Hivelocity Ventures Corporation
Type 2 SOC 2
2018

REPORT ON HIVELOCITY VENTURES CORPORATION'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY AND AVAILABILITY

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

April 1, 2017 Through March 31, 2018

Table of Contents

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS AT HIVELOCITY VENTURES CORPORATION RELEVANT TO SECURITY AND AVAILABILITY

To Hivelocity Ventures Corporation:

We have examined the attached description titled "Description of Hivelocity Ventures Corporation's Colocation Services System Throughout the Period April 1, 2017 To March 31, 2018" (the description) and the suitability of the design and operating effectiveness of controls to meet the criteria for the security and availability principles set forth in TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Technical Practice Aids*) (applicable trust services criteria), throughout the period April 1, 2017 to March 31, 2018. The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of Hivelocity Ventures Corporation's ('Hivelocity' or 'the Company') controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

Hivelocity has provided the attached assertion titled "Management of Hivelocity Ventures Corporation's Assertion Regarding Its Colocation Services System Throughout the Period April 1, 2017 To March 31, 2018," which is based on the criteria identified in management's assertion. Hivelocity is responsible for (1) preparing the description and assertion; (2) the completeness, accuracy, and method of presentation of both the description and assertion; (3) providing the services covered by the description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in Hivelocity's assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period April 1, 2017 to March 31, 2018.

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

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

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

a. the description fairly presents the system that was designed and implemented throughout the period April 1, 2017 to March 31, 2018.

b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period April 1, 2017 to March 31, 2018, and user entities applied the complementary user-entity controls contemplated in the design of Hivelocity's controls throughout the period April 1, 2017 to March 31, 2018.
c. the controls tested, which together with the complementary user-entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period April 1, 2017 to March 31, 2018.

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

This report and the description of tests of controls and results thereof are intended solely for the information and use of Hivelocity; user entities of Hivelocity's Colocation Services System during some or all throughout the period April 1, 2017 to March 31, 2018; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

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

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

April 2, 2018
Tampa, Florida

SECTION 2

MANAGEMENT OF HIVELOCITY VENTURES CORPORATION'S ASSERTION REGARDING ITS SYSTEM THROUGHOUT THE PERIOD APRIL 1, 2017 TO MARCH 31, 2018

Management of Hivelocity Ventures Corporation's Assertion Regarding Its System Throughout the Period April 1, 2017 to March 31, 2018

April 2, 2018

We have prepared the attached description titled "Description of Hivelocity Ventures Corporation's Colocation Services System Throughout the Period April 1, 2017 To March 31, 2018" (the description), based on the criteria in items (a)(i)–(ii) below, which are the criteria for a description of a service organization's system in paragraphs 1.34–.35 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (the description criteria). The description is intended to provide users with information about the Colocation Services System, particularly system controls intended to meet the criteria for the security and availability principles set forth in TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Technical Practice Aids*) (applicable trust services criteria). We confirm, to the best of our knowledge and belief, that:

a. The description fairly presents the Colocation Services System throughout the period April 1, 2017 to March 31, 2018, based on the following description criteria:

   i. The description contains the following information:

      (1) The types of services provided.

      (2) The components of the system used to provide the services, which are the following:

         - *Infrastructure*. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).
         - *Software*. The application programs and IT systems software that supports application programs (operating systems, middleware, and utilities).
         - *People*. The personnel involved in governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
         - *Processes*. The automated and manual procedures.
         - *Data*. Transaction streams, files, databases, tables, and output used or processed by a system.

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

      (4) How the system captures and addresses significant events and conditions.

      (5) The process used to prepare and deliver reports and other information to user entities or other parties.

      (6) If information is provided to, or received from, subservice organizations or other parties, how such information is provided or received; the role of the subservice organization or other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

      (7) For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the service organization's system.

      (8) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons therefore.

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

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

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

b. The controls stated in description were suitably designed throughout the specified period to meet the applicable trust services criteria.

c. The controls stated in the description operated effectively throughout the specified period to meet the applicable trust services criteria.

Lionel Martinez
CFO
Hivelocity Ventures Corporation

SECTION 3

DESCRIPTION OF HIVELOCITY VENTURES CORPORATION'S SYSTEM THROUGHOUT THE PERIOD APRIL 1, 2017 TO MARCH 31, 2018

OVERVIEW OF OPERATIONS

Company Background

Hivelocity operates two enterprise class data centers (TPA1 and TPA2) located in Tampa Bay as well as POP sites in Atlanta, Miami, Los Angeles and New York.

TPA1 and TPA2 are above the FEMA 500-year flood plain and have brick and concrete construction built to withstand extreme environmental conditions. TPA1 has 3,750 gallons of diesel fuel on premise allowing the 1.25-megawatt Cummins generator to keep the facility fully powered for up to one week. The 250+ tons of data center air conditioning keeps its Tampa colocation facility at 72 degrees. TPA2 has 2,500 gallons of diesel fuel on premise allowing the 1.5-megawatt Cummins generator to keep the facility fully powered for up to 5 days. The 160 tons of data center air conditioning keeps its Tampa colocation facility at 72 degrees with provisions for an additional 300 tons with further expansion.

Hivelocity's data centers maintain fuel contracts with diesel vendors across three counties and is on the government list of critical facilities if the need for emergency refueling were to arise. Hivelocity's data centers maintain proper humidity conditions year-round.

Description of Services Provided

Hivelocity's colocation services offer the connectivity, redundancy, and security needed for state-of-the art data center hosting. The services include secure data centers with 24/7 engineering support.

Connectivity

Hivelocity connects with Tier1 Providers and Peering exchanges via multiple 10 Gbps fiber optics links. This allows for over 800 Gbps of capacity to the web. Hivelocity ensures that it has reliable, high-speed communications by analyzing and optimizing traffic in real time using Noction Intelligent Routing Platform for BGP routing.

Hivelocity has built out a complex, high capacity network to serve its customers. It begins with 400 Gbps private network rings that service Tampa Bay and Los Angeles which connects Hivelocity's data centers and POPs. In addition, Hivelocity has several direct 10Gbps "waves" inter-connecting the facilities that Hivelocity services its customers. Hivelocity further enhances its network by connecting to popular peering exchanges in Los Angeles, Atlanta, Miami, New York and Tampa, which helps to reduce overall latency to all Hivelocity's customers that are all inter-connected to Hivelocity's backbone.

The ability to connect directly to common networks i.e. Google, Microsoft, etc. via direct peer along with dynamically optimizing traffic based on real time statistics such as latency, packet loss and jitter allows any service using Hivelocity's network to get the absolute best and most reliable connections and speeds. Combined with the latest networking hardware and network design, this combination provides an extremely high level of service for Hivelocity's clients. Hivelocity's network capacity is complimented via purpose built layer7 network monitoring and DDOS mitigation system. This provides resiliency and durability even in the faces of denial of service("DOS") or distributed DOS attacks which are common on today's internet.

Key features providing connectivity services:

- Transit Providers - Level3, CenturyLink, Cogent, Hurricane Electric, Comcast, XO, NTT, Telia Italia
- Routing Protocol - BGP and Noction Intelligent Routing platform
- Connectivity - multiple 10 Gbps ports to each transit provider
- Peering - private peering established in LA, Atlanta, Miami, Tampa and New York
- Network Capacity - over 800 Gbps

Redundancy

Hivelocity provides a high level of hosting service and reliability. Its data centers use redundant Juniper and Brocade components to eliminate any single point of network layer failure. Its network is multi-homed through redundant Tier 1 carriers, resulting in fast and reliable Internet connectivity. Hivelocity also has multiple fiber entry points into its data centers to protect its Internet connectivity.

Hivelocity's data centers use redundant computer room air conditioning ("CRAC") systems to maintain optimum temperature and humidity levels. Both data centers also use redundant uninterruptible power supply ("UPS") systems backed up by diesel generator power to ensure extended uptime. If there is a utility power interruption, data center power immediately fails over to N+1 UPS and battery banks. If utility power has not been fully restored after 5 seconds, the diesel generator automatically starts, and power is transferred to the generator 5 seconds later. Generator power is maintained for 30 minutes after reliable utility power has been fully restored. Power is automatically conditioned during each transfer by N+1 UPS and battery banks to maintain clean and reliable power. Hivelocity maintains on-site diesel fuel capacity for one week, with refueling provisions for longer outages.

Hivelocity provides redundant communications through redundant fiber optic entry points, multiple transit providers, and redundant network equipment.

Major components providing redundancy at TPA 1:

- Eight transit providers
- Fiber entry points at opposite ends of the data center
- N+1 UPS and battery installations
- Diesel generator with one-week run-time fuel capacity
- N+1 CRAC cooling
- Preventive maintenance contracts on all critical assets

Major components providing redundancy at TPA 2:

- Fiber entry points at opposite ends of the data center
- N+1 UPS and battery installations
- Diesel generator with 5-day run-time fuel capacity
- N+1 CRAC cooling
- Preventive maintenance contracts on all critical assets

Security

Hivelocity maintains industry best practices in the physical security of its data centers. Only Hivelocity employees and authorized vendor support personnel are allowed unescorted access to the data centers and offices. Access to the building is only granted via employee proximity cards or after security clearance from within the secured lobby. If a customer needs physical access to colocation space, they are provided unescorted access to their area through a separate back entrance. Secure computer labs and work benches are provided off the data center floor for on-site customer needs. Additional security measures include fire detection and suppression systems and video monitoring and recording.

Infrastructure

Primary infrastructure used to provide Hivelocity's Colocation services system includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Firewall	Juniper	Filters traffic in and out of corporate servers and network

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Switch	Brocade and Juniper	Provide switching between servers on the same network
Routers	Brocade and Juniper	Connects multiple unique networks and switches packets within each network
Web Servers	Dedicated and Virtual	Supports the client facing web application
Ubersmith	Dedicated and Virtual	Billing System, support system and bandwidth monitoring for services

Software

Primary software used to provide Hivelocity's Colocation services system includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
MyVelocity	Linux	Client portal access for Hivelocity Services
Ubersmith	Linux	Billing System, support system and bandwidth monitoring for services
Webservers	Linux	Web Server for all client facing services
Databases	Linux	Master and Slave Database Servers

People

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

- Executive management - provides general oversight and strategic planning of operations
- Development team - responsible for delivering a responsive system that fully complies with the functional specification
- DevOps team - verifies that the system complies with the functional specification through functional testing procedures. Also, responsible for the effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the system. Performs regular scheduled audits relative to the defined standards, provides continuous improvement feedback, and assesses legal and regulatory requirements
- Support team - serves customers by providing product and services information that includes resolving product and service issues

Customer equipment is managed by the customer. Customer information is captured by Hivelocity in delivering its colocation services. Such information includes but is not limited to, the following:

- Space, power, connectivity
- Rack Location
- Alert notifications received from automated systems

Processes

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Hivelocity policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Hivelocity team member.

Physical Security

Security of customer data and systems are especially critical in a colocation environment. The data centers are designed with security of these critical assets as a primary objective. Hivelocity offers predictable, reliable security of customers' critical systems through consistent monitoring of all critical areas 24/7/365. Physical security of the data centers is provided by a combination of proximity badge access control system, hi-resolution motion-sensing digital video surveillance system, and onsite data center personnel. The buildings are secured at all entrances. Each entrance can only be accessed by a proximity badge access system. Access into the inner data centers require a proximity badge and personal identification number (PIN) authentication. Positive identification is required before access to either facility can be granted. Security features include:

- Strictly enforced security policies - Escort requirements limit unescorted access to the inner data center and other areas of the facility to authorized Hivelocity, vendor support personnel and to customers in a designated customer area
- Indoor and outdoor security monitoring - closed circuit TV (CCTV) is used throughout both data centers with real-time recording of activity. The surveillance images are maintained for a minimum of 90 days

To gain access to the internal areas of either data center, visitors must abide by the Hivelocity physical access procedures contained in the Hivelocity Information Security Policy.

Proximity Badge Access System

The facilities are secured using a proximity badge access system. The system prevents unauthorized entry throughout the facilities. Access to various security zones in the building is defined for authorized individuals based on their job function or visit purpose.

An individual must scan their card to enter secured zones within the facilities. PIN entry is also required for entry into the inner data centers. Authorized Hivelocity employees grant access to the specified zones within the facility.

Additionally, at TPA 2 an individual must present their card to the biometric read and a valid finger print to enter the data center.

The proximity badge access system records and logs individuals' movements throughout the facilities. As directed by the Hivelocity security policies, employees are required to scan their cards individually at each point controlled by the proximity badge access system to ensure all employees' activity is appropriately logged. Visitors must be escorted to and from different zones by Hivelocity personnel.

Hivelocity revokes terminated employees' physical access to the Hivelocity facilities. Terminated employees access is revoked within 24 hours of notification from Human Resources. Communications are sent out to the Chief Operating Officer for employee on-boarding and termination processing. Hivelocity removes network and physical access and follows a formal terminated employee checklist that includes processing steps when an employee leaves the Company.

Power

Equipment in the data centers are connected to a redundant UPS system to provide temporary electricity in the event of a power outage and to mitigate the risk of power surges impacting infrastructure in the data centers.

Hivelocity has separate and secure power management and power backup systems. Power is provided to the data centers from the local substation. Hivelocity has redundant UPS systems for fault tolerance to customer server cabinets.

Loss of utility power triggers an automatic transfer switch, which automatically signals the generator to start. The generator system comes online and provides power until utility power is restored.

Backup Power Features at TPA 1:

UPS system:
- Dual UPS systems
- Preventative maintenance is performed twice a year
- Quarterly inspections use an infrared sensor to detect grounds and shorts

Generator:
- 1.25 MW standby diesel generation
- One-week on-site fuel supply
- Automatic power transfer switch monitoring backup generator power

Heating, Ventilation, and Air Conditioning (HVAC):
- Redundant CRAC systems to maintain optimum temperature and humidity levels
- The data center has over 200 tons of N+1 cooling capacity

Backup Power Features at TPA 2:

UPS system:
- Redundant UPS systems
- Preventative maintenance is performed twice a year
- Quarterly inspections use an infrared sensor to detect grounds and shorts

Generator:
- 1.5 MW standby diesel generation
- 5-day on-site fuel supply
- Automatic power transfer switch monitoring backup generator power

Heating, Ventilation, and Air Conditioning (HVAC):
- Redundant CRAC systems to maintain optimum temperature and humidity levels
- The data center has over 180 tons of N+1 cooling capacity

Data Center Installation

Colocation equipment is maintained in cabinets and located on a raised floor to protect the equipment from localized flooding. The data centers are equipped with a temperature monitoring, humidity monitoring and a leak detection system to alert onsite personal if temperature, humidity, or water leak parameters are exceeded.

Data

Hivelocity provides customers with colocation services and does not handle customer data.

Boundaries of the System

The scope of this report includes the Colocation services system performed in the Hampton Oaks and Woodlands Tampa, FL facilities.

Significant Events and Conditions

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

Preparation and Delivery of Reports and Data

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

Subservice Organizations

No subservice organizations were included in the scope of this assessment.

Criteria Not Applicable to the System

The following criteria are not applicable to the system:

Criteria Not Applicable to the System		
Principle	**Criteria**	**Reason**
Common Criteria	CC5.7	Hivelocity services do not include the transmission, movement, and removal of customer information

Significant Changes Since the Last Review / in the Last 12 Months

No significant changes have occurred to the services provided to user entities since the organization last review.

CONTROL ENVIRONMENT

Integrity and Ethical Values

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

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

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook
- Background checks are performed for employees as a component of the hiring process

Commitment to Competence

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

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

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements
- Ongoing training is provided to maintain the skill level of personnel in certain positions

Management's Philosophy and Operating Style

Hivelocity's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

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

- Management is periodically briefed on regulatory and industry changes affecting the services provided
- Management meetings are held on a weekly basis to discuss operational issues

Organizational Structure and Assignment of Authority and Responsibility

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

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

Human Resources Policies and Practices

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

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

- Hiring procedures are in place
- Evaluations for each employee are performed on an annual basis
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

RISK ASSESSMENT

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

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

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

Hivelocity has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Hivelocity attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

TRUST SERVICES PRINCIPLES AND CRITERIA

In-Scope Trust Services Principles

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

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

Integration with Risk Assessment

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

Control Activities Specified by the Service Organization

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

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

MONITORING

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

On-Going Monitoring

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

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

Reporting Deficiencies

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

INFORMATION AND COMMUNICATION SYSTEMS

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

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, meetings are held semi-annually to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead these meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Hivelocity personnel via e-mail messages.

Specific information systems used to support Hivelocity's colocation system are described in the Description of Services section above.

COMPLEMENTARY USER ENTITY CONTROLS

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

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

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

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

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

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

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

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

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

Control Activities Specified by the Service Organization

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC1.0	**Common Criteria Related to Organization and Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.1	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.	A documented organizational chart is in place to communicate organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place to communicate organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Reporting relationships and organizational structures are reviewed periodically by senior management.	Inquired of the human resource manager regarding the review of reporting relationships and organizational structure to determine that reporting relationships and organizational structures were reviewed periodically by senior management.	No exceptions noted.
			Inspected the organizational chart versioning to determine that reporting relationships and organizational structures were reviewed periodically by senior management.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel.	Inspected a sample of job descriptions to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC1.0	**Common Criteria Related to Organization and Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Senior management reviews job descriptions on an annual basis and makes updates, if necessary.	Inquired of the human resource manager regarding the review of job descriptions to determine that senior management reviewed job descriptions on an annual basis and made updates, if necessary.	No exceptions noted.
			Inspected a sample of job descriptions to determine that senior management reviewed job descriptions on an annual basis and made updates, if necessary.	No exceptions noted.
		A documented organizational chart is in place to assign responsibility and delegate lines of authority to personnel.	Inspected the organizational chart to determine that a documented organizational chart was in place to assign responsibility and delegate lines of authority to personnel.	No exceptions noted.
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security and availability.	A documented organizational chart is in place to assign responsibility and delegate lines of authority to personnel.	Inspected the organizational chart to determine that a documented organizational chart was in place to assign responsibility and delegate lines of authority to personnel.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC1.0	**Common Criteria Related to Organization and Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability and provides resources necessary for personnel to fulfill their responsibilities.	Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process.	Inquired of the human resource manager regarding hiring procedures to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements were evaluated as part of the hiring or transfer evaluation process.	No exceptions noted.
			Inspected a sample of job descriptions to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements were evaluated as part of the hiring or transfer evaluation process.	No exceptions noted.
		A new hire checklist is completed by human resource personnel for new hire employees as part of the entity's onboarding process.	Inspected a sample of new hire checklists to determine that a new hire checklist was completed by human resource personnel for new hire employees as part of the entity's onboarding process.	No exceptions noted.
		The experience and training of candidates for employment or transfer are evaluated before they assign the responsibilities of their respective position.	Inspected job requirements listed within a sample of job descriptions to determine that the experience and training of candidates for employment or transfer were evaluated before they assigned the responsibilities of their respective position.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC1.0	**Common Criteria Related to Organization and Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Employee evaluations are performed for employees on an annual basis.	Inspected the employee performance reviews for a sample of current employees to determine that employee evaluations were performed for employees on an annual basis.	No exceptions noted.
		Management documents skills and continued training to establish the organization's commitments and requirements for employees.	Inspected the information security awareness training policy to determine that management documented skills and continued training to establish the organization's commitments and requirements for employees.	No exceptions noted.
		Management tracks and monitors compliance with training requirements.	Inquired of the human resource manager regarding the monitoring of training to determine that management tracked and monitored compliance with training requirements.	No exceptions noted.
			Inspected the training sign-in sheets to determine that management tracked and monitored compliance with training requirements.	No exceptions noted.
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 system requirements as they relate to security and availability.	Personnel are required to sign and accept the employee handbook upon hire and annually thereafter.	Inspected signed employee handbook acknowledgement forms for a sample of newly hired employees to determine that personnel were required to sign and accept the employee handbook upon hire and annually thereafter.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC1.0	**Common Criteria Related to Organization and Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Personnel are required to complete a background check provided by a third-party vendor upon hire.	Inspected the background check policy and information release authorizations for a sample of newly hired employees to determine that personnel were required to complete a background check provided by a third-party vendor upon hire.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC2.0	**Common Criteria Related to Communications**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.	System descriptions are communicated to authorized external users via service level agreements (SLA) that delineate the boundaries of the system and describe relevant system components.	Inspected a sample of SLA acknowledgements to determine that system descriptions were communicated to authorized external users via service level agreements that delineated the boundaries of the system and described relevant system components.	No exceptions noted.
		A description of the system is posted on the entity's intranet and is available to the entity's internal users. This description delineates the boundaries of the system.	Inspected the policy and procedure centralized document repository to determine that a description of the system was posted on the entity's intranet and was available to the entity's internal users. This description delineated the boundaries of the system.	No exceptions noted.
		A description of the entity organization structure, system support functions, processes, and organizational roles and responsibilities is posted on the entity's intranet.	Inspected the organizational chart to determine that a description of the entity organization structure, system support functions, processes, and organizational roles and responsibilities was posted on the entity's intranet.	No exceptions noted.
		Customer responsibilities are outlined and communicated through service level agreements.	Inspected a sample of SLA acknowledgements to determine that customer responsibilities were outlined and communicated through service level agreements.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC2.0	**Common Criteria Related to Communications**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.2	The entity's security and availability commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.	Security and availability commitments are communicated to external users via defined SLA.	Inspected a sample of SLA acknowledgements to determine that security and availability commitments were communicated to external users via defined SLA.	No exceptions noted.
		Policies and procedures are documented for significant processes and are available to personnel on the entity's intranet.	Inspected the policy and procedure centralized document repository to determine that policies and procedures were documented for significant processes and were available to personnel on the entity's intranet.	No exceptions noted.
		Personnel are required to attend annual security training.	Inspected the security awareness training sign in sheets to determine that personnel were required to attend annual security training.	No exceptions noted.
		Personnel are required to read and accept the entity's employee handbook and non-disclosure agreement upon hire.	Inspected signed employee handbooks and non-disclosure agreements for a sample of newly hired employees to determine that personnel were required to read and accept the entity's employee handbook and non-disclosure agreement upon hire.	No exceptions noted.
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	Policies and procedures are documented for significant processes and are available to personnel on the entity's intranet.	Inspected the policy and procedure centralized document repository to determine that policies and procedures were documented for significant processes and were available to personnel on the entity's intranet.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC2.0	**Common Criteria Related to Communications**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Roles and responsibilities are defined in job descriptions and communicated to personnel responsible for system security and availability.	Inspected a sample of job descriptions to determine that roles and responsibilities were defined in job descriptions and communicated to personnel responsible for system security and availability.	No exceptions noted.
		Senior management reviews job descriptions on an annual basis and makes updates, if necessary.	Inquired of the human resource director regarding the review of job descriptions to determine that senior management reviewed job descriptions on an annual basis and made updates, if necessary.	No exceptions noted.
			Inspected a sample of job descriptions to determine that senior management reviewed job descriptions on an annual basis and made updates, if necessary.	No exceptions noted.
		Customer responsibilities are described on the customer facing website and/or in system documentation.	Inspected a sample of SLA acknowledgements to determine that customer responsibilities were described on the customer website and/or in system documentation.	No exceptions noted.
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.	Policies and procedures are documented for significant processes and are available to personnel on the entity's intranet.	Inspected the policy and procedure centralized document repository to determine that policies and procedures were documented for significant processes and were available to personnel on the entity's intranet.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC2.0	**Common Criteria Related to Communications**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Processes are monitored through service level management procedures to help ensure compliance with service level commitments and agreements.	Inspected a sample of email notifications to determine that processes were monitored through service level management procedures to help ensure compliance with service level commitments and agreements.	No exceptions noted.
		Customer responsibilities are described on the customer website and/or in system documentation.	Inspected a sample of SLA acknowledgements to determine that customer responsibilities were described on the customer website and/or in system documentation.	No exceptions noted.
		Personnel attend training courses on an annual basis to further their knowledge of technical subjects.	Inspected the security awareness training sign in sheets to determine that personnel attended training courses on an annual basis to further their knowledge of technical subjects.	No exceptions noted.
CC2.5	Internal and external users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel.	The organization's security policies and code of behavior are communicated to employees in the employee handbook.	Inspected the employee handbook to determine that the organization's security policies and code of behavior were communicated to employees in the employee handbook.	No exceptions noted.
		Documented incident response policies and procedures are in place and are available for review by employees on the company intranet.	Inspected the incident response plan to determine that documented incident response policies and procedures were in place and were available for review by employees on the company intranet.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC2.0	**Common Criteria Related to Communications**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Defined SLAs are in place and communicated to authorized external users. The SLAs include communication procedures for reporting security and availability related failures, incidents, and concerns to personnel.	Inspected a sample of SLA acknowledgements to determine that defined SLAs were in place and communicated to authorized external users. The SLAs included communication procedures for reporting security and availability related failures, incidents, and concerns to personnel.	No exceptions noted.
CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security and availability are communicated to those users in a timely manner.	Proposed system changes affecting customers are emailed to the entity's customers. Changes made to systems are communicated and confirmed with customers through ongoing communication mechanisms.	Inquired of the development & operations leader regarding system changes to determine that proposed system changes affecting customers were emailed to the entity's customers. Changes made to systems were communicated and confirmed with customers through ongoing communication mechanisms.	No exceptions noted.
			Inspected the incident response plan and a sample of incident tickets to determine that proposed system changes affecting customers were emailed to the entity's customers. Changes made to systems were communicated and confirmed with customers through ongoing communication mechanisms.	No exceptions noted.

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

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC3.0	**Common Criteria Related to Risk Management and Design and Implementation of Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.	Management has defined a formal risk management process that specifies the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the most recently completed risk assessment report to determine that management had defined a formal risk management process that specified the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
		Internal and external vulnerability scans are performed on a quarterly basis and remedial actions are taken.	Inspected a sample of internal and external network vulnerability scans to determine that internal and external vulnerability scans were performed on a quarterly basis and remedial actions were taken.	No exceptions noted.
		Business recovery plans are tested on an annual basis.	Inspected the business continuity plan and incident response test to determine that business recovery plans were tested on an annual basis.	No exceptions noted.
		During the risk assessment and management process, management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.	Inspected the most recently completed risk assessment report to determine that during the risk assessment and management process, management personnel identified changes to business objectives, commitments and requirements, internal operations, and external factors that threatened the achievement of business objectives and updated the potential threats to system objectives.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC3.0	**Common Criteria Related to Risk Management and Design and Implementation of Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		During the risk assessment and management process, management personnel identify environmental, regulatory, and technological changes that have occurred.	Inspected the most recently completed risk assessment report to determine that during the risk assessment and management process, management personnel identified environmental, regulatory, and technological changes that have occurred.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC4.0	**Common Criteria Related to Monitoring of Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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 availability, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. This software sends automated messages to operations personnel when specific predefined thresholds are met.	Observed the NMIS (Network Management Information Systems) configurations to determine that monitoring software was used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. This software sent automated messages to operations personnel when specific predefined thresholds were met. Inspected the NMIS (Network Management Information Systems) configurations and a sample email notification to determine that monitoring software was used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. This software sent automated messages to operations personnel when specific predefined thresholds were met.	No exceptions noted. No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC4.0	**Common Criteria Related to Monitoring of Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Operations and security personnel follow defined protocols for resolving and escalating reported events.	Inspected the incident response plan to determine that the operations and security personnel followed defined protocols for resolving and escalating reported events. Inspected a sample of incident tickets to determine that operations and security personnel followed defined protocols for resolving and escalating reported events.	No exceptions noted. No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability.	The Hivelocity online application (MyVelocity) matches each user account to a single customer account number. Users' access is restricted to their respective data.	Inspected the application configurations to determine that the Hivelocity online application (MyVelocity) matched each user account to a single customer account number and that users' access was restricted to their respective data.	No exceptions noted.
		A role based security process has been defined with an access control system that is required to use roles when possible.	Inspected the network and application user listings to determine that a role based security process had been defined with an access control system that was required to use roles when possible.	No exceptions noted.
		Privileged access to sensitive resources is restricted to defined user roles.	Inspected the application superuser listing and network administrator listing to determine that privileged access to sensitive resources was restricted to defined user roles.	No exceptions noted.
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security and availability. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Hivelocity users are authenticated via an authorized user account, password, and yubikey.	Inspected application authentication procedures and login configurations to determine that Hivelocity users were authenticated via an authorized user account, password, and yubikey.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Terminated employee access to Ubersmith is revoked as a component of the termination procedures.	Inspected the termination checklists and cross-referenced it to the Ubersmith user listing for a sample of terminated employees to determine that terminated employee access to Ubersmith was revoked as a component of the termination procedures.	No exceptions noted.
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security and availability.	The Hivelocity online application (MyVelocity) matches each user account to a single customer account number. Users' access is restricted to their respective data.	Inspected the application configurations to determine that the Hivelocity online application (MyVelocity) matched each user account to a single customer account number and that users' access was restricted to their respective data.	No exceptions noted.
		Users can only access the system remotely through secure sockets layer (SSL) encryption.	Inspected the SSL certificate to determine that users could only access the system remotely through secure sockets layer (SSL) encryption.	No exceptions noted.
		The Ubersmith application is configured to enforce minimum password complexity standards before granting access the application.	Inspected the Ubersmith application authentication configurations to determine that the Ubersmith application was configured to enforce minimum password complexity standards, and expiration before granting access the application.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security and availability.	User access requests are documented, tracked, and approved by a direct supervisor.	Inspected the approved access change forms for a sample of newly hired employees to determine that user access requests were documented, tracked, and approved by a direct supervisor.	No exceptions noted.
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security and availability.	A badge and Personal Identification Number (PIN) 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 the physical access procedures to the data center facilities to determine that a badge and PIN based physical access control system had been implemented within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities.	No exceptions noted.
		Access to the building is only granted via employee proximity cards or after security clearance from within the secured lobby.	Observed the physical access procedures to the data center facilities to determine that access to the building was only granted via employee proximity cards or after security clearance from within the secured lobby.	No exceptions noted.
		Access into the inner data center requires proximity badge and PIN authentication.	Observed the physical access procedures to the data center facilities to determine that access into the inner data center required proximity badge and PIN authentication.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Visitors must be escorted at all times by Hivelocity personnel or the customer who authorized their entrance to the colocation area of the data center.	Observed the physical access procedures for visitors to determine that visitors were escorted at all times by Hivelocity personnel or the customer who authorized their entrance to the colocation area of the data center.	No exceptions noted.
		Physical access of terminated employees is revoked as a component of the termination procedures.	Inspected the card holder details for a sample of terminated employees to determine that physical access of terminated employees was revoked as a component of the termination procedures.	No exceptions noted.
		Doors that access the inner data center can only be opened by the PINs of designated personnel.	Observed the physical access procedures to the data center facilities to determine that doors that accessed the inner data center could only be opened by the PINs of designated personnel.	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.	External access to nonpublic sites is restricted through the use of user authentication and message encryption systems such as SSL.	Inspected the SSL certificate to determine that external access to nonpublic sites was restricted through the use of user authentication and message encryption systems such as SSL.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security and availability.	Not applicable - Hivelocity services do not include the transmission, movement, and removal of information.	Not applicable.	Not applicable.
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.	The ability to install software on workstations and laptops is restricted to IT support personnel.	Inspected workstation configurations to determine that the ability to install software on workstations and laptops was restricted to IT support personnel.	No exceptions noted.
		Antivirus software is installed on workstations, laptops, and servers supporting such software.	Inspected the remote administrator antivirus software configurations to determine that antivirus software was installed on workstations, laptops, and servers supporting such software.	No exceptions noted.
		Antivirus software is configured to receive an updated virus signature at least daily.	Inspected the antivirus software configurations to determine that antivirus software was configured to receive an updated virus signature at least daily.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC6.0	**Common Criteria Related to System Operations**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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 and availability.	An enterprise monitoring application is utilized to monitor the network and associated devices, services, environmental systems and attributes including, but not limited to the following: • Availability of the network, host services and ports • IP packet: transmissions and latency • Bandwidth utilization and performance	Inspected the NMIS configurations via Opsview to determined that an enterprise monitoring application was utilized to monitor the network and associated devices, services, environmental systems and attributes including, but not limited to the following: • Availability of the network, host services and ports • IP packet: transmissions and latency • Bandwidth utilization and performance	No exceptions noted.
		Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	Inspected the incident response plan to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident.	No exceptions noted.
		Antivirus software is installed on workstations, laptops, and servers supporting such software.	Inspected the remote administrator antivirus software configurations to determine that antivirus software was installed on workstations, laptops, and servers supporting such software.	No exceptions noted.
		Antivirus software is configured to receive an updated virus signature at least daily.	Inspected the antivirus software configurations to determine that antivirus software was configured to receive an updated virus signature at least daily.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC6.0	**Common Criteria Related to System Operations**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Antivirus software is configured to perform full system scans on a daily basis.	Inspected the antivirus scan configuration to determine that Antivirus software was configured to perform full system scans on a daily basis.	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.	Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	Inspected the incident response plan to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident.	No exceptions noted.
		The Ubersmith application is utilized to document and track incidents related to security and availability.	Inspected the Ubersmith ticketing system console to determine that the Ubersmith application was utilized to document and track incidents related to security and availability.	No exceptions noted.
		Resolution of events is communicated to both internal and external users within the corresponding ticket.	Inspected a sample of incident tickets to determine that resolution of events was communicated to both internal and external users within the corresponding ticket	No exceptions noted.
		Change management requests are opened for events that require permanent fixes.	Inspected a sample of incident tickets to determine that change management requests were opened for events that require permanent fixes.	No exceptions noted.
		Entity policies include probation, suspension, and termination as potential sanctions for employee misconduct.	Inspected the employee handbook to determine that entity policies included probation, suspension, and termination as potential sanctions for employee misconduct.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC7.0	**Common Criteria Related to Change Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.1	The entity's commitments and system requirements, as they relate to security and availability, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	Customer service requests are evaluated to determine the potential effect of the change on security and availability commitments and requirements throughout the change management process.	Inspected a sample of incident tickets to determine that customer service requests were evaluated to determine the potential effect of the change on security and availability commitments and requirements throughout the change management process.	No exceptions noted.
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security and availability.	Management has defined a formal risk management process that specifies the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the most recently completed risk assessment report to determine that management had defined a formal risk management process that specified the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
		A formal risk assessment is performed on an annual basis to identify threats that could impair systems security and availability commitments and requirements.	Inspected the most recently completed risk assessment report to determine that a formal risk assessment was performed on an annual basis to identify threats that could impair systems security and availability commitments and requirements.	No exceptions noted.
		Identified risks are rated using a risk evaluation process and ratings are reviewed by management.	Inspected the most recently completed risk assessment report to determine that identified risks were rated using a risk evaluation process and ratings were reviewed by management.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC7.0	**Common Criteria Related to Change Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the most recently completed risk assessment report to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
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.	Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inspected a sample of incident tickets to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security and availability commitments and system requirements.	System change requests are documented and tracked in a ticketing system.	Inquired of the Human Resource Director regarding the ticketing console and an example change ticket to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.
			Inspected the ticketing console and an example change ticket to determine that system change requests were documented and tracked in a ticketing system.	Testing of the control activity disclosed that no system change requests occurred during the review period.
		Incident tickets requiring system changes are documented to include original submission, last updated, status, and priority.	Inspected a sample of incident tickets to determine that incident tickets requiring system changes were documented to include original submission, last updated, status, and priority.	No exceptions noted.

A1.0	AVAILABILITY CRITERIA			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.	Enterprise monitoring software is utilized to notify personnel when predefined thresholds are exceeded on production systems.	Inspected the system monitoring software configurations and an example alert notification to determine that enterprise monitoring software was utilized to notify personnel when predefined thresholds were exceeded on production systems.	No exceptions noted.
		Hivelocity offers security monitoring of customers' critical systems on a 24/7/365 basis.	Inspected the staff schedule to determine that Hivelocity offered security monitoring of customers' critical systems on a 24/7/365 basis.	No exceptions noted.
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.	Environmental protections have been installed including the following: • HVAC • UPS • Generator backups in the event of power failure • Redundant communication lines • Smoke detectors • Fire extinguishers • Fire suppression system	Observed the environmental protection equipment at each data center to determine that environmental protections had been installed including the following: • HVAC • UPS • Generator backups in the event of power failure • Redundant communication lines • Smoke detectors • Fire extinguishers • Fire suppression system	No exceptions noted.
		Operations personnel monitor the status of environmental protections during each shift.	Inspected the staff schedule to determine that operations personnel monitored the status of environmental protections during each shift.	No exceptions noted.

A1.0	AVAILABILITY CRITERIA			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Environmental protections receive preventative maintenance on at least an annual basis.	Inspected the maintenance schedule and completed maintenance reports for the HVAC, UPS, generator and fire suppression systems to determine that environmental protections received preventative maintenance on at least annually.	No exceptions noted.
		Business continuity and disaster recovery plans have been developed and updated annually.	Inspected the business continuity plan and incident test results to determine that business continuity and disaster recovery plans, including restoration of backups, were tested annually.	No exceptions noted.
A1.3	Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.	Business continuity and disaster recovery plans, including restoration of backups, are tested annually.	Inspected the business continuity plan and incident test results to determine that business continuity and disaster recovery plans, including restoration of backups, were tested annually.	No exceptions noted.
		Test results are reviewed and the contingency plan is adjusted as necessary.	Inspected the business continuity plan and incident test results to determine that test results were reviewed and the contingency plan was adjusted as necessary.	No exceptions noted.