System and Organization Control (SOC) 3 Report

For Security and Availability of Datacate's Colocation and Cloud Services System

For the Period of April 1, 2023 through March 31, 2024

holbrook &manter

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations™

Table of Contents

SECTION 1

SECTION 2

SECTION 3

Independent Service Auditor's Report

Independent Service Auditor's Report

To the Management of
Datacate, Inc.
2999 Gold Canal Drive
Rancho Cordova, CA 95670

Scope

We have examined Datacate's accompanying assertion titled "Assertion of Datacate's Colocation and Cloud Services System" (assertion) that the controls within Datacate's Colocation and Cloud Services System (system) were effective throughout the period April 1, 2023 to March 31, 2024, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to **Security and Availability** (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Datacate, to achieve Datacate's service commitments and system requirements based on the applicable trust services criteria. The description presents Datacate's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Datacate's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

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

Service Organization's Responsibilities

Datacate is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Datacate's service commitments and system requirements were achieved. Datacate has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, the Company is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services

criteria. Our examination was conducted 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 management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that controls were not effective to achieve the Company's service commitments and system requirements based on the applicable trust service criteria.
- performing procedures to obtain evidence about whether controls within the system were effective to achieve the Company's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within the Company's Colocation and Cloud Services System were effective throughout the period April 1, 2023 to March 31, 2024, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if the subservice organizations and user entities applied the complementary controls assumed in the design of Datacate's controls throughout that period.

Holbrook & Manter

Holbrook & Manter, CPAs
Columbus, Ohio
July 10, 2024

Datacate's Management Assertion

Datacate's Management Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Datacate's Colocation and Cloud Services System (system) through the period April 1, 2023, to March 31, 2024, to provide reasonable assurance that the Company's service commitments and system requirements relevant to **Security and Availability** were achieved. Our description of the boundaries of the system is presented in Section 3 and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2023 to March 31, 2024, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to **Security and Availability** (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria). The Company's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section 3.

Datacate uses subservice organizations to provide Colocation services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Datacate, to achieve Datacate's service commitments and system requirements based on the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Datacate's controls. The description does not disclose the actual controls of the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Datacate, to achieve Datacate's service commitments and system requirements based on the applicable trust services criteria. The description presents the service organization's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period April 1, 2023, to March 31, 2024, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Datacate's controls throughout the period.

The Management of Datacate
July 10, 2024

Description of Datacate's Colocation and Cloud Services System

Background

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

The scope of this report covers the Datacate Data Center's 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), and public and private cloud offerings. Datacate provides the following services, all of which are covered by this report. If a customer of Datacate's infrastructure-as-a-service public and private cloud offerings has not purchased certain services, the portions of the description that cover those services will not be relevant to those customers. For that reason, it is recommended that customers confirm the services they have purchased by contacting their Datacate account executive.

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 its 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.
Managed Hosting / 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 the customer for 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, Inc.'s client-facing system infrastructure is supported by its owned/operated primary Tier III/IV data center in Rancho Cordova, CA, and one secondary data center (zones) located in Santa Clara, CA, managed by Evocative, Inc. Ethernet over IP tunneling (EoIP) is used as the protocol suite to secure data flows between facilities. Datacate customers can choose the zone for the deployment of a particular resource during initial configuration, and the creation of redundant and/or load-balanced systems is supported.

Edge routers with integrated firewall capabilities are at each location and manage connections to and from the Internet. Spamhaus' DROP, eDROP, and Botnet C&C lists are used to reject malicious traffic at Datacate's edge. Monitoring and detection are employed via syslog alerts and SNMP traps. These tools are utilized as Datacate's Intrusion Detection/Prevention System (IPS).

Datacate, Inc servers include a combination of physical and virtual architecture. Physical architecture is comprised primarily of HP hardware including blade arrays, standalone servers, and storage clusters. Web facing services are primarily virtualized on the hypervisor platform best suited for their needs.

Datacate, Inc uses Microsoft Windows Server for servers, databases, workstations, and laptops, with Linux OSes (primarily Ubuntu or CentOS) being employed in 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 has approximately 12 associates staffing at its Rancho Cordova, CA location. Staffing requirements in other locations are met by the entity managing each location.

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 of 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 2023 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, and physical and environmental security/availability systems. Datacate has a data classification system to support the 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 test definitions, results and measurements, Alerts, Reports, and Support ticket

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.

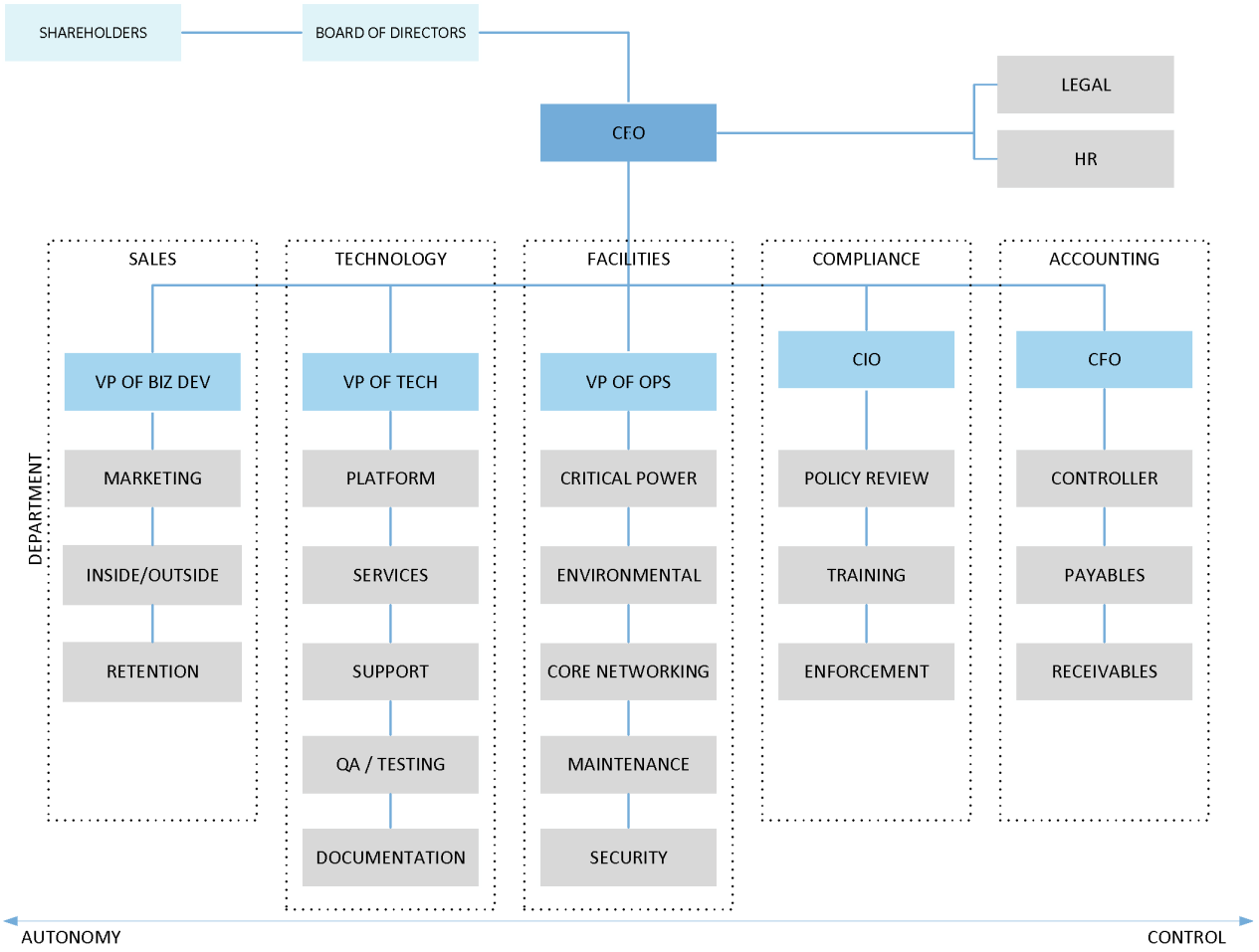
Datacate is committed to designing and operating a system of internal control procedures that is appropriate to the needs of their business and to ensure data and information are securely processed and professionally managed. Management has established internal control policies and procedures according 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.

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 technology officer (CTO) 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 acknowledgment that they have received, reviewed, and understood the contents of the handbook. The Employee Handbook covers the following key items in addition 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. Automated and manual control activities are in place to achieve 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.

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 employee's 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 to be 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 biometric and proximity card readers.

Physical access to the Datacate Rancho Cordova Data Center administrative offices is controlled on a 24-hour basis via a 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 that 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 exceeds a prescribed value, an alert is generated and emailed to facility management for response and mitigation, and the event is logged. The CRAC units are also individually monitored for the proper functioning of internal systems and components.

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 power during the time period of utility outage to generator supply. Each device in the chain is monitored by staff. Output power from the UPS units travels to various step-down transformers depending on the intended use and then to a series of breaker panels from which circuits are run to data center colocation space (customer spaces) as well as facility infrastructure services such as core networking, HVAC and security systems. In the event of a utility grid power interruption greater than 15 seconds, the prime-source diesel generator bank is started via the ATS and, within seconds, provides full power to the facility. The generator has several days' worth of fuel stored onsite and can be refueled via a standing contract with a local fuel supplier. Both full-load/no-load power tests are performed on a regular basis.
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 a 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 the 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 by 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 automation.

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. A periodic access review is performed by Datacate to assist in the validation of users' access and/or the removal of terminated associates.

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, networks, 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.

Complementary User Entity Controls

The Datacate control environment is designed with the assumption that certain internal controls will be implemented by User Organizations. The application of such internal controls by User Organizations is necessary to achieve certain control objectives 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.

Subservice Organizations

The Datacate control environment is designed with the assumption that certain internal controls will be implemented by Subservice Organizations. The application of such internal controls by these Subservice Organizations is necessary to meet certain criteria and control objectives identified in this report.

Datacate uses subservice providers to perform aspects of its Colocation and Cloud Services System. The description includes only the control objectives and related controls of Datacate and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by Datacate can be achieved only if complementary subservice organization controls assumed in the design of Datacate's controls are suitably designed and operating effectively at Datacate. The description does not extend to controls of the subservice organizations.

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
1	**Evocative (EVODC, LLC)**	**Active**	Santa Clara, CA	Disaster Recovery, Facilities Access/Physical Access, Environmental Controls, and Hardware Security	CC6.0 & A1.0

1 – Evocative Corporation:
Evocative provides services to clients based around data centers. The offerings start at the colocation level in which clients bring their own services and put them in the data centers, which leads to Infrastructure-as-a-Service (IaaS) services. Evocative also provides managed services, such as help desk services, managed backup and managed disaster recovery in their data center or on site for the client, and security offerings which include managed firewall services and intrusion detection system (IDS) observing and alerting. Evocative offers networking services to help connectivity in and out of the data center.

Complementary Subservice Provider Control Considerations

The Datacate control environment is designed with the assumption that certain internal controls will be implemented by in-scope Subservice Organizations. The application of such internal controls by these Subservice Organizations is necessary to meet certain criteria and control objectives identified in this report.

Datacate uses a subservice organization, Evocative to host portions of its infrastructure. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Datacate, to achieve Datacate's service commitments and system requirements based on the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Datacate's controls. The description does not disclose the actual controls of the subservice organizations.

Complementary Subservice Organization Controls	Dependent Criteria
Controls should be in place to ensure all risks have been adequately evaluated and measures are in place to address possible threats that could impair system security.	**CC3.0** – Risk Assessment
Controls should be in place to monitor subservice organization activities and controls on a regular basis.	**CC4.0** – Monitoring Activities
Controls should be in place to ensure facilities housing system components are adequately protected from unauthorized physical access.	**CC6.0** – Logical and Physical Access Controls
Controls should be in place to ensure facilities housing system components are adequately protected from environmental threats.	**CC6.0** – Logical and Physical Access Controls
Controls should be in place to ensure that information is protected during transmission, storage, and removal as agreed.	**CC6.0** – Logical and Physical Access Controls
Controls should be in place to identify, report, and remediate security incidents.	**CC7.0** – System Operations
Controls should be in place to communicate and coordinate changes with user entities to ensure system security is not compromised.	**CC8.0** – Change Management