JNN GROUP

Report on Controls at a Service Organization Relevant to Security and Availability Trust Principles

DataCate Colocation and Cloud Cloud Services System

SOC 3

AS OF JUNE 30, 2018

UNRESTRICTED

Table of Contents

Section 1. Independent Service Auditors' Report

To the Management of Datacate, Inc. (Datacate):

SCOPE

We have examined the attached description titled "Datacate Inc.'s Colocation and Cloud Services System Description" for the period October 1, 2017 to June 30, 2018 (the description) and the suitability of the design and operating effectiveness of Datacate Inc.'s (Datacate) controls to meet the criteria for Security and Availability principles set forth in TSP section 100, Trust Services Principles, Criteria, and Illustrations (Trust Services Principles and Criteria), throughout the period October 1, 2017 to June 30, 2018.

The information in section 5 of management's description of the service organization's system, "HIPAA Security" provides a mapping of Datacate's controls to the HIPAA security rule and is presented by management of Datacate to provide additional information and is not a part of Datacate's description of its system made available to user entities as of June 30, 2018. The additional information has not been subjected to the procedures applied in the examination of the description of the system and of the suitability of the design of controls to meet the criteria for the security and availability principles, and, accordingly, we express no opinion on it.

DATACATE'S RESPONSIBILITIES

In the management assertion section of this report, Datacate has provided its assertion with respect to the Security and Availability principles of its system. Datacate Inc. 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.

SERVICE AUDITORS' RESPONSIBILITIES

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in Datacate's management assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable Trust Services Criteria. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). 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 October 1, 2017 to June 30, 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.

Our examination was not conducted for the purpose of evaluating Datacate's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program

INHERENT LIMITATIONS

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable Trust Services Criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of

the controls to meet the applicable Trust Services Criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

OPINION

In our opinion, Datacates' management assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security and availability.

1. The description fairly presents the Colocation and Cloud Services System that was designed and implemented throughout the period October 1, 2017 to June 30, 2018.
2. 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 October 1, 2017 to June 30, 2018, and user entities applied the complementary user-entity controls contemplated in the design of Datacate's controls throughout the period October 1, 2017 to June 30, 2018.
3. The controls tested, which together with the complementary user-entity controls referred to in the scope paragraph of this report, if operating effectively, which were those necessary to provide reasonable assurance that the applicable Trust Services Criteria were met, operated effectively throughout the period October 1, 2017 to June 30, 2018.

Jnn Group, Inc

JNN Group, Inc.
Pasadena, CA 91103
September 15, 2018

Section 2. Management Assertion

Datacate's Assertion on the Description of the Colocation and Cloud Services System

We have prepared the accompanying description of Datacate's Colocation and Cloud Services System included in Section 3 of this document and titled " Datacate, Inc.'s Colocation and Cloud Services " throughout the period October 1, 2017, to June 30, 2018, (description) based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) (description criteria). The description is intended to provide report users with information about the Colocation and Cloud Services System that may be useful when assessing the risks arising from interactions with Datacate's system, particularly information about system controls that Datacate has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, Privacy, (AICPA, Trust Services Criteria), and the criteria set forth in the CSA Cloud Controls Matrix (CCM) Version 3.0.1 control specifications.

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

a) The description fairly presents the Colocation and Cloud Services System as of September 1, 2018 (the "specified date"), 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:

a) Infrastructure. The physical and hardware components of a system (facilities, equipment, and networks)

b) Software. The programs and operating software of a system (systems, applications, and utilities)

c) People. The personnel involved in the operation and use of a system (developers, operators, users, and managers)

d) Procedures. The automated and manual procedures involved in the operation of a system

e) Data. The information used and supported by a system (transaction streams, files, databases, and tables)

(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 and 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) For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented

at carved-out subservice organizations to meet those criteria; and for privacy, the types of activities that the subservice organization would need to perform to comply with our privacy commitments

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

(10) 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.

(11) 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 the description were suitably designed as of the throughout the period to October 1, 2017, to June 30, 2018 to meet the applicable trust services criteria and the CCM criteria.

c) The controls stated in the description operated effectively throughout the period October 1, 2017, to June 30, 2018, to meet the applicable trust services criteria and the CCM criteria.

Datacate, Inc.
September 7, 2018

Section 3. Datacate, Inc.'s Colocation and Cloud Services

3.01 Overview of Operations

BACKGROUND

Datacate, Inc. (Datacate) provides cloud computing, managed hosting, colocation and related services to organizations worldwide. These services are primarily provided from the corporate office in Rancho Cordova, CA; and, Data Centers in Sacramento, CA, Ashburn, VA and other ancillary locations as may be offered by Datacate from time to time.

The scope of this report covers the Datacate Data Center physical and environmental availability and related security services where Datacate is responsible for the physical security in the Datacate facility and operations.

PRODUCTS AND SERVICES

This description addresses Datacate's colocation service, infrastructure-as-a service (IaaS), public, and private cloud offerings. Datacate provides the following services, all of which are covered by this report.

PRODUCTS AND SERVICES	DETAILS
Colocation Services • Cloud computing (sites and/or servers) • Redundant upstream networking • Redundant cooling and environmental controls • Redundant and conditioned power delivery • Physical security and access	Datacate grants their customers the right to operate customer owned equipment at the Colocation Space, as specified on the customer's order. Except as specifically provided, the customer expressly assumes all risk of loss to customer owned equipment in the Colocation Space.
Cloud Services • Virtual Server Hosting • Infrastructure planning and implementation • Disaster recovery solutions • Managed Intrusion Protection System (IPS) • Managed load balancing • Managed firewalling and Virtual Private Network (VPN)	Datacate provides the use of a Virtual Server to customer, for the exclusive use by the customer. Each customer represents and warrants that they have or have access to the knowledge and expertise necessary to configure, maintain, monitor, and secure the Virtual Server. Datacate further agrees to maintain the hardware on which the Virtual Server is located. Except with respect to the use or configuration of the management interface for the Virtual. Datacate does not provide phone or e-mail support or other technical assistance for the administration of the Virtual Server or otherwise related to the Services.

COMPONENTS OF THE SYSTEM

Infrastructure

Datacate's customer facing system infrastructure is supported by its owned/operated primary Tier III/IV data center in Rancho Cordova, CA, and two (2) secondary data centers (zones) located in Sacramento, CA, Ashburn, VA, and Santa Clara, CA managed by Raging Wire and Innap respectively.

Datacate utilizes an active data center with a fully replicated DR site. Datacate's primary data center is located in a Tier 3 data center in Rancho Cordova, CA. Datacate's DR site is located in Phoenix, AZ and contains a full copy of Datacate's customer facing services, which are replicated in real time.

The infrastructure supporting the achievement of the Security and Availability Principles and Criteria includes the security cameras, physical access control devices and the servers supporting the applications listed in the Software section below. The Data Center is also equipped with UPS, fire detection and suppression systems, water sensors, backup generators, and HVAC systems to protect against threats to environmental security / availability.

Network

Ethernet over IP tunneling (EoIP) is used as the protocol suite to secure data flows between facilities. Datacate customers can choose the zone for deployment of a particular resource during initial configuration, in which the creation of redundant and/or load-balanced systems is supported. Edge routers with integrated firewall capabilities are at each location to manage connections to and from the Internet. Spamhaus' Don't Route or Peer (DROP), Extended DROP (eDROP), and Botnet C&C lists are used to reject malicious traffic at Datacate's edge. Monitoring and detection are performed via syslog alerts and simple network management protocol (SNMP) traps. These tools are used as Datacate's Intrusion Detection and Prevention System (IDS/IPS).

Datacate cloud offerings include virtual architecture. Physical architecture is comprised primarily of HP hardware including blade arrays, standalone servers, and storage clusters. Microsoft Windows is deployed for servers, databases, workstations, and laptops. Linux OS (primarily Ubuntu or CentOS) deployed for applications that are better suited to Linux.

Software

Datacate provides cloud services using the hardware identified under the heading "Infrastructure," which supports a range of operating systems. These provide common or dedicated platforms for customer-based applications including status and support tools. In addition, for certain customers that have contracted with Datacate to perform these services, Datacate will also provide server backups, management of dedicated customer firewalls, and managed load-balancing.

Personnel

Datacate employs and directly manages staffing at its Rancho Cordova, CA location. Staffing requirements in other locations are met by the entity managing each location. Datacate employees provide 24/7 onsite security and management of the facility.

Datacate's Rancho Cordova, CA office houses and maintains all human resource functions, global policies, and technical capabilities for data collection, processing, and analysis. Teams are recruited and managed using Datacate's policies and procedures which are described in the following sections. Datacate is organized in the following functional areas:

FUNCTIONAL AREAS	RESPONSIBILITIES INCLUDE
Finance and Accounting	Oversight for all corporate financial processes.
Human Resources	Employee employment and benefits needs.
Network Operations	System support, network management, and access.
Sales and Marketing	The promotion of Datacate products and services.
Systems Development	Database/application development and support.

Policies and Procedures

Formal IT policies and procedures exist and are reviewed on an annual basis. All departments and teams are expected to adhere to Datacate policies and procedures that define how services should be delivered. Policies and procedures are located on the company's internal wiki and can be accessed by any Datacate team member with valid login credentials.

The fourteen (14) policies and procedures reviewed for 2018 which are used to safeguard Datacate systems include:

- Access Control Policy
- BCP & DRP Policy
- Change Management Policy
- Data Classification Policy
- Device & Media Handling Policy
- Employee Handbook
- Incident Response Policy
- Information Security Policy
- Physical & Environmental Policy
- Risk Assessment Policy
- Secure Communications & Data Transfer Policy
- Security Awareness & Training Policy
- Security Management Plan
- Suppliers & 3rd Party Providers

Data

Data, as defined for data center services, is information relevant to processing, operations, physical and environmental security / availability systems. Datacate has a data classification system to support least privileged or need-to-know to ensure that information is protected from unauthorized disclosure, use, modification, and deletion. Datacate platforms process and store the following data elements: User accounts (name, email), Hashes of passwords, network performance tests definitions, results and measurements, Alerts, Reports, and Support tickets.

3.02 Overview of Internal Controls

CONTROL ENVIRONMENT

Datacate's internal controls are a set of processes and procedures with oversight by subject matter experts (SME), and the senior leadership team to provide reasonable assurance that controls are designed and operating effectively to support the business and compliance needs.

Datacate is committed to designing and operating a system of internal control procedures that is appropriate to the needs of their business and to ensure data and information is securely processed and professionally managed. Management has established internal control policies and procedures according to the key control objectives and applicable Trust Services Criteria relevant to the services provided. It is management's responsibility to ensure the designed control procedures operate effectively on a continuous basis.

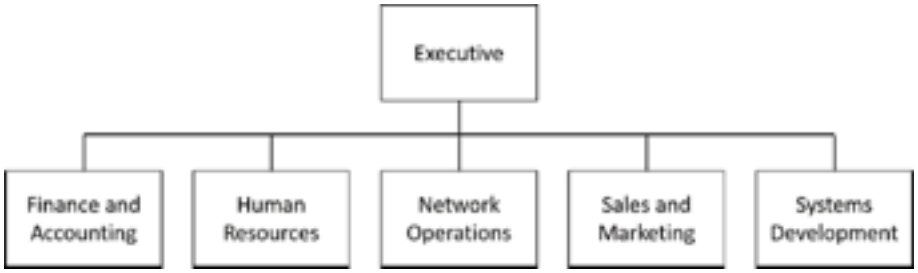
Datacate engaged JNN Group, Inc. (JNN Group) to examine the controls addressing the Trust Services Principles and Criteria for Security and Availability described in the attached report for the period of October 1, 2017 to June 30, 2018.

Management's Philosophy and Operating Style

Senior management has frequent interaction in both formal and informal settings, such as regularly scheduled management meetings. Meetings to address general management issues are held on a regular basis to facilitate communication and the decision-making process. Management places importance on controls and security in its processes, policies, procedures, and organizational structure. In designing its controls, Datacate has taken into consideration the relevance of controls to meet the trust criteria.

Organizational Structure

Reporting relationships are clearly established and posted on Datacate's internal wiki with regular updates. Data Center operations are under the direction of the chief information officer (CIO) of Datacate.



Assignment of Authority and Responsibility

Datacate has assigned responsibility and delegated authority to key management personnel to handle organizational goals and objectives, operating functions, and regulatory requirements.

HR Policies and Practices

Human Resource (HR) policies and practices are documented in Datacate's Employee Handbook. HR controls are designed to ensure that qualified and competent talent are recruited, developed, and retained to achieve Datacate's goals. Prospective employees complete an employment application and go through a formal interview and vetting process. Employment offers are contingent on passing both a reference and background check. Upon hire, new associates attend a "new associate orientation" where policies and procedures are introduced and reviewed in detail. Employees are provided a copy of the Associate Handbook and are required to sign an acknowledgement that they have received, reviewed, and understood the contents of the handbook. The Employee Handbook covers the following key items, in additional to role specific requirements.

Company Background	Anti-Discrimination	Harassment
Training	Workplace Commitments	Code of Professional Conduct
Company Property	Privacy	Document and File Control
Video Surveillance	Access	Employee Workplace Safety
Security	Digital Images	Disclosure
Investigation Procedures	Attendance Policies	Discipline Policies

Employees are reminded that infractions of rules of conduct may result in disciplinary action, up to and including termination of employment.

Risk Assessment Process

Datacate has practices in place to assist management in identifying, assessing, and managing risks that could affect the organization's ability to achieve its objectives. Risks also surround data stored and in transport. In addition, Datacate has addressed the risks of securing both Datacate and customer data. These practices are used to identify and measure the significant risks for the respective organization, initiate the identification and/or implementation of appropriate risk mitigation measures, and assist management in monitoring risk and remediation activities. The risk management practices implemented by Datacate management consist of internal controls derived from its policies, processes, personnel, and systems. Ongoing monitoring procedures are built into the normal recurring activities of Datacate and include regular management and supervisory activities. Managers of the various organizational units are regularly in touch with personnel and may question the accuracy of information that differs significantly from their knowledge of operations.

Information and Communication

Datacate strives to ensure that all employees understand their roles and responsibilities with respect to controls. Datacate's information security policy, employee handbook, security management policy, and incident response policies describe the requirements for all employees with respect to maintaining data security and reporting any policy violations. These policies are formally communicated to and acknowledged by all employees when they commence work. Datacate also holds regular awareness sessions and meetings to communicate and ensure that all employees are committed to the mission, vision, and core trust principals of Security and Availability. Regular meetings are also held with the entire organization to ensure critical workflow barriers are identified and that all teams understand priorities associated with critical customer project work in progress (WIP). Security awareness sessions are held on a regular basis to remind employees of their responsibilities and to address threats, vulnerabilities, risks and specific emerging security topics. Overall, effective communication occurs in a broader sense throughout Datacate. Management continually stresses the importance of control responsibilities to personnel.

Pertinent control information is critical to maintaining an effective internal control system. Information is identified, captured, and communicated in a form and timetable that enables personnel to carry out their responsibilities in an efficient and effective manner. Information systems produce reports containing operational, financial, and compliance related information that make it possible to monitor and perform control activities. Datacate not only uses internally generated data for detective and preventative monitoring, but also information about external events, activities, and conditions necessary for business decision making and external reporting.

Datacate uses various methods of communication to help ensure that associates and user entities are updated on current events and policies of Datacate. Datacate uses the intranet to share relevant information and updates internally.

CONTROL ACTIVITIES

Datacate control activities are performed to ensure that management directives are carried out to mitigate risks that could impact Datacate's objectives. Whether automated or manual, control activities, relate to internal compliance objectives. Control activities occur throughout Datacate at all levels and in all functions. Activities include approvals, authorizations, verifications, reconciliations, monitoring of operating performance, security of assets, and segregation of duties.

Specific control activities examined as part of this audit are provided in Section 3 - Information Provided by the Service Auditor. To eliminate any redundancy, they have not been listed in this section.

Management and Administration

Datacate has developed a risk-based security program, which is built to address their core tenets of:

1. Security to ensure that their systems and operations are protected against unauthorized physical and logical access;
2. Availability to ensure that data and information are continuously available.

To address these tenets, Datacate developed its risk-based security program in alignment with industry best practices.

Datacate is committed to providing a safe and secure working environment for its employees, vendors, and customers. Management strives to hire qualified individuals who are talented, customer focused, and ethical. Management is committed to completing a criminal background check on every new employee and offers of employment are contingent on candidates successfully passing their background check.

Due to the highly confidential nature of the data and information that runs through Datacate's operations, they have adopted policies and procedures to protect and maintain the integrity of data and information. Policies are designed to protect sensitive and confidential information in electronic and physical formats.

Effective security is a company-wide effort that requires the participation and support of all Datacate employees who deal with, or have access to, information and/or information systems. Regular system audits are performed to make sure access rights are appropriate and are still required as part of an employees' job responsibility.

Datacate maintains commercial general liability and errors and omissions insurance coverage appropriate to the nature of its business. Coverage is reviewed annually and adjusted as necessary.

Physical and Environmental

Physical security is in place to help ensure access is authorized to Datacate owned facilities and the assets located within. The buildings are secured by a proximity card access control system. Requests for physical access privileges to Datacate computer facilities require approval from authorized IT management personnel. Datacate visitors such as contractors, vendors, customers, and employees without access are required to go through a sign-in process at the Receptionist's desk. The visitor is issued a guest badge and must be escorted by an authorized individual throughout

the data center. All Datacate facilities have controlled access 24/7/365.

Physical access to the Rancho Cordova data center floor is controlled by a man trap double door entry system. The first entry door requires a proximity card for entry. The second door requires the first door is closed, and biometric (handprint) authentication along with a PIN code supplied at the time access is initially granted. Both the proximity card reader and biometric facilities log events including successful and unsuccessful biometric impressions, PIN codes, and proximity card swipes. Doors automatically lock upon multiple unsuccessful attempts at biometric and PIN identification. The man traps employ high-definition surveillance equipment on each side of each door as well as the biometric and proximity card readers.

Physical access to the Datacate Rancho Cordova Data Center administrative offices is controlled on a 24-hour basis via proximity card that is restricted to authorized personnel and monitored by surveillance cameras. The proximity card reader logs all events such as valid card swipes and invalid swipes. Entry into the parking lot of the facility is recorded by high- definition surveillance equipment with license plate detection and recording software.

Environmental controls include monitoring data center temperature, humidity, 24/7 air conditioning, backup power (UPS), smoke detectors, fire extinguishers, fire suppression, redundant communication lines, and all protections receive maintenance on at least an annual basis. Additional details are provided in the table on the following page.

ENVIRONMENTAL FEATURE	DETAILS
Electrostatic Discharge	The data center is equipped with raised floor panels that are electrostatic discharge (ESD) compliant. All metal surfaces are grounded to facilitate relieving build up charge. The data center computer room air conditioning (CRAC) units are equipped to provide a controlled level of humidity within the data center on a constant basis.
Temperature and Humidity Control	The Data Center floor has multiple independent and redundant CRAC (Computer Room Air Conditioner) units which incorporate real-time environmental controls and monitors. Each unit also contains and controls output humidity independently. Air flow at various points within each CRAC unit is monitored by temperature probes strategically placed throughout the facility to ensure that temperatures stay within prescribed values. If any measurement
Electrical Power	Power is provided to the facility by the local power utility (SMUD). The power feed to the facility data center is separate from the feed to the administrative offices and originates from a separate utility-owned transformer. Utility electrical feeds pass through an Automatic Transfer Switch (ATS) to main breaker panels where they are branched out to multiple independent Uninterruptible Power Supply (UPS) units. Each UPS unit contains one or more strings of batteries to supply
Fire Suppression	The data center is equipped with a dry pipe pre-action fire suppression system that incorporates an FM-200 chemical fire retardant for primary response. Monitors throughout the data center are designed to detect the presence of excessive heat, open flame, and smoke as indications of a fire condition. In the event that any two of these three factors are detected on two or more sensors, the following actions will result: (1) a 20 second warning alarm within the data center will sound and a warning strobe will flash; (2) a live monitoring panel connected to the fire suppression system will send a fire alarm notification to the 24/7 monitoring service, who will notify local authorities and fire departments; (3) the FM-200 dry chemical fire suppression agent will be discharged into the data center after the 20 second warning has elapsed; (4) the overhead conventional sprinkler system (Viking MOD H-1 4 inch Pre-Action Sprinkler Riser) will be pressurized by the utility water supply and will remain pressurized until the system is manually shut off and the pipes are drained, which will be done by authorized personal once it has been confirmed that the fire danger has been neutralized.

Perimeter Controls

The network configuration restricts access to authorized individuals only, through firewalls and demilitarized zones (DMZs). Firewalls are in place and configured to prevent unauthorized traffic from accessing the Datacate internal network. Only the firewall administrators have administrative access to the firewall management systems. Firewall systems are configured to trigger alerts on specific conditions and will send out email notices to various members of IT security and IT management for assessment and, if necessary, follow up actions. In addition, the firewall systems produce log files that can be reviewed by the IT security department for incidents.

Remote Access

For users that are authorized remote access, Datacate uses virtual private networking (VPN) software to restrict access. Users are authenticated by the VPN server to the Datacate network using their network login credentials of user ID and password. Datacate remote access VPN uses L2TP over IPSec.

Network Access

Access to Datacate network resources and Windows applications is accomplished through Active Directory. This applies to all users, associates, and contract personnel alike. Customers do not access the Datacate network.

All users authenticating to Active Directory managed network resources must use a valid user ID and password. Password strength is enforced through specific settings such as:

- Expiration setting
- Minimum length parameters
- Complexity settings (e.g., use of alpha, numeric, etc.)
- Disallowance of previous passwords and other common names or words

Hardware Security

Disposal of decommissioned customer data obtained via disks, tapes, or other portable media, includes degaussing, according to National Institute of Standards and Technology (NIST) specifications and physical destruction of media whenever appropriate.

Database Administration

The ability to make changes to the database software is restricted to authorized database administrators (DBAs) and production support personnel within IT. Passwords on installation/administration accounts delivered with the software are changed, and access to the accounts is restricted to approved database administrators.

Vulnerability Assessment

Datacate contracts with third party vendors to conduct periodic security reviews and vulnerability assessments. Results and recommendations are reported to senior IT management for review and follow up.

Incident Management

Datacate communicates the incident response policy to users and provides training to users of Datacate in scope information systems to contact their supervisor and the information security representative if they become aware of a possible security breach. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. Incidents are tracked through the tracking application, which includes the corrective actions implemented in accordance with the defined policies and procedures. Security training is performed annually and Datacate has a checklist for tracking activities.

Malicious Code and Intrusion Prevention

Anti-virus software is part of the standard build on Datacate Windows' servers and both Mac and Windows desktops/ laptops. Virus signature files are kept current with the latest vendor code release. Parent servers check for and download new definition files, and customer servers/workstations receive updates from the parent server.

Intrusion detection systems are in place and configured to detect and prevent unauthorized traffic into Datacate networking system. IPS tools are used to monitor inbound e mail traffic between the Internet and all customer facing systems. Datacate monitors for a wide variety of intrusion attempts such as worms, Trojans, brute force login attacks, reconnaissance scans and other fingerprinting techniques, protocol vulnerabilities, and denial of service attacks.

Logical Security

Datacate systems are safeguarded through user identification and authentications to help ensure only authorized users can perform actions or access information on a workstation or network as required by job function. Access requires a unique username and password. Customer access is restricted to only their data.

User Access

New user access requests or requests for changes in a user's access from Datacate internal users must be submitted and approved from an authorized manager. User access requests are provided to the access management team for provisioning of access. The ability to create or modify users and user access privileges is limited to authorized personnel. The tool to facilitate this process of access is Freshdesk. Freshdesk is an online cloud-based customer service software providing helpdesk support with smart automations.

Users are assigned a user role to restrict access to information resources based on the individual's role and responsibilities within the organization. Terminated user's access is removed and/or disabled upon the individual's departure from the organization. To assist in the validation of users' access and/or the removal of terminated associates, a periodic access review is performed by Datacate.

A designated customer representative from each customer provides the contact person to be granted to the Datacate onboarding team. Datacate customer service representative from the respective onboarding team creates the user and assigns the admin privileges. All other customer user accounts are created by the customer admin once the account has been established.

Change Management

The Change Management process adds oversight, visibility, and control of changes to the Datacate systems' environment. These changes may impact systems, applications, system software, hardware, network, or any other aspect of the information processing environment. Changes must follow a formal approval process prior to implementation.

Datacate maintains a formally documented change management process. Changes to hardware, operating systems, and system/application software are authorized, tested (when applicable), and approved prior to implementation. Changes to system infrastructure and system/application software are developed and tested in a separate development or test environment before being implemented into production. The ability to migrate changes into production environments is restricted to authorized IT personnel.

Emergency changes are documented and approved by the designated change manager.

MONITORING

Datacate monitoring controls include procedures to evaluate the completeness of associates' tasks and the quality of their performance. This monitoring is performed over a wide variety of functions at all levels of the organization. Datacate management also monitors its systems and facilities for unauthorized attempts to gain logical and physical access.

3.03 Complementary User Entity Controls

Datacate controls were designed with the assumption that certain internal controls would be in place at customer organizations. The application of such internal controls by customer organizations is necessary to achieve certain criteria identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for the processing of transactions for Datacate customers related to the information processed. Datacate does not have access to User Entity data.

For customers to rely on the information processed through Datacate applications, each customer is expected to evaluate its own internal controls to ensure appropriate control activities are in place. The following general procedures are controls to be considered. They should not be regarded as a comprehensive list of all controls that should be implemented by customer organizations:

- The User entity is responsible for performing periodic reviews of user access to ensure that access rights to Datacate systems are appropriate.
- The User entity is responsible for appropriately authorizing and notifying Datacate of new users.
- The User entity is responsible for protecting assigned user IDs and passwords within their organizations.
- The User entity is responsible for notifying Datacate of terminated users, requiring the deletion of their access to Datacate applications.
- The User entity is responsible for sending data to Datacate via a secure connection and/or the data should be encrypted.
- The User entities are responsible for notifying Datacate if they detect or suspect a security incident related to the Datacate colocation and cloud services.
- The User entity is responsible for reviewing email and other forms of communications related to changes that may affect the data center's availability, customers and users, and their security obligations.
- The User entity is responsible for identifying an alternate location in the event of a disaster to the Datacate Rancho Cordova Data Center.

3.04 Subservice Organizations

Datacate uses subservice organizations for data center hosting and management services in support of its production applications. Datacate periodically reviews the quality of the outsourced operations by various methods including:

- Review of subservice organizations' SOC 2 reports
- Regular meetings to discuss performance
- Nondisclosure agreements

NO.	SUBSERVICE ORGANIZATION	STATUS	LOCATIONS	SUBSERVICE CONTROLS	TRUST SERVICES CRITERIA REVIEWED
001	Telx	Inactive	N/A	N/A	N/A
002	INAP Corporation	Active	Santa Clara, CA	Disaster Recovery, Facilities Access/ Physical Access, Environmental Controls, and Hardware Security	CC5.0 & A1.0
003	Net Data Center (NDC)	Inactive	N/A	N/A	N/A
004	RagingWire	Active	Sacramento, CA	Disaster Recovery, Facilities Access/ Physical Access, Environmental Controls, and Hardware Security	CC5.0 & A1.0

001 - Telx:
Services were discontinued and replaced by INAP in January 2017.

002 – INAP Corporation:
INAP is a high-performance Internet infrastructure provider. The hybrid infrastructure delivers performance without compromise – blending virtual and bare-metal cloud, hosting, and colocation services across a global network of data centers, optimized from the application to the end user and backed by rock-solid customer support and a 100% uptime guarantee. Since 1996, the most innovative companies have relied on INAP to make their applications faster and more scalable. INAP operates in two business segments: Data Center and Network Services, which includes Colocation and IP services, and Hosting Services. Datacate reviews the INAP SOC 2 and Bridge Letter on a regular basis. The most current SOC 2 report focuses on the operational effectiveness of controls for data center services, which primarily include physical space for collocating customers' network and other equipment plus associated

services such as redundant power, environmental controls, and security. INAP uses a combination of facilities that are operated by INAP and by third parties, referred to as INAP data centers and non-core sites, respectively.

003 – Net Data Center (NDC):
Services were discontinued and replaced by RagingWire in January 2017.

001 - RagingWire:
RagingWire operates data centers in Sacramento, California, Ashburn, Virginia, and Garland, Texas. It delivers colocation services through enterprise data center facilities engineered to offer a 100% uptime service level agreement (SLA), even during maintenance windows.

Founded in Sacramento, California, in May 2000, RagingWire designs, builds, and operates data centers that deliver 100% availability and high-density power, providing custom and flexible colocation solutions that accommodate the business needs of large, data-intensive enterprise and web-centric companies. It operates reliable and secure 2N+2 enterprise data center facilities engineered to provide high availability, with scalable power and cooling. In 2012, RagingWire expanded its operations to the East coast, commissioning a data center campus located in Ashburn, Virginia. Then in 2017, RagingWire expanded its operations to the Southern region of the United States, commissioning a data center campus located in Garland, Texas.

In February 2014, NTT America, Inc. acquired an 80% ownership stake in RagingWire and the executive management team continues to operate the company under the RagingWire brand and maintain a minority interest in the company.

RagingWire has nearly 1,000,000 square feet of data center space, across six facilities that feature a. wholesale and retail data center space; b. Over 200 watts per square foot power density; c. Robust and diverse carrier neutral connectivity; d. 24 hours per day information technology (IT) and facility operations; e. Affiliated with the global data center portfolio of NTT Communications that includes 140 facilities under the Nexcenter brand.