by the Independent Service Auditor* of this report.

This section highlights those internal control responsibilities that the Company believes should be present at each user entity and has considered in developing the Company's controls described in this report. In order for user entities to rely on the controls relating to objectives reported on herein, each user entity must evaluate its own internal control environment to determine if the following procedures are in place. Furthermore, the following list of controls is intended to address only those controls surrounding the interface and communication between the user entity and the Company. Accordingly, this list does not purport to be, and is not, a complete listing of the controls that provide a basis for the assertions underlying the financial statements of user entities.

- The client is responsible for controls governing access to functionality and data used by their applications. This includes the use of application configuration parameters, database configuration, and OS security parameters.
- The client is responsible for maintaining and securing their remote access into their systems that are located at the Datacenter facility.
- The client is responsible for establishing physical security protections over all workstations, servers and communication hardware that interface with their environment at the Datacenter
- The client is responsible for establishing physical security protections over all workstations, servers and communication hardware that interface with their environment at the Datacenter and that are housed in their facilities or other locations under their control or supervision. As a rule, physical access should be limited to only those individuals that require such access to perform their jobs.
- The client is responsible for maintaining a current list of personnel who have been designated to have access rights to the Datacenter. The client is also responsible for communicating changes to this list as they occur.
- The client is responsible for identifying upgrades/changes that are to be made to their environment.
- The client is responsible for encryption of stored data.
- The client is responsible for specifying initial firewall settings, and for initiating any changes to the existing configurations as needed.
- The client is responsible for administering local user and administrative accounts on their servers.
- The client is responsible for appropriately monitoring and aiding in the resolution of trouble tickets, as needed.
- The client is responsible for obtaining, monitoring, and appropriately using SSL encryption certificates, if required.

Section IV – Information Provided by the Independent Service Auditor

Purpose and Objectives of the Independent Service Auditor's Examination

This report on controls placed in operation and tests of operating effectiveness is intended to provide interested parties with information sufficient to obtain an understanding of those aspects of the Company's controls that may be relevant to a user entity's internal control environment, and reduce the assessed level of control risk below the maximum for certain financial statement assertions. This report, when coupled with an understanding of the internal controls in place at the user entity, is intended to assist in the assessment of certain General Information Technology procedures of the Company pertaining to its Dallas Texas Datacenter. As such, our examination did not extend to other TierPoint processes, locations, related entities or applications not specifically referenced in the accompanying report. Further, our examination did not extend to the procedures and controls performed by outside third parties.

The examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. It is each interested party's responsibility to evaluate this information in relation to the internal controls in place at user entities to obtain an overall understanding of the internal controls and assess control risk. The portions of the control environment provided by the user entities and TierPoint must be evaluated together. If effective user entity internal controls are not in place, then TierPoint's controls may not compensate for such weaknesses.

Our examination included inquiries of management, supervisory, and staff personnel, inspection of documents and records, and observation of activities and operations which were performed during the period from March 1, 2013 to February 28, 2014 and were applied to those controls relating to control objectives specified by TierPoint.

The Company's description of certain General Information Technology procedures pertaining to its Dallas Texas Datacenter and related control objectives is the responsibility of TierPoint's management. Our responsibility is to express an opinion that the controls are operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives, specified by TierPoint, were achieved during the period covered by our report. Concerns, if any, noted by Holtzman Partners LLP regarding the adequacy of the controls identified to achieve the stated objective or the level of compliance with the controls are presented in this section under the caption "Results of Tests". Concerns identified herein are not necessarily weaknesses in the total system of internal controls of TierPoint, as this determination can only be made after consideration of controls in place for user organizations. Control considerations that should be exercised by user organizations in order to complement the controls of TierPoint to attain the stated objective are presented when considered applicable.

Tests of Overall Control Environment

Internal control is a process designed to provide reasonable assurance that business objectives related to: (1) the reliability of financial reporting, (2) the effectiveness and efficiency of operations, and (3) compliance with applicable laws and regulations, are met. In addition to the tests of operating effectiveness of specific control activities, our procedures included tests of the following components of the overall control environment of TierPoint:

Control Environment

- Reviewed a copy of the TierPoint Employee Handbook.
- Performed a walkthrough of TierPoint's hiring practices.
- Obtained and reviewed the organization chart of TierPoint.
- Obtained evidence of EMT meetings.

Risk Management

- Obtained the organization chart and reviewed organizational structure of TierPoint.
- Reviewed a random selection of vendor contracts and verified that the vendor's obligations and liability for non-performance were included.
- Obtained evidence of EMT meetings.

Information and Communication

- Reviewed copies of the TierPoint Employee Handbook and Security policies.
- Obtained evidence of EMT meetings.

Monitoring

- Reviewed a monthly capacity report and confirmed that it contained operational information.
- Obtained evidence of EMT meetings.

* * * * *

The following tables describe the control objectives and related controls that were specified by management of the Company and the tests of operating effectiveness of those controls that were performed by Holtzman Partners, LLP. The control environment was considered in planning the nature, timing, and extent of these tests.

Certain General Information Technology Procedures

Organization and Administration

Control Objective #1 – *Controls provide reasonable assurance that the organization follows a structured hiring process, promotes appropriate employee behavior and segregates responsibilities within the organization.*

	Controls Specified by TierPoint	Tests Performed by Holtzman Partners	Results of Testing
1.1	Organizational charts are in place to communicate key areas of responsibility and appropriate lines of reporting.	Confirmed through inspection of the Company's organizational chart during the period under review that it appeared to identify areas of responsibility and lines of reporting.	No exceptions noted.
1.2	Management has established an Employee Handbook which includes sections on Employment Policies, Employee Conduct, Compensation Policies, Operations Policies and Employee Benefits.	Confirmed through inspection of the Company's Employee Handbook during the period under review that it included sections on Employment Policies, Employee Conduct, Compensation Policies, Operations Policies and Employee Benefits.	No exceptions noted.
1.3	Prior to hiring, background checks are obtained for potential employees which are performed by an external third-party.	For a selection of newly hired employees during the period under review, confirmed through inspection of documentation that background checks were obtained and these checks were performed by an external third-party.	No exceptions noted.
1.4	Upon hiring, employees are issued a copy of the Employee Handbook and are required to sign a Handbook Acknowledgement form verifying that they have received, read and agreed to abide by the terms of this Handbook.	For a selection of newly hired employees during the period under review, confirmed through inspection of documentation whether a Handbook Acknowledgement form was signed.	**Exception noted:** For 1 of 3 newly hired employees, they were hired on 8/20/13 and were terminated 3 months later without signing an Acknowledgment form. For an additional 1 of 3 newly hired employees, hired on 9/27/13, the Acknowledgment form was signed on 12/18/13. A new updated employee handbook was not available for review until that date.

Physical Security and Environmental Safeguards

Control Objective #2 – *Controls provide reasonable assurance that physical access to the Datacenter facility is restricted to authorized personnel and sufficient measures are in place and maintained for protection of these items from environmental hazards.*

	Controls Specified by TierPoint	Tests Performed by Holtzman Partners	Results of Testing
2.1	The Company maintains policies and procedures for Physical Security in and around the Datacenter.	Confirmed through inspection of the Company's policies during the period under review that they addressed Physical Security in and around the Datacenter.	No exceptions noted.
2.2	A Shipping and Receiving policy is also maintained to provide guidance for the secure temporary storage of customer packages and equipment.	Confirmed through inspection of the Company's Shipping and Receiving policy during the period under review that the policy appeared to provide guidance for the secure temporary storage of customer packages and equipment.	No exceptions noted.
2.3	NOC personnel walk through the facility every four hours to confirm that cabinets and cages are locked.	Confirmed through observation during the period under review that client cabinets and cages in the Datacenter appeared to be locked.	No exceptions noted.
2.4	Automated Helpdesk Tickets are emailed to NOC personnel to remind them of the walkthrough and these Tickets are closed once the walkthrough has been completed.	Confirmed through observation during the period under review that the Helpdesk system was configured to send reminder Tickets to NOC personnel. For a random selection of days during the period under review, attempted to confirm through inspection of documentation that Help Desk Tickets were closed indicating completion of the walkthrough.	No exceptions noted regarding the system configuration. **Exception noted:** Help Desk Tickets were not closed upon completion of the walkthrough by NOC personnel.

Physical Security and Environmental Safeguards (continued)

Control Objective #2 – *Controls provide reasonable assurance that physical access to the Datacenter facility is restricted to authorized personnel and sufficient measures are in place and maintained for protection of these items from environmental hazards.*

	Controls Specified by TierPoint	Tests Performed by Holtzman Partners	Results of Testing
2.5	Over 140 security cameras cover the exterior, interior, and Datacenter floor. Recorded video is retained for at least 90 days.	Confirmed through observation during the period under review that the security cameras existed in the Datacenter and security camera video was retained for at least 90 days.	No exceptions noted.
2.6	Access to the facility is restricted to authorized personnel (i.e. Company employees, clients, etc.) through the use of a proximity card access system.	Confirmed through observation during the period under review that a proximity card access system was in place at the Datacenter and appeared to cover all entrances to the facility.	No exceptions noted.
2.7	Authorized personnel are provided with proximity cards which are assigned access according to their requirements.	Confirmed through inspection of the Company's listing of proximity access cards for the Datacenter during the period under review that personnel included on the list were current Company employees.	No exceptions noted.
2.8	Datacenter access for new TierPoint employees is authorized by TierPoint management.	For a random selection of new employees granted access to the Datacenter during the period under review, confirmed through inspection of documentation that access was authorized by TierPoint management.	No exceptions noted.
2.9	Client access to the Datacenter is restricted to authorized individuals on client access lists.	For a random selection of clients during the period under review, confirmed through inspection of documentation that access lists were maintained for personnel permitted access to client resources within the Datacenter facility. For a random selection of requests to change client access lists during the period under review, confirmed through inspection of documentation that the changes were performed as requested.	No exceptions noted.

Physical Security and Environmental Safeguards (continued)

Control Objective #2 – *Controls provide reasonable assurance that physical access to the Datacenter facility is restricted to authorized personnel and sufficient measures are in place and maintained for protection of these items from environmental hazards.*

	Controls Specified by TierPoint	Tests Performed by Holtzman Partners	Results of Testing
2.10	Changes (additions or removals) to these lists may only be requested by the primary client contact (or client designee) and client requests and approvals are documented in a Helpdesk Ticket.	For a random selection of changes to client Datacenter access lists during the period under review, confirmed through inspection of documentation that changes were requested by the designated contact and were documented in a Helpdesk Ticket.	No exceptions noted.
2.11	Other third party access (i.e. contractors, etc.) is authorized by TierPoint management.	For a random selection of changes to third party Datacenter access during the period under review, confirmed through inspection of documentation that access was authorized by TierPoint management.	No exceptions noted.
2.12	Individuals without authorized access must sign in at the front desk and be escorted by an individual with authorized access.	Confirmed through observation during the period under review that individuals without authorized access were required to sign in at the front desk and were escorted by an individual with authorized access.	No exceptions noted.
2.13	Access for terminated TierPoint employees is revoked upon their termination.	For a random selection of terminated TierPoint employees during the period under review, confirmed through inspection of documentation that Datacenter access was revoked upon their termination.	No exceptions noted.
2.14	Multiple redundant Computer Room Air Conditioners (CRAC's) are in place to maintain a constant temperature and humidity level.	Confirmed through observation during the period under review that the Datacenter maintained multiple redundant Computer Room Air Conditioners (CRAC's).	No exceptions noted.

Physical Security and Environmental Safeguards (continued)

Control Objective #2 – *Controls provide reasonable assurance that physical access to the Datacenter facility is restricted to authorized personnel and sufficient measures are in place and maintained for protection of these items from environmental hazards.*

	Controls Specified by TierPoint	Tests Performed by Holtzman Partners	Results of Testing
2.15	The Datacenter is equipped with multiple High Sensitivity Smoke Detection (HSSD) sensors which continuously monitor the air throughout the facility.	Confirmed through observation during the period under review that the Datacenter maintained multiple High Sensitivity Smoke Detection sensors throughout the facility.	No exceptions noted.
2.16	Chemical fire extinguishers are located prominently throughout the facility.	Confirmed through observation during the period under review that the Datacenter maintained multiple chemical fire extinguishers.	No exceptions noted.
2.17	The fire suppression system in the facility is a Dual Interlock, Dry Pipe, Pre-Action sprinkler system.	Confirmed through observation during the period under review that the Datacenter maintained a Dual Interlock, Dry Pipe, Pre-Action sprinkler system.	No exceptions noted.
2.18	Temperature, humidity, fire, and smoke detection and action systems are maintained on an annual basis to help ensure that they are operating properly.	Confirmed through inspection of documentation that during the period under review, temperature, humidity, fire, and smoke detection and action systems were tested.	No exceptions noted.
2.19	Conditioned UPS (Uninterruptible Power Supply) units are utilized to supply power for short term power issues and these units are monitored real-time to help ensure that they are healthy and can be used in the event of an issue.	Confirmed through observation during the period under review that the Datacenter maintained multiple UPS units and these units appeared to be monitored by Datacenter personnel.	No exceptions noted.
2.20	In the event of an extended power outage, on-site diesel generators are in place to generate power for the facility until power is restored.	Confirmed through observation during the period under review that on-site diesel generators were in place at the Datacenter.	No exceptions noted.

Logical Security

Control Objective #3 – *Controls provide reasonable assurance that logical access to the network systems and devices is restricted to authorized individuals.*

	Controls Specified by TierPoint	Tests Performed by Holtzman Partners	Results of Testing
3.1	The Company utilizes Active Directory as a central point of verification for access to its network and user id and password requirements have been established for TierPoint servers and network devices.	Confirmed through observation during the period under review that the Company utilized Active Directory which appeared to be a central point of verification for access to the Company's network.	No exceptions noted.
3.2	Password parameters for servers and network devices are in compliance with documented standards including minimum length, complexity, and age requirements.	Confirmed through observation that the Company's servers and network devices were configured for additional password requirements including minimum length, complexity, and maximum age.	No exceptions noted.
3.3	Passwords to shared accounts for the network, servers and devices are stored in an in-house developed password management tool.	Confirmed through observation during the period under review that passwords to shared accounts for the network, servers and devices appeared to be stored in an in-house developed password management tool.	No exceptions noted.
3.4	Access to the password tool is restricted to current NOC personnel, the General Manager and the Director of Facilities.	Confirmed through observation during the period under review that access to the password tool was restricted to current NOC personnel, the General Manager and the Director of Facilities.	No exceptions noted.
3.5	Passwords stored in the tool are encrypted to enhance the security of the data.	Confirmed through observation during the period under review that passwords stored in the tool were encrypted.	No exceptions noted.

Logical Security (continued)

Control Objective #3 – *Controls provide reasonable assurance that logical access to the network systems and devices is restricted to authorized individuals.*

	Controls Specified by TierPoint	Tests Performed by Holtzman Partners	Results of Testing
3.6	Administrative access to the Company's network and servers is restricted to current NOC personnel, the General Manager and the Director of Facilities.	Confirmed through observation during the period under review that administrative access to the Company's network and servers was restricted to current NOC personnel, the General Manager and the Director of Facilities.	No exceptions noted.
3.7	An encrypted Virtual Private Network (VPN) is utilized to grant remote access.	Confirmed through observation during the period under review that an encrypted Virtual Private Network (VPN) was utilized to grant remote access.	No exceptions noted.
3.8	Access to the VPN is restricted to TierPoint employees.	Confirmed through inspection of the VPN access listing during the period under review that access to the Company's VPN was restricted to TierPoint employees.	No exceptions noted.
3.9	Access to the network, servers and devices is removed upon termination of a TierPoint employee.	For a random selection of terminated TierPoint employees during the period under review, confirmed through inspection of documentation that their access to the network, servers and devices had been removed.	No exceptions noted.

Logical Security (continued)

Control Objective #3 – *Controls provide reasonable assurance that logical access to the network systems and devices is restricted to authorized individuals.*

	Controls Specified by TierPoint	Tests Performed by Holtzman Partners	Results of Testing
3.10	Various network security policies and procedures are documented to include Encryption, Acceptable Use, Anti-virus, Password, Remote Access, and Server Security.	Confirmed through inspection of the Company's network security policies during the period under review and confirmed through inspection of documentation that they included Encryption, Acceptable Use, Anti-virus, Password, Remote Access, and Server Security.	No exceptions noted.
3.11	Network diagrams are documented to detail the connections between communications equipment.	Confirmed through inspection of the Company's network diagrams during the period under review that the diagrams documented connections between communications equipment.	No exceptions noted.
3.12	Virus protection software is installed on NOC workstations and is scheduled to scan on a weekly basis.	Confirmed through observation during the period under review that virus protection software appeared to be installed on NOC workstations and was configured to perform weekly scans.	No exceptions noted.

Service Management

Control Objective #4 – *Controls provide reasonable assurance that service incidents are tracked, recorded, and resolved.*

	Controls Specified by TierPoint	Tests Performed by Holtzman Partners	Results of Testing
4.1	Network Trouble Escalation procedures are documented to ensure rapid resolution of issues to the network, server or device impacted.	Confirmed through inspection of the Company's Network Trouble Escalation procedure during the period under review that it appeared to address procedures to help ensure resolution of issues to the network, server or device impacted.	No exceptions noted.
4.2	Servers, devices and the network are monitored for DDoS attacks and abnormal network traffic.	Confirmed through inspection of the monitoring tool configuration that the tool was configured to monitor server, device and network traffic.	No exceptions noted.
4.3	Events that are captured in the network monitoring system result in Tickets (within the Helpdesk System) being either automatically or manually generated.	For a random selection of network related Help Desk tickets during the period under review, confirmed through inspection of documentation that they appeared to be related to aberrant or exceptional conditions and confirmed through inspection of documentation that the potential issue was addressed.	No exceptions noted.
4.4	Once an event has been addressed and resolved, the Ticket is updated and closed.	For a random selection of IT Infrastructure changes during the period under review, confirmed through inspection of documentation that approval from an Operations or TSC Manager was obtained prior to deployment into production.	No exceptions noted.