



---

***System and Organization Control (SOC) 2 Type 2 Report  
Report on the Suitability of the Design and Operating Effectiveness  
of Controls of Datacate’s Colocation and Cloud Services System  
Relevant to Security and Availability  
For the Period of April 1, 2022 through March 31, 2023***

---

**holbrook  
&manter**



## Table of Contents

**Independent Service Auditor’s Report .....4**

### SECTION 2

**Datacate’s Management Assertion .....9**

### SECTION 3

**Description of Datacate’s Colocation and Cloud Services System .....11**

**Background ..... 12**

**Products and Services..... 12**

**Components of The System ..... 13**

Infrastructure ..... 13

Network..... 13

Software ..... 13

Personnel ..... 13

Policies and Procedures ..... 14

Data ..... 14

**Control Environment ..... 14**

Management’s Philosophy and Operating Style ..... 15

Organizational Structure ..... 15

Assignment of Authority and Responsibility ..... 16

HR Policies and Practices..... 16

Risk Assessment Process ..... 16

**Information and Communication..... 17**

**Control Activities ..... 17**

Management and Administration ..... 17

Physical and Environmental ..... 18

Perimeter Controls ..... 20

Remote Access ..... 20

Network Access ..... 20

Hardware Security ..... 20

Database Administration ..... 20

Vulnerability Assessment ..... 20

Incident Management ..... 20

Malicious Code and Intrusion Prevention ..... 21

Logical Security ..... 21

User Access ..... 21

Change Management ..... 21

**Monitoring ..... 22**

**Subsequent Changes to the System ..... 22**

**Addition to Management’s Description of the Service Organization’s System ..... 22**

**Complementary User Entity Controls ..... 23**

**Subservice Organizations ..... 24**

**Complementary Subservice Provider Control Considerations ..... 25**

**Objectives of the Review ..... 26**

**SECTION 4**

**Datacate’s Control Objectives and Related Controls and Independent Service Auditor’s Tests of Controls and Results of Tests ..... 27**

**SECTION 5**

**Datacate’s Control Objectives and Related Controls on the Cloud Security Alliance and HIPAA Security ..... 50**

Cloud Security Requirements Matrix ..... 51

HIPAA Security Standards ..... 43

*HIPAA Security Standards: Administrative Safeguards ..... 44*

*HIPAA Security Standards: Physical Safeguards ..... 54*

*HIPAA Security Standards: Technical Safeguards ..... 57*

# 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 description of its Colocation and Cloud Services System found in Section 3 titled "Datacate's Description of its Colocation and Cloud Services System throughout the period April 1, 2022, through March 31, 2023" (description) based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2<sup>®</sup> Report (AICPA, Description Criteria), and the suitability of the design of controls stated in the description throughout the period April 1, 2022, through March 31, 2023, to provide reasonable assurance that Datacate's service commitments and system requirements were achieved based on the trust services criteria relevant to **Security and Availability** (applicable trust services category) 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 disaster recovery, facilities access, and hardware security 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



**Audit, Assurance, & Technology Risk Specialists**  
Ohio offices in Columbus, Dublin, Lewis Center, Marion, & Marysville

Datacate's service commitments and system requirements were achieved. In Section 2, Datacate has provided the accompanying assertion titled Datacate's Management Assertion (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Datacate is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

### **Service Auditors' Responsibilities**

Our responsibility is to express an opinion on the description on the suitability of the design and operating effectiveness of controls stated in the description based on our examination. 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, in all material respects, the description is presented in accordance with the description criteria and the controls therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the controls involves—

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operating effectively.
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- evaluating the overall presentation of the description.

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



## **Inherent Limitations**

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 individual report users may consider important to meet their informational needs. There are inherent limitations in 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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating 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.

## **Description of Tests of Controls**

The specific controls we tested, and the nature, timing, and results of those tests are listed in Section 4, Description of Criteria, Controls, Tests, and Test Results of this report.

## **Other Matter**

The information in Section 5 titled "Datacate's Control Objectives and Related Controls on the Cloud Security Alliance (CSA) and HIPPA Security Standards", is presented by Datacate's management to describe the service organizations controls related to the cloud security alliance and HIPPA Security Standards. Information about Datacate's control objectives and controls related to CSA and the HIPPA Security Standards have not been subjected to the procedures applied in the examination and, accordingly, we express no opinion on it.

## **Opinion**

In our opinion, in all material respects,

- a. the description presents Datacate's Colocation and Cloud Services System that was designed and implemented throughout the period April 1, 2022, to March 31, 2023, in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that Datacate's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Datacate's controls throughout that period.
- c. The controls stated in the description operated effectively throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that Datacate's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organizations controls and complementary user entity controls assumed in the design of Datacate's controls operated effectively throughout that period.

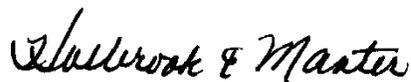


## Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Datacate; user entities of Datacate's Colocation and Cloud Services System during some or all of the period April 1, 2022 to March 31, 2023, business partners of Datacate subject to risks arising from interactions with the Datacate System, practitioners providing services to such user entities and business partners, prospect user entities and business partners, 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, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements 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.



Holbrook & Manter, CPAs  
Columbus, Ohio  
September 29, 2023



## Datacate's Management Assertion

## Datacate's Management Assertion

To: Holbrook & Manter, CPAs,

We have prepared the description of Datacate's Colocation and Cloud Services System titled "Datacate's Description of its Colocation and Cloud Services System" for the period of April 1, 2022, to March 31, 2023 (description) based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2<sup>®</sup> 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 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 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.

Datacate uses subservice organizations to provide disaster recovery, facilities access, and hardware security 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.

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

- 1) The description presents Datacate's Colocation and Cloud Services System that was designed and implemented throughout the period April 1, 2022, to March 31, 2023, in accordance with the description criteria.
- 2) The controls stated in the description were suitably designed throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that Datacate's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Datacate's controls throughout the period.
- 3) The controls stated in the description operated effectively throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that Datacate's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Datacate's controls operated effectively throughout that period.



Chris James  
CEO, Datacate  
September 29, 2023

## 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 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'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
<p><b>Colocation Services</b></p> <ul style="list-style-type: none"> <li>• Cloud computing (sites and/or servers)</li> <li>• Redundant upstream networking</li> <li>• Redundant cooling and environmental controls</li> <li>• Redundant and conditioned power delivery</li> <li>• Physical security and access</li> </ul>	<p>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.</p>
<p><b>Managed Hosting / Cloud Services</b></p> <ul style="list-style-type: none"> <li>• Virtual Server Hosting</li> <li>• Infrastructure planning and implementation</li> <li>• Disaster recovery solutions</li> <li>• Managed Intrusion Protection System (IPS)</li> <li>• Managed load balancing</li> <li>• Managed firewalling and Virtual Private Network (VPN)</li> </ul>	<p>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.</p>

## 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 INAP 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 the 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 a combination of physical and 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) is 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 has approximately 14 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 2022 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 & 3<sup>rd</sup> 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.

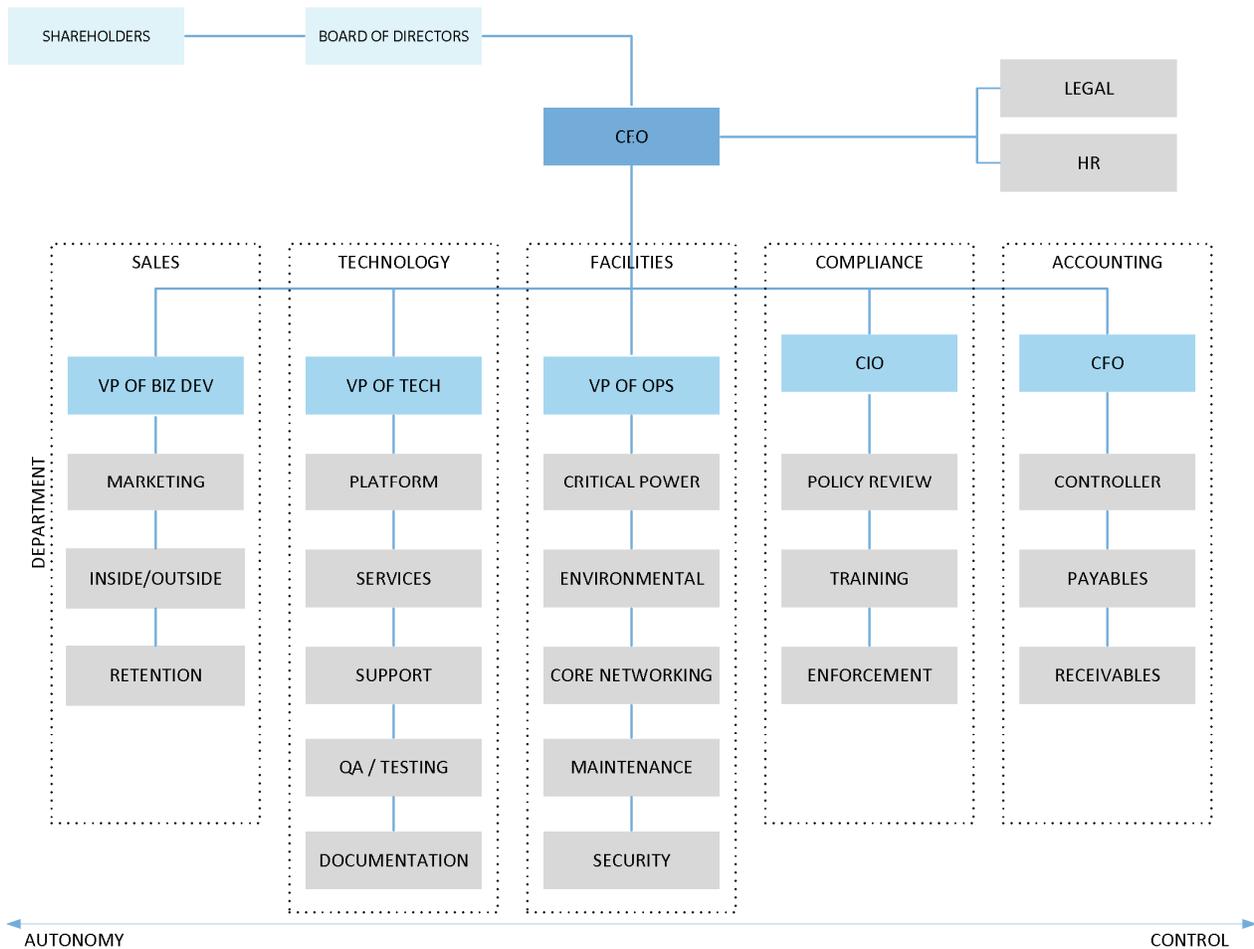
Datacate is committed to designing and operating a system of internal control procedures that is appropriate to the needs of their business and to ensure data and information are securely processed and professionally managed. Management has established internal control policies and procedures according 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
<b>Electrostatic Discharge</b>	<p>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.</p>
<b>Temperature and Humidity Control</b>	<p>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.</p>
<b>Electrical Power</b>	<p>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 on-site 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.</p>
<b>Fire Suppression</b>	<p>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.</p>

### *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. 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, 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.

### Subsequent Changes to the System

There were no substantive changes that are likely to affect report users' understanding of how Datacate provides services since March 31, 2023, through the date of this report.

### Addition to Management's Description of the Service Organization's System

The coronavirus (COVID-19) pandemic necessitated that Datacate (the service organization) transition part of its workforce to working remotely from home at times during the period. The service organization had well-established internal controls in place to support its remote workforce. These internal controls associated with Datacate's work-at-home program have been carefully considered to ensure that there are solid controls in place to manage the remote workforce. These previously established controls associated with our work-at-home activities positioned Datacate well for the pandemic, and we are unaware of any related control issues.

## 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	INAP Corporation	Active	Santa Clara, CA	Disaster Recovery, Facilities Access/Physical Access, Environmental Controls, and Hardware Security	CC6.0 & A1.0

### 1 – 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’ networks 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.

### 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, INTERNAP 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.	<b>CC3.0</b> – Risk Assessment
Controls should be in place to monitor subservice organization activities and controls on a regular basis.	<b>CC4.0</b> – Monitoring Activities
Controls should be in place to ensure facilities housing system components are adequately protected from unauthorized physical access.	<b>CC6.0</b> – Logical and Physical Access Controls
Controls should be in place to ensure facilities housing system components are adequately protected from environmental threats.	<b>CC6.0</b> – Logical and Physical Access Controls
Controls should be in place to ensure that information is protected during transmission, storage, and removal as agreed.	<b>CC6.0</b> – Logical and Physical Access Controls
Controls should be in place to identify, report, and remediate security incidents.	<b>CC7.0</b> – System Operations
Controls should be in place to communicate and coordinate changes with user entities to ensure system security is not compromised.	<b>CC8.0</b> – Change Management

## Objectives of the Review

This report is intended to provide interested parties with information sufficient to obtain an understanding of those aspects of Datacate's controls that may be relevant to user organizations' internal controls. This report, when coupled with an understanding of the internal controls in place at user organizations and subservice provider organizations, is intended to assist in the assessment of controls surrounding the operation of Datacate's Colocation and Cloud Services System.

Holbrook & Manter, CPAs review was restricted to selected services provided to user organizations by Datacate and, accordingly, did not extend to controls in effect at user locations or at any subservice organizations. The review was conducted in accordance with *AT-C sections 105, 205, and 320 Attest Engagements (AICPA Professional Standards)*. It is each interested party's responsibility to evaluate this information relative to controls in place at user locations in order to assess the total internal control structure. The user organization and Datacate controls must be evaluated together. If effective user organization controls are not in place, the Datacate controls may not compensate for such weaknesses.

Holbrook & Manter, CPAs review included inquiry of appropriate management, supervisory and staff personnel; inspection of documents and records; observation of activities and operations onsite; and verification that controls surrounding and provided by Datacate were implemented. Holbrook & Manter, CPAs test of controls covered the period from April 1, 2022, to March 31, 2023, and were applied to those controls relating to the control objectives specified by Datacate.

The description of the controls is the responsibility of Datacate's management. Holbrook & Manter, CPAs responsibility is to express an opinion that the controls were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the applicable control objectives were achieved during the period of this report, with the assumed subservice organization controls and if user entities applied the complementary controls assumed in the design of Datacate's controls.

## **Datacate's Control Objectives and Related Controls and Independent Service Auditor's Tests of Controls and Results of Tests**

Key	Control Activity	Testing Performed	Results of Tests
<b>CC1.0 - Control Environment</b>			
<b>CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.</b>			
<b>1.1.1</b>	Personnel are required to read and accept the code of conduct and the statement of confidentiality upon their hire.	Inquired of management to obtain an understanding of the organizational structure, reporting lines, authorities, and responsibilities.  Obtained and inspected a sample of signed code of conduct and confidentiality statements from new hires during the audit period.	No Exceptions Noted.
<b>1.1.2</b>	The Company performs background checks on all new potential employees.	Inspected a sample of new hires to verify background checks were performed.	No Exceptions Noted.
<b>1.1.3</b>	The Company performs performance evaluations and assessments on an annual basis for their employees.	Inspected a sample of employees from the audit period to determine whether the employee was properly evaluated for the specified job requirements.	No Exceptions Noted.
<b>CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.</b>			
<b>1.2.1</b>	Formal organizational structures and defined roles exist. The Company has a Board of Directors, which is independent from Management, and recorded minutes are documented.	Inspected a sample minutes from the Board of Director Minutes.	No Exceptions Noted.

Key	Control Activity	Testing Performed	Results of Tests
<b>CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.</b>			
1.3.1	The Company evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revises these when necessary to help meet changing commitments and requirements.	<p>Inquired of management to obtain an understanding of the organizational structure, reporting lines, authorities, and responsibilities.</p> <p>Inspected the organizational chart to determine whether the defined organizational structure, reporting lines, authorities, and responsibilities exist and are updated as needed.</p>	No Exceptions Noted.
<b>CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.</b>			
1.4.1	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.	<p>Inquired of management to obtain an understanding of the organizational structure, reporting lines, authorities, and responsibilities.</p> <p>Inspected a selection of new hires to determine whether roles and responsibilities are defined in written job descriptions.</p>	No Exceptions Noted.
1.4.2	The Company performs background checks on all new potential employees.	Inspected a selection of new hires from the audit period under review to determine whether the Company properly performed background checks.	No Exceptions Noted.

Key	Control Activity	Testing Performed	Results of Tests
<b>CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.</b>			
1.5.1	The Company evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revises these when necessary to help meet changing commitments and requirements.	<p>Inquired of management to obtain an understanding of the organizational structure, reporting lines, authorities, and responsibilities.</p> <p>Inspected the organizational chart to determine whether the defined organizational structure, reporting lines, authorities, and responsibilities exist and are updated as needed.</p>	No Exceptions Noted.
<b>CC2.0 - Communication and Information</b>			
<b>CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.</b>			
2.1.1	Datacate has dedicated security personnel responsible for promoting security awareness and training employees on Datacate security and privacy commitments. Training is conducted at least annually. Datacate has security policies that have been approved by management.	Inquired with Management to gain an understanding of how security awareness and employee training is conducted.	Exceptions Noted. Security awareness training procedures were completed during the audit period for security staff but not all employees.

Key	Control Activity	Testing Performed	Results of Tests
<b>CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.</b>			
<b>2.2.1</b>	Responsibility and accountability are defined through formal job descriptions. Employees are to receive a copy of their job description and are required to acknowledge that they have read the employee handbook that outlines their responsibilities.	Inspected a sample of new hires to determine whether roles and responsibilities are defined in written job descriptions and whether the sampled users acknowledged receipt of the employee handbook.	No Exceptions Noted.
<b>2.2.2</b>	The Company's security processes are communicated to both employees and customers.	Inquired of management to obtain an understanding of how security processes are communicated to internal and external system users.  Inspected the Employee Handbook and the Information Security Policy to verify security processes are described and communicated.  Inspected a sample of Master Service Agreements detailing the Company's security commitments.	No Exceptions Noted.
<b>2.2.3</b>	Policy and procedures for significant processes that address system requirements are available and communicated to all internal and external users.	Inquired of management to obtain an understanding of how security processes are communicated to internal and external system users.  Obtained and inspected a selection of policies and procedures to verify security is addressed and communicated.	No Exceptions Noted.
<b>2.2.4</b>	The Company's employees are required to sign and acknowledge their review of the information security policy during onboarding.	Inspected documentation for a sample of personnel and their acknowledgment and review of the information security policy.	No Exceptions Noted.

Key	Control Activity	Testing Performed	Results of Tests
2.2.5	The responsibilities of external users are communicated in the contract with each client.	Obtained and inspected a sample of client service agreements detailing the responsibilities of external users.	No Exceptions Noted.
2.2.6	The Company's security awareness program trains employees on how to identify and report possible security breaches.	Inquired of management to obtain an understanding of how security processes are communicated to internal and external system users.	Exceptions Noted. Security awareness training procedures were completed during the audit period for security staff but not all employees.
<b>CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.</b>			
2.3.1	Responsibility and accountability are defined through formal job descriptions. Employees are to receive a copy of their job description and are required to acknowledge that they have read the employee handbook that outlines their responsibilities.	<p>Inquired of management to obtain an understanding of how security processes are communicated to internal and external system users.</p> <p>Inspected a sample of new hires to determine whether roles and responsibilities are defined in written job descriptions and whether the sampled users acknowledged receipt of the employee handbook.</p>	No Exceptions Noted.

Key	Control Activity	Testing Performed	Results of Tests
2.3.2	<p>Datacate established a standard services agreement between its clients and Datacate that defines service levels, when applicable, and rules of use and additional terms for governing each Datacate service product.</p>	<p>Obtained and inspected a sample of client service agreements detailing the terms of engagement between the company and the client.</p> <p>Inquired of Management and confirmed system changes are planned, tracked in the ticketing system, and communicated to impacted users in a timely manner.</p>	<p>No Exceptions Noted.</p>
2.3.3	<p>The Company's security processes are communicated to both employees and customers.</p>	<p>Inquired of management to obtain an understanding of how security processes are communicated to internal and external system users.</p> <p>Inspected documentation for a sample of new hires and the related New Hire Acknowledgement Agreements from the audit period under review to determine whether they had signed and acknowledged their review of the Employee Handbook and the Information Security Policy at the time of orientation.</p> <p>Inspected a sample of Master Service Agreements detailing the Company's security commitments.</p>	<p>No Exceptions Noted.</p>

Key	Control Activity	Testing Performed	Results of Tests
2.3.4	The Company's security awareness program trains employees on how to identify and report possible security breaches.	Inquired of management to obtain an understanding of how security processes are communicated to internal and external system users.	Exceptions Noted. Security awareness training procedures were completed during the audit period for security staff but not all employees.
<b>CC3.0 - Risk Assessment</b>			
<b>CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.</b>			
3.1.1	A formal risk management process for evaluating risks based on identified threats and specified tolerances has been established.	Inspected the most recently completed risk assessment to determine that they entity defined a formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats.	No Exceptions Noted.
<b>CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.</b>			
3.2.1	The Company has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inquired of management to obtain an understanding of the risk management process.  Inspected the risk assessment documentation to determine whether it included specified procedures to address identified risks, that the risks were adequately analyzed for significance, and include mitigation strategies.	No Exceptions Noted.

Key	Control Activity	Testing Performed	Results of Tests
3.2.2	During the risk assessment and management process, management identifies changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and updates the potential threats to system objectives.	<p>Inquired of management to obtain an understanding of the risk management process.</p> <p>Inspected the risk assessment documentation to determine whether it included specified procedures to address identified risks, that the risks were adequately analyzed for significance, and include mitigation strategies.</p>	No Exceptions Noted.
<b>CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.</b>			
3.3.1	The Company has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	<p>Inquired of management to obtain an understanding of the risk management process.</p> <p>Inspected the risk assessment documentation to determine whether it included specified procedures to address identified risks, that the risks were adequately analyzed for significance, and include mitigation strategies.</p>	No Exceptions Noted.
3.3.2	During the risk assessment and management process, management identifies changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and updates the potential threats to system objectives.	<p>Inquired of management to obtain an understanding of the risk management process.</p> <p>Inspected the risk assessment documentation to determine whether it included specified procedures to address identified risks, that the risks were adequately analyzed for significance, and include mitigation strategies.</p>	No Exceptions Noted.

Key	Control Activity	Testing Performed	Results of Tests
<b>CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.</b>			
<b>3.4.1</b>	Change Management policies, including security code reviews, are in place, and procedures for tracking, testing, and approving are documented.	Inspected the Change Management policy and change log.	No Exceptions Noted.
<b>CC4.0 - Monitoring Activities</b>			
<b>CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.</b>			
<b>4.1.1</b>	The security committee has the responsibility to review and approve security policy. This committee provides additional leadership, guidance, and oversight of security programs and activities, including risk management and approval of the selection of baseline controls. An annual review and approval of the security policies is required.	Obtained and inspected documentation of the security committee meeting during the audit period and performed the annual review and approval of the information security policies.	No Exceptions Noted.
<b>CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.</b>			
<b>4.2.1</b>	The security committee has the responsibility to review and approve security policy. This committee provides additional leadership, guidance, and oversight of security programs and activities, including risk management and approval of the selection of baseline controls. An annual review and approval of the security policies is required.	Obtained and inspected documentation of the security committee meeting during the audit period and performed the annual review and approval of the information security policies.	No Exceptions Noted.

Key	Control Activity	Testing Performed	Results of Tests
<b>CC5.0 - Control Activities</b>			
<b>CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.</b>			
<b>5.1.1</b>	The Company has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	<p>Inquired of management to obtain an understanding of the risk management process.</p> <p>Inspected the annual risk assessment documentation to determine whether it included specified procedures to address identified risks, was adequately analyzed for significance, and included mitigation strategies.</p>	No Exceptions Noted.
<b>5.1.2</b>	The Company's policy and procedures are reviewed annually by upper-level management for consistency with the organization's risk mitigation strategy and updated as necessary for changes in the strategy.	Inspected the policy and procedure manuals to ascertain whether policies and procedures had been updated in the risk mitigation strategy and whether these policies and procedures had been formally approved by upper-level management.	No Exceptions Noted.
<b>CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.</b>			
<b>5.2.1</b>	The Company has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	<p>Inquired of management to obtain an understanding of the risk management process.</p> <p>Inspected the annual risk assessment documentation to determine whether it included specified procedures to address identified risks, was adequately analyzed for significance, and included mitigation strategies.</p>	No Exceptions Noted.

Key	Control Activity	Testing Performed	Results of Tests
5.2.2	The Company's policy and procedures are reviewed annually by upper-level management for consistency with the organization's risk mitigation strategy and updated as necessary for changes in the strategy.	Inspected the policy and procedure manuals to ascertain whether policies and procedures had been updated in the risk mitigation strategy and whether these policies and procedures had been formally approved by upper-level management.	No Exceptions Noted.
<b>CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.</b>			
5.3.1	The company has a complete body of policies and procedures that communicate expected behavior regarding internal control.	Inspected the policy and procedure manuals to ascertain whether policies and procedures had been updated in the risk mitigation strategy and whether these policies and procedures had been formally approved by upper-level management.	No Exceptions Noted.
<b>CC6.0 - Logical and Physical Access Controls</b>			
<b>CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.</b>			
6.1.1	Monitoring and alarming are configured by Datacate security teams to identify and notify management of incidents when thresholds are crossed on key security and operational metrics, including system performance, suspicious user activity, unauthorized changes to security protocols, and data center environmental stability. Issues, if any, are routed through incident management for resolution.	Inspected the performance monitoring software configurations and sample e-mail alerts to determine that monitoring software is configured appropriately.	No Exceptions Noted.

Key	Control Activity	Testing Performed	Results of Tests
6.1.2	Access to Datacate systems requires a unique ID and password.	Per inquiry with Management, confirmed that a unique ID and password is required to access systems. In addition, confirmed that user IDs are not shared.  Inspected the Group policy to verify that user id and password requirements are enabled.	No Exceptions Noted.
6.1.3	Administrator access to the Datacate system is restricted to authorized personnel and authenticated through secured Kerberos protocol authentication with LDAP authorization management.	Obtained and inspected administrator configuration noting appropriate authentication procedures enabled.	No Exceptions Noted.
6.1.4	<p>Password standards for all Datacate systems are documented and systematically enforced as follows:</p> <ul style="list-style-type: none"> <li>• Maximum password age - 90 days</li> <li>• Minimum password age - 0 days</li> <li>• Minimum length - 8 characters</li> <li>• Complexity–enabled</li> <li>• Store passwords w/reversible encryptions – Yes</li> <li>• History – 5</li> <li>• Invalid logon attempts - 5</li> </ul>	Inspected the Group Policy password configurations for the review period to confirm all settings.	Exception Noted. Password complexity requirements were set to disabled. All other password parameters are met.
<p><b>CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.</b></p>			
6.2.1	Upon termination during the exit interview process, access to Datacate systems and tools, including corporate email, is removed.	Inquired of Management regarding termination procedures.  Inspected termination checklist for a sample of terminated personnel during the audit period.	No Exceptions Noted.

Key	Control Activity	Testing Performed	Results of Tests
6.2.2	Datacate applications match each user ID to a single end-user account. Access to end-user system records is based on a customer-approved request for access.	<p>Per inquiry with Management, confirmed that a unique ID and password are required to access systems. In addition, confirmed that user IDs are not shared.</p> <p>Inspected the Group policy to verify that user ID and password requirements are enabled.</p>	No Exceptions Noted.
<p><b>CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.</b></p>			
6.3.1	The ability to create or modify users and user access privileges is limited to authorized personnel. User access privileges are reviewed at least annually to verify which permissions are currently active for each user and to remove any access that is no longer required.	<p>Inquired of Management to obtain an understanding of the logical and physical access control processes in place.</p> <p>Inspected documentation from the annual user access review.</p> <p>Inspected a selection of employees from the audit period under review to determine whether access rights were properly approved by management and appropriate based on job function.</p>	No Exceptions Noted.

Key	Control Activity	Testing Performed	Results of Tests
6.3.2	User access is limited by profiles and roles assigned to users based on their job function (role-based security).	<p>Inquired of Management to obtain an understanding of the logical and physical access control processes in place.</p> <p>Inspected documentation from the annual user access review.</p> <p>Inspected a selection of employees from the audit period under review to determine whether access rights were properly approved by management and appropriate based on job function.</p>	No Exceptions Noted.
<p><b>CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.</b></p>			
6.4.1	<p>Physical access to the data center is authorized by the customer point of contact (POC). Access cards are provisioned by Datacate personnel based on authorized requests from the customer point of contact (POC).</p> <p>Physical access reviews are performed annually. The review includes active Datacate employees. Upon customer request, Datacate will provide a data center electronic access usage report.</p>	<p>Obtained and inspected the physical access review completed by management during the audit period.</p> <p>Obtained and inspected physical access RFID event logs throughout the audit period.</p>	No Exceptions Noted.

Key	Control Activity	Testing Performed	Results of Tests
6.4.2	<p>Physical security measures in place include:</p> <ol style="list-style-type: none"> <li>1) Data center entrances have a perimeter security system consisting of badge readers or a biometric access system.</li> <li>2) Data center utilizes a badge reader or biometric access to raised floor spaces and locks/keys to restrict access to facility rooms within the building.</li> <li>3) Visitors to the data center facilities must gain appropriate approval, sign in at the front, and remain with an escort during the duration of their visit.</li> <li>4) All staff members are required to badge in to gain access to the facility.</li> <li>5) All cages, suites, and private rooms are secured using lock/key, badge access control, or biometric access controls.</li> <li>6) Key sign-out sheet and/or log of badge reader activity exist and cover access to Datacate spaces.</li> </ol>	<p>Obtained and inspected office sign-in sheets for visitors throughout the audit period.</p> <p>Obtained and inspected the SOC 2 Datacenter Reports and noted all physical security measures were addressed.</p>	<p>No Exceptions Noted.</p>
<p><b>CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.</b></p>			
6.5.1	<p>Management annually obtains and inspects SOC reports from subservice providers who provide physical access controls.</p>	<p>Obtained SOC reports from Subservice Providers and verified that Management completed the review of the reports during the period.</p>	<p>No Exceptions Noted.</p>

Key	Control Activity	Testing Performed	Results of Tests
<b>CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.</b>			
<b>6.6.1</b>	Monitoring and alarming are configured by Datacate security teams to identify and notify management of incidents when thresholds are crossed on key security and operational metrics, including system performance, suspicious user activity, unauthorized changes to security protocols, and data center environmental stability. Issues, if any, are routed through incident management for resolution.	Obtained and inspected monitoring and alerting configurations noting appropriate monitoring and alerting criteria enabled when key security and operational thresholds are crossed.	No Exceptions Noted.
<b>6.6.2</b>	Firewall devices are configured to restrict access to the computing environment and enforce the boundaries of computing clusters.	Inspected the firewall configuration and discussed access restrictions with Management.	No Exceptions Noted.
<b>CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.</b>			
<b>6.7.1</b>	Monitoring and alarming are configured by Datacate security teams to identify and notify management of incidents when thresholds are crossed on key security and operational metrics, including system performance, suspicious user activity, unauthorized changes to security protocols, and data center environmental stability. Issues, if any, are routed through incident management for resolution.	Obtained and inspected monitoring and alerting configurations noting appropriate monitoring and alerting criteria enabled when key security and operational thresholds are crossed.	No Exceptions Noted.

Key	Control Activity	Testing Performed	Results of Tests
<b>CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.</b>			
6.8.1	Administrator access to the Datacate system is restricted to authorized personnel and authenticated through secured Kerberos protocol authentication with LDAP authorization management.	Obtained and inspected administrator configuration noting appropriate authentication procedures enabled.	No Exceptions Noted.
6.8.2	Antivirus software is installed on workstations, laptops, and servers.	Inspected the antivirus population comprised of workstations, laptops, and servers.	No Exceptions Noted.
<b>CC7.0 - System Operations</b>			
<b>CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.</b>			
7.1.1	Monitoring and alarming are configured by Datacate security teams to identify and notify management of incidents when thresholds are crossed on key security and operational metrics, including system performance, suspicious user activity, unauthorized changes to security protocols, and data center environmental stability. Issues, if any, are routed through incident management for resolution.	Obtained and inspected monitoring and alerting configurations noting appropriate monitoring and alerting criteria enabled when key security and operational thresholds are crossed.	No Exceptions Noted.
7.1.2	Datacate performs and/or contracts with 3rd parties to perform vulnerability and penetration testing at least annually.	Inspected the most recent vulnerability and penetration testing results.  Inspected the on-call support procedure, incident handling and response procedures and security logs to determine that the management followed defined for resolving and escalating reported events.	No Exceptions Noted.

Key	Control Activity	Testing Performed	Results of Tests
<p><b>CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.</b></p>			
<p><b>7.2.1</b></p>	<p>A formal risk management process for evaluating risks based on identified threats and specified tolerances has been established.</p>	<p>Inspected the specific components of the risk assessment process that are performed during routine management meetings.</p> <p>Observed results and action items are communicated to the respective owners and tracked through Datacate's internal risk management tool.</p>	<p>No Exceptions Noted.</p>
<p><b>CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.</b></p>			
<p><b>7.3.1</b></p>	<p>Policy and procedures for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints (and the process for doing so) are made available to internal and external users.</p>	<p>Inspected the full population of the Datacate policies and procedures to confirm that the documents were readily available.</p> <p>Inquired regarding the communication of incidents to customers to determine that internal and external users were informed via email of incidents in a timely manner and advised of corrective measures to be taken on their part.</p>	<p>No Exceptions Noted.</p>

Key	Control Activity	Testing Performed	Results of Tests
<b>CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.</b>			
<b>7.4.1</b>	Policy and procedures for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints (and the process for doing so) are made available to internal and external users.	<p>Obtained and inspected the policies and procedures comprising the information security and general operations processes.</p> <p>Observed the availability of resources to internal and external users.</p>	No Exceptions Noted.
<b>CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.</b>			
<b>7.5.1</b>	Operations personnel follow defined protocols for resolving and escalating reported events. Incidents are logged within a ticketing system, assigned a severity rating, and tracked to resolution.	<p>Inspected the incident response policy.</p> <p>Inspected the ticketing system and a sample of incident tickets from the audit period.</p> <p>Inspected examples of email broadcasts and communications to determine that internal and external users were informed of incidents via email in a timely manner and advised of corrective measure to be taken on their part.</p>	No Exceptions Noted.
<b>CC8.0 - Change Management</b>			
<b>CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.</b>			
<b>8.1.1</b>	Change Management policies, including security code reviews, are in place, and procedures for tracking, testing, and approving are documented.	Inspected the Change Management policy and change log.	No Exceptions Noted.

Key	Control Activity	Testing Performed	Results of Tests
<b>CC9.0 - Risk Mitigation</b>			
<b>CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.</b>			
<b>9.1.1</b>	The company maintains a comprehensive Disaster Recovery/Business Continuity plan that is reviewed annually.	Obtained and inspected the Business Continuity Plan and the Disaster Recovery Plan Policies.	No Exceptions Noted.
<b>CC9.2 - The entity assesses and manages risks associated with vendors and business partners.</b>			
<b>9.2.1</b>	Related party and vendor systems are subject to review as part of the vendor risk management process. Attestation reports (SOC 2 reports) are evaluated when available.	Obtained SOC reports from Subservice Providers and verified that Management completed review of the reports during the period.  Obtained and inspected the Suppliers and 3rd Party Vendors Policy.	No Exceptions Noted.
<b>A1.0 - Additional Criteria for Availability</b>			
<b>A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.</b>			
<b>A1.1.1</b>	Monitoring and alarming are configured by Datacate security teams to identify and notify management of incidents when thresholds are crossed on key security and operational metrics, including system performance, suspicious user activity, unauthorized changes to security protocols, and data center environmental stability. Issues, if any, are routed through incident management for resolution.	Obtained and inspected monitoring and alerting configurations noting appropriate monitoring and alerting criteria enabled when key security and operational thresholds are crossed.	No Exceptions Noted.

Key	Control Activity	Testing Performed	Results of Tests
<b>A1.1.2</b>	Environmental protections have been installed, including the following: cooling systems, battery and diesel generator backup in the event of power failure, redundant communications lines, smoke detectors, and dry pipe sprinklers.	Observed environmental protection systems during facility walkthrough.  Obtained environmental protections reports (fire suppression, etc.).	No Exceptions Noted.
<b>A1.1.3</b>	Environmental and building protections receive maintenance on at least an annual basis.	Obtained and inspected documentation of maintenance procedures completed throughout the audit period.	No Exceptions Noted.
<b>A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.</b>			
<b>A1.2.1</b>	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. Fire detection equipment is in place and includes fire/smoke detectors and fire extinguishers.	Inquired of Management to confirm the existence of the fire detection and suppression system.  Obtained and inspected maintenance reports on the fire suppression system.	No Exceptions Noted.
<b>A1.2.2</b>	A Disaster Recovery Plan/Policy exists and is reviewed and assessed annually for ongoing effectiveness and to identify opportunities for improvement.	Obtained and inspected the Business Continuity Plan and the Disaster Recovery Plan Policies noting proof of annual review by Management.	No Exceptions Noted.
<b>A1.2.3</b>	Datacate uses a multi-location strategy for its facilities to permit the resumption of operations at other entity facilities in the event of loss of a facility.	Obtained SOC reports from Subservice Providers and verified that Management completed review of the reports during the period.	No Exceptions Noted.

Key	Control Activity	Testing Performed	Results of Tests
A1.2.4	Datacate utilizes an active data center with a fully replicated DR site. Backups are monitored for failure using an automated system, and the incident management process is automatically invoked.	<p>Inspected SOC 2 evidential reports for the datacenter.</p> <p>Made inquiries of appropriate personnel to corroborate strategy.</p> <p>Observed data center backup and replication system configurations during process walkthroughs.</p>	No Exceptions Noted.
<b>A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.</b>			
A1.3.1	A Disaster Recovery Plan/Policy exists and is reviewed and assessed annually for ongoing effectiveness and to identify opportunities for improvement.	Obtained and inspected the Business Continuity Plan and the Disaster Recovery Plan Policies noting proof of annual review by Management.	No Exceptions Noted.
A1.3.2	The Disaster Recovery Plan is tested periodically to ensure data/system restore capability.	Obtained and inspected documentation of periodic recovery testing completed during the audit period.	No Exceptions Noted.
A1.3.3	Datacate utilizes an active data center with a fully replicated DR site. Backups are monitored for failure using an automated system, and the incident management process is automatically invoked.	<p>Inspected SOC 2 evidential reports for the datacenter.</p> <p>Made inquiries of appropriate personnel to corroborate strategy.</p> <p>Observed data center backup and replication system configurations during process walkthroughs.</p>	No Exceptions Noted.

## **Datacate's Control Objectives and Related Controls on the Cloud Security Alliance and HIPPA Security**

### Cloud Security Requirements Matrix

Datacate is an IaaS or Infrastructure-as-a-service provider. Key Cloud Security Requirement Controls for IaaS are being provided for reference with mapping to Cloud Security Alliance (CSA) guidelines. This mapping is limited to a self-assessment of the applicable Trust Service Principles of Security and Availability.

Domain & Cloud Control ID		Specification	Physical	Network	Storage	TSP	2017 Trust Service Criteria
Data center Security Asset Management	DCS-01	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly and assigned ownership by defined roles and responsibilities.	X			Security & Availability	<p><b>CC3.2</b> COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.</p> <p><b>CC6.1</b> The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.</p> <p><b>A1.1</b> The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.</p>
Data center Security Controlled Access Points	DCS-02	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	X			Availability	<p><b>CC6.1</b> The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.</p> <p><b>CC6.4</b> The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.</p> <p><b>CC7.2</b> The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.</p>

Domain & Cloud Control ID		Specification	Physical	Network	Storage	TSP	2017 Trust Service Criteria
Data center Security Equipment Identification	DCS-03	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	X	X	X	Security	<p><b>CC6.1</b> The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.</p>
Data center Security Off-Site Authorization	DCS-04	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premise.	X		X	Security	<p><b>CC6.1</b> The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.</p> <p><b>CC6.4</b> The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.</p>
Data center Security Off-Site Equipment	DCS-05	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premises. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full overwrite of the drive to ensure that the erased drive is released to inventory for reuse and deployment, or securely stored until it can be destroyed.	X	X	X	Security	<p><b>CC3.3</b> COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.</p> <p><b>CC6.5</b> The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.</p>

Domain & Cloud Control ID		Specification	Physical	Network	Storage	TSP	2017 Trust Service Criteria
Data center Security Policy	DCS-06	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	X			Security & Availability	<p><b>CC6.4</b> The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.</p> <p><b>CC7.2</b> The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.</p> <p><b>A1.2</b> The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.</p>

Domain & Cloud Control ID		Specification	Physical	Network	Storage	TSP	2017 Trust Service Criteria
Data center Security Secure Area Authorization	DCS-07	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	X	X	X	Security & Availability	<p><b>CC6.1</b> The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.</p> <p><b>CC6.4</b> The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.</p> <p><b>CC7.2</b> The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.</p> <p><b>A1.2</b> The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.</p>

Domain & Cloud Control ID		Specification	Physical	Network	Storage	TSP	2017 Trust Service Criteria
Data center Security Unauthorized Persons Entry	DCS-08	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	X	X	X	Availability	<p><b>CC6.1</b> The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.</p> <p><b>CC6.4</b> The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.</p> <p><b>CC7.2</b> The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.</p> <p><b>A1.2</b> The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.</p>

Domain & Cloud Control ID		Specification	Physical	Network	Storage	TSP	2017 Trust Service Criteria
Data center Security User Access	DCS-09	Physical access to information assets and functions by users and support personnel shall be restricted.	X			Security	<p><b>CC6.1</b> The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.</p> <p><b>CC6.3</b> The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.</p> <p><b>CC6.4</b> The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.</p>

Domain & Cloud Control ID		Specification	Physical	Network	Storage	TSP	2017 Trust Service Criteria
Infrastructure & Virtualization Security Audit Logging / Intrusion Detection	IVS-01	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	X	X	X	Security	<p><b>CC6.1</b> The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.</p> <p><b>CC7.2</b> The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.</p> <p><b>CC7.3</b> The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.</p> <p><b>CC7.4</b> The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.</p>
Infrastructure & Virtualization Security Clock Synchronization	IVS-03	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.		X		Security	<p><b>CC7.4</b> The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.</p>
Infrastructure & Virtualization Security Information System Documentation	IVS-04	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.		X	X	Availability	<p><b>A1.1</b> The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.</p>

Domain & Cloud Control ID		Specification	Physical	Network	Storage	TSP	2017 Trust Service Criteria
Infrastructure & Virtualization Security SecurityNetwork Security	IVS-06	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually and supported by a documented justification for use for all allowed services, protocols, ports, and by compensating controls.	X	X	X	Security	<p><b>CC6.1</b> The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.</p> <p><b>CC6.6</b> The entity implements logical access security measures to protect against threats from sources outside its system boundaries.</p> <p><b>CC6.7</b> The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.</p> <p><b>CC6.8</b> The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.</p> <p><b>CC7.1</b> To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.</p> <p><b>CC8.1</b> The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.</p>

Domain & Cloud Control ID		Specification	Physical	Network	Storage	TSP	2017 Trust Service Criteria
Infrastructure & Virtualization Security Production / Non-Production Environments	IVS-08	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	X	X	X	Security	<p><b>CC5.1</b> COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.</p> <p><b>CC5.2</b> COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.</p> <p><b>CC6.1</b> The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.</p> <p><b>CC6.6</b> The entity implements logical access security measures to protect against threats from sources outside its system boundaries.</p> <p><b>CC8.1</b> The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.</p>

Domain & Cloud Control ID		Specification	Physical	Network	Storage	TSP	2017 Trust Service Criteria
Infrastructure & Virtualization Security Segmentation	IVS-09	<p>Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.</p> <p>Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations:</p> <ul style="list-style-type: none"> <li>• Established policies and procedures</li> <li>• Isolation of business critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance</li> <li>• Compliance with legal, statutory, and regulatory compliance obligations [PCI, HIPAA, etc...]</li> </ul>	X	X	X	Security	<p><b>CC6.6</b> The entity implements logical access security measures to protect against threats from sources outside its system boundaries.</p>

Domain & Cloud Control ID		Specification	Physical	Network	Storage	TSP	2017 Trust Service Criteria
Infrastructure & Virtualization Security Wireless Security	IVS-12	<p>Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following:</p> <ul style="list-style-type: none"> <li>• Perimeter firewalls implemented and configured to restrict unauthorized traffic</li> <li>• Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings)</li> <li>• User access to wireless network devices restricted to authorized personnel</li> <li>• The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network</li> </ul>	X	X	X	Security	<p><b>CC6.1</b> The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.</p> <p><b>CC6.3</b> The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.</p> <p><b>CC6.6</b> The entity implements logical access security measures to protect against threats from sources outside its system boundaries.</p> <p><b>CC6.7</b> The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.</p> <p><b>CC7.1</b> To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.</p> <p><b>CC7.2</b> The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.</p>



## HIPAA Security Standards

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information (ePHI) that is created, received, used, or maintained by a covered entity. Datacate has determined that it may operate as the Business Associate of its customers' covered entity health plans for our applicable services and has taken significant steps to help customers comply with the HIPAA. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of (ePHI). Consistent with requirements, Datacate provides appropriate and reasonable security measures and practices designed to safeguard protected health information. The tables include a mapping of the HIPAA Security Standards to the SOC 2 controls included in this SOC 2 examination. The mapping serves as a crosswalk between the two frameworks and is not intended as a HIPAA Security controls audit.

*HIPAA Security Standards: Administrative Safeguards*

Section	Criteria	Safeguard Description	Datacate Control Activity
164.308(a)(1)(i) Security Mgmt. Process	<b>CC1.0</b>	Implement policies and procedures to prevent, detect, contain, and correct security violations.	Datacate has dedicated security personnel responsible for promoting security awareness and training employees on Datacate security, privacy commitments and HIPAA requirements. Training is conducted at least annually. Datacate has security policies that have been approved by management and published on the intranet which is accessible to all employees.
164.308(a)(1)(ii)(A) Risk Analysis (_R_)	<b>CC3.0</b>	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by the covered entity or business associate.	A formal risk management process for evaluating risks based on identified threats and specified tolerances have been established. Specific components of the risk assessment process are performed during routine management meetings to address the following: 1. Evaluation of the Datacate organizational structure, capability, capacity, reporting lines, authorities, and responsibilities. 2. Identification and evaluation of environmental, regulatory, and technological changes that have occurred. 3. Evaluation of the need for additional tools and resources in order to achieve business objectives. 4. Evaluation of threats and vulnerabilities of achieving commitments to customers. 5. Results and action items are communicated to the respective owners and tracked through Datacate's internal risk management tool.

Section	Criteria	Safeguard Description	Datacate Control Activity
<p>164.308(a)(1)(ii)(B) Risk Mgmt. (_R_)</p>	<p><b>CC3.0</b></p>	<p>Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).</p>	<p>A formal risk management process for evaluating risks based on identified threats and specified tolerances have been established. Specific components of the risk assessment process are performed during routine management meetings to address the following: 1. Evaluation of the Datacate organizational structure, capability, capacity, reporting lines, authorities, and responsibilities. 2. Identification and evaluation of environmental, regulatory, and technological changes that have occurred. 3. Evaluation of the need for additional tools and resources in order to achieve business objectives. 4. Evaluation of threats and vulnerabilities of achieving commitments to customers. 5. Results and action items are communicated to the respective owners and tracked through Datacate's internal risk management tool.</p> <p>Monitoring and alarming are configured by Datacate security teams to identify and notify management of incidents when thresholds are crossed on key security and operational metrics including system performance, suspicious user activity, unauthorized changes to security protocols, and data center environmental stability. Issues, if any, are routed through incident management for resolution.</p> <p>Datacate performs and/or contracts with 3rd parties to perform vulnerability and penetration testing at least annually. Issue, if any, are routed through incident and risk management processes for resolution.</p>
<p>164.308(a)(1)(ii)(C) Sanction Policy (_R_)</p>	<p><b>CC1.0</b></p>	<p>Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.</p>	<p>Personnel are required to read and accept the code of conduct, the statement of confidentiality and privacy practices upon their hire and to formally reaffirm them annually thereafter. Violations are subject to disciplinary actions and/or termination.</p> <p>Datacate has dedicated security personnel responsible for promoting security awareness and training employees on Datacate security, privacy commitments and HIPAA requirements. Training is conducted at least annually.</p>

Section	Criteria	Safeguard Description	Datacate Control Activity
164.308(a)(1)(ii)(D) Information System Activity Review (_R_)	<b>CC4.0</b> <b>CC6.0</b>	Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Annual user profile and access reviews are performed by domain administrator. The review includes a review of all active users, including employees and contractors.  Monitoring and alarming are configured by Datacate security teams to identify and notify management of incidents when thresholds are crossed on key security and operational metrics including system performance, suspicious user activity, unauthorized changes to security protocols, and data center environmental stability. Issues, if any, are routed through incident management for resolution.
164.308(a)(2) Assigned Security Responsibility	<b>CC1.0</b>	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	Datacate has dedicated security personnel responsible for promoting security awareness and training employees on Datacate security and privacy commitments and HIPAA requirements. Training is conducted at least annually. Datacate has security policies that have been approved by management and published on the intranet which is accessible to all employees.
164.308(a)(3)(i) Workforce Security	<b>CC1.0</b> <b>CC5.0</b>	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information (ePHI), as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information (ePHI).	By nature of the services provided within the contract, Datacate personnel does not have access to ePHI. User access is limited by profiles and roles assigned to users based on their job function (role-based security).
164.308(a)(3)(ii)(A) Authorization and/ or Supervision (A)	<b>CC5.0</b>	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information (ePHI) or in locations where it might be accessed.	Access to production machines, network devices, and support tools is authorized through group memberships and is approved by respective group administrators prior to account provisioning.  Annual user profile and access reviews are performed by domain administrator. The review includes a review of all active users, including employees and contractors.

Section	Criteria	Safeguard Description	Datacate Control Activity
164.308(a)(3)(ii)(B) Workforce Clearance Procedures (A)	<b>CC5.0</b>	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	<p>Datacate corporate office access is restricted through badge access cards which are distributed only after all required background investigations are completed.</p> <p>Access to production machines, network devices, and support tools is authorized through group memberships and is approved by respective group administrators prior to account provisioning.</p> <p>Annual user profile and access reviews are performed by domain administrator. The review includes a review of all active users, including employees and contractors.</p>
164.308(a)(3)(ii)(C) Termination Procedures (A)	<b>CC5.0</b> <b>CC6.0</b>	Implement procedures for terminating access to electronic protected health information (ePHI) when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	<p>By nature of the services provided within the contract, Datacate personnel does not have access to ePHI.</p> <p>Upon termination during the exit interview process, access to Datacate systems and tools, including corporate email, is removed.</p> <p>Annual user profile and access reviews are performed by domain administrator. The review includes a review of all active users, including employees and contractors.</p>
164.308(a)(4)(i) Information Access Management	<b>CC5.0</b> <b>CC6.0</b>	Implement policies and procedures for authorizing access to (ePHI) that are consistent with the applicable requirements of subpart E of this part [the Privacy Rule].	See information at 164.308(a)(3)(ii)(A) Authorization and/or Supervision.
164.308(a)(4)(ii)(A) Isolation Health Clearinghouse Functions (_R_)	<b>CC9.0</b>	If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the (ePHI) of the clearinghouse from unauthorized access by the larger organization.	Not applicable – Datacate is not a healthcare clearinghouse.
164.308(a)(4)(ii)(B) Access Authorization	<b>CC6.0</b>	Implement policies and procedures for granting access to (ePHI), for example, through access to a workstation, transaction, program, process, or other mechanism.	See information at 164.308(a)(3)(i) Workforce Security.

Section	Criteria	Safeguard Description	Datacate Control Activity
164.308(a)(4)(ii)(C) Access Establishment & Modification (A)	<b>CC6.0</b>	Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	See information at 164.308(a)(3)(ii)(A) Authorization and/or Supervision.
164.308(a)(5)(i) Security Awareness Training	<b>CC1.0</b> <b>CC2.0</b>	Implement a security awareness and training program for all members of its workforce (including management).	Datacate has dedicated security personnel responsible for promoting security awareness and training employees on Datacate security and privacy commitments and HIPAA requirements. Training is conducted at least annually. Datacate has security policies that have been approved by management and published on the intranet which is accessible to all employees.
164.308(a)(5)(ii)(A) Security Reminders (A)	<b>CC1.0</b> <b>CC2.0</b>	Periodic security updates.	<p>Datacate has dedicated security personnel responsible for promoting security awareness and training employees on Datacate security and privacy commitments and HIPAA requirements. Training is conducted at least annually</p> <p>Datacate has security policies that have been approved by management and published on the intranet which is accessible to all employees.</p> <p>Patches to infrastructure elements and changes to network configurations (e.g., firewall, port, and IP access) are reviewed and approved prior to deployment.</p>
164.308(a)(5)(ii)(B) Protection from Malicious Software (A)	<b>CC6.0</b>	Procedures for guarding against, detecting, and reporting malicious software.	<p>Monitoring and alarming are configured by Datacate security teams to identify and notify management of incidents when thresholds are crossed on key security and operational metrics including system performance, suspicious user activity, unauthorized changes to security protocols, and data center environmental stability. Issues, if any, are routed through incident management for resolution.</p> <p>Antivirus software is installed on workstations, laptops, and servers supporting such software.</p>

Section	Criteria	Safeguard Description	Datacate Control Activity
<p>164.308(a)(5)(ii)(C) Log-in Monitoring (A)</p>	<p><b>CC4.0</b> <b>CC5.0</b> <b>CC7.0</b></p>	<p>Procedures for monitoring log-in attempts and reporting discrepancies.</p>	<p>Monitoring and alarming are configured by Datacate security teams to identify and notify management of incidents when thresholds are crossed on key security and operational metrics including system performance, suspicious user activity, unauthorized changes to security protocols, and data center environmental stability. Issues, if any, are routed through incident management for resolution.</p> <p>Policy and procedures for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints (and the process for doing so) are made available to internal and external users.</p>
<p>164.308(a)(5)(ii)(D) Password Management (A)</p>	<p><b>CC6.0</b></p>	<p>Procedures for creating, changing, and safeguarding passwords.</p>	<p>Password standards for all Datacate systems are documented and systematically enforced as follows:</p> <ul style="list-style-type: none"> <li>• Maximum password age - 60 days</li> <li>• Minimum length - 8 characters</li> <li>• Complexity – enabled</li> <li>• History – 5</li> <li>• Invalid logon attempts – 5</li> </ul> <p>Administrator access to the Datacate system is restricted to authorized personnel and authenticated through secured Kerberos protocol authentication with LDAP authorization management.</p> <p>Access to Datacate systems requires a unique ID and password.</p>
<p>164.308(a)(6)(i) Security Incident Procedures</p>	<p><b>CC6.0</b></p>	<p>Implement policies and procedures to address security incidents.</p>	<p>Monitoring and alarming are configured by Datacate security teams to identify and notify management of incidents when thresholds are crossed on key security and operational metrics including system performance, suspicious user activity, unauthorized changes to security protocols, and data center environmental stability. Issues, if any, are routed through incident management for resolution.</p> <p>Policy and procedures for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints (and the process for doing so) are made available to internal and external users.</p>

Section	Criteria	Safeguard Description	Datacate Control Activity
164.308(a)(6)(ii) Response & Reporting (_R_)	<b>CC7.0</b>	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	See information at 164.308(a)(6)(i) Security Incident Procedures.
164.308(a)(7)(i) Contingency Plan	<b>CC7.0 A1.0</b>	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain (ePHI).	<p>Business continuity and disaster recovery plans have been developed and are updated annually.</p> <p>Business continuity plans, including restoration of backups, are tested annually.</p> <p>Weekly full-system and daily incremental backups are performed using an automated system.</p> <p>Datacate uses a multi-location strategy for its facilities to permit the resumption of operations at other entity facilities in the event of loss of a facility.</p>
164.308(a)(7)(ii)(A) Data Backup Plan (_R_)	<b>CC7.0 A1.0</b>	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	Not applicable – Datacate does not have access to back up data that contains (ePHI).
164.308(a)(7)(ii)(B) Disaster Recovery Plan (_R_)	<b>CC7.0 A1.0</b>	Establish (and implement as needed) procedures to restore any loss of data.	See information at 164.308(a)(7)(i) Contingency Plan.
164.308(a)(7)(ii)(C) Emergency Mode Operation Plan (_R_)	<b>CC7.0 A1.0</b>	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of (ePHI) while operating in emergency mode.	See information at 164.308(a)(7)(i) Contingency Plan.
164.308(a)(7)(ii)(D) Testing & Revision Procedures (A)	<b>CC7.0 A1.0</b>	Implement procedures for periodic testing and revision of contingency plans.	See information at 164.308(a)(7)(i) Contingency Plan.

Section	Criteria	Safeguard Description	Datacate Control Activity
<p>164.308(a)(7)(ii)(E) Application and Data Criticality Analysis (A)</p>	<p><b>CC3.0</b> <b>CC9.0</b> <b>A1.0</b></p>	<p>Assess the relative criticality of specific applications and data in support of other contingency plan components.</p>	<p>Business continuity and disaster recovery plans have been developed and are updated annually.</p> <p>A formal risk management process for evaluating risks based on identified threats and specified tolerances have been established. Specific components of the risk assessment process are performed during routine management meetings to address the following:</p> <ol style="list-style-type: none"> <li>1) Evaluation of the Datacate organizational structure, capability, capacity, reporting lines, authorities, and responsibilities.</li> <li>2) Identification and evaluation of environmental, regulatory, and technological changes that have occurred.</li> <li>3) Evaluation of the need for additional tools and resources in order to achieve business objectives.</li> <li>4) Evaluation of threats and vulnerabilities of achieving commitments to customers.</li> </ol> <p>Results and action items are communicated to the respective owners and tracked through Datacate's internal risk management tool.</p>

Section	Criteria	Safeguard Description	Datacate Control Activity
164.308(a)(8) Evaluation	<b>CC3.0</b> <b>CC4.0</b>	Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of (ePHI), that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.	<p>A formal risk management process for evaluating risks based on identified threats and specified tolerances have been established. Specific components of the risk assessment process are performed during routine management meetings to address the following:</p> <ol style="list-style-type: none"> <li>1) Evaluation of the Datacate organizational structure, capability, capacity, reporting lines, authorities, and responsibilities.</li> <li>2) Identification and evaluation of environmental, regulatory, and technological changes that have occurred.</li> <li>3) Evaluation of the need for additional tools and resources in order to achieve business objectives.</li> <li>4) Evaluation of threats and vulnerabilities of achieving commitments to customers.</li> </ol> <p>Results and action items are communicated to the respective owners and tracked through Datacate's internal risk management tool.</p> <p>Datacate works performs and/or contracts with 3rd parties to perform vulnerability and penetration testing at least annually. Issue, if any, are routed through incident and risk management processes for resolution.</p>

Section	Criteria	Safeguard Description	Datacate Control Activity
<p>164.308(b)(1) &amp; (b)(2) Business Associate Contracts &amp; Other Arrangements</p>	<p><b>CC2.0</b> <b>CC9.0</b></p>	<p>(b)(1) A covered entity may permit a business associate to create, receive, maintain, or transmit (ePHI) on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.</p> <p>(b)(2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit (ePHI) on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.</p>	<p>Datacate establishes agreements, including non-disclosure agreements and HIPAA business associate agreements, when applicable, for preserving confidentiality of information and software exchanges with external parties.</p> <p>Datacate has business associate agreements for customers and keeps these in documents stored in the HIPAA BAA folder.</p>
<p>164.308(b)(3) Written Contract (_R_)</p>	<p><b>CC2.0</b> <b>CC9.0</b></p>	<p>Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).</p>	<p>Datacate establishes agreements, including non-disclosure agreements and HIPAA business associate agreements, when applicable, for preserving confidentiality of information and software exchanges with external parties.</p> <p>Datacate has business associate agreements for customers and keeps these in documents stored in the HIPAA BAA folder.</p>

*HIPAA Security Standards: Physical Safeguards*

Section	Criteria	Safeguard Description	Datacate Control Activity
164.310(a)(1) Facility Access Controls	<b>CC6.0</b>	Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	<p>Datacate does not have direct access to ePHI.</p> <p>Datacate corporate office access is restricted through badge access cards which are distributed only after all required background investigations are completed.</p> <p>Physical access to the data center is authorized by the customer point of contact (POC). Access cards are provisioned by Datacate personnel based on authorized request from the customer point of contact (POC).</p> <p>Physical access to the Datacate facility is restricted and authorized. Physical access reviews are performed annually. The review includes active Datacate employees. Upon customer request, Datacate will provide a data center electronic access usage report.</p> <p>Visitors must be signed in by an employee before a temporary badge that authorizes them can be issued. All visitors must be escorted by an entity employee when visiting facilities where sensitive system and system components are maintained and operated.</p> <p>Physical security measures in place are listed in section CC6.0.</p>
164.310(a)(2)(i) Contingency Operations (A)	<b>A1.0</b>	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	<ol style="list-style-type: none"> <li>1. Business continuity and disaster recovery plans have been developed and are updated annually.</li> <li>2. Business continuity plans, including restoration of backups, are tested annually.</li> <li>3. Weekly full-system and daily incremental backups are performed using an automated system.</li> <li>4. Datacate uses a multi-location strategy for its facilities to permit the resumption of operations at other entity facilities in the event of loss of a facility.</li> </ol>
164.310(a)(2)(ii) Facility Security Plan (A)	<b>CC6.0</b>	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	See information at 164.310(a)(1) Facility Access Controls.

Section	Criteria	Safeguard Description	Datacate Control Activity
<p>164.310(a)(2)(iii) Access Control Validation Procedures (A)</p>	<p><b>CC5.0</b></p>	<p>Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.</p>	<p>See information at 164.310(a)(1) Facility Access Controls.</p>
<p>164.310(a)(2)(iv) Maintenance Records (A)</p>	<p><b>A1.0 CC7.0</b></p>	<p>Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).</p>	<p>Environmental and building protections receive maintenance on at least an annual basis.</p> <p>Monitoring and alarming are configured by Datacate security teams to identify and notify management of incidents when thresholds are crossed on key security and operational metrics including system performance, suspicious user activity, unauthorized changes to security protocols, and data center environmental stability. Issues, if any, are routed through incident management for resolution.</p> <p>Change Management policies, including security code reviews, are in place and procedures for tracking, testing, and approving are documented.</p>
<p>164.310(a)(2)(iv) Maintenance Records (A) 164.310(b) Workstation Use</p>	<p><b>CC1.0</b></p>	<p>Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.</p>	<p>Datacate has dedicated security personnel responsible for promoting security awareness and training employees on Datacate security, privacy commitments and HIPAA requirements. Training is conducted at least annually. Datacate has security policies that have been approved by management and published on the intranet which is accessible to all employees.</p> <p>Personnel are required to read and accept the code of conduct, the statement of confidentiality and privacy practices upon their hire and to formally reaffirm them annually thereafter.</p> <p>Access to production machines, network devices, and support tools is authorized through group memberships and is approved by respective group administrators prior to account provisioning.</p> <p>Monitoring and alarming are configured by Datacate security teams to identify and notify management of incidents when thresholds are crossed on key security and operational metrics including system performance, suspicious user activity, unauthorized changes to security protocols, and data center environmental stability. Issues, if any, are routed through incident management for resolution.</p>

Section	Criteria	Safeguard Description	Datacate Control Activity
164.310(c) Workstation Security	<b>CC5.0</b>	Implement physical safeguards for all workstations that access electronic protected health information (ePHI), to restrict access to authorized users.	See information at 164.310(a)(1) Facility Access Controls.
164.310(d)(1) Device & Media Controls	<b>CC1.0 CC6.0 A1.0</b>	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information (ePHI) into and out of a facility, and the movement of these items within the facility.	Decommission checklist is required for removal of storage.
164.310(d)(2)(i) Disposal (_R_)	<b>CC1.0</b>	Implement policies and procedures to address the final disposition of electronic protected health information (ePHI), and/or the hardware or electronic media on which it is stored.	Decommission checklist is required for removal of storage.  Datacate has developed Data Classification Guidelines and Security Labels for Datacate Information to establish procedures for information labeling and handling in accordance with the Datacate data classification guidelines.
164.310(d)(2)(ii) Media Re-use (_R_)	<b>N/A</b>	Implement procedures for removal of electronic protected health information (ePHI) from electronic media before the media are made available for re-use.	Not applicable – Media is not reused. Please refer to 164.310(d)(2)(i) Disposal (_R_).
164.310(d)(2)(iii) Accountability (A)	<b>CC5.0</b>	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	See information at 164.310(a)(1) Facility Access Controls.
164.310(d)(2)(iv) Data Backup & Storage (A)	<b>N/A</b>	Create a retrievable, exact copy of electronic protected health information (ePHI), when needed, before movement of equipment.	Not applicable – Datacate is not responsible for maintaining back up electronic protected health information (ePHI).

## HIPAA Security Standards: Technical Safeguards

Section	Criteria	Safeguard Description	Datacate Control Activity
164.312(a)(1) Access Control	<b>CC6.0</b>	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information (ePHI) to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	<p>The Datacate environment is authenticated through SSL-protected endpoints both from the internet and within the internal system infrastructure and includes SSL defined points.</p> <p>Datacate network devices are configured to restrict access to authorized ports and trusted IP addresses when authenticating to infrastructure systems.</p> <p>Access to production machines, network devices, and support tools is authorized through group memberships and is approved by respective group administrators prior to account provisioning.</p> <p>User access is limited by profiles and roles assigned to users based on their job function (role-based security).</p>
164.312(a)(2)(i) Unique User Identification (_R_)	<b>CC6.0</b>	Assign a unique name and/or number for identifying and tracking user identity.	<p>Access to Datacate systems requires a unique ID and password.</p> <p>Administrator access to the Datacate system is restricted to authorized personnel and authenticated through secured Kerberos protocol authentication with LDAP authorization management.</p>
164.312(a)(2)(ii) Emergency Access Procedure (_R_)	<b>CC6.0</b> <b>CC9.0</b> <b>A1.0</b>	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information (ePHI) during an emergency.	<p>Business continuity and disaster recovery plans have been developed and are updated annually.</p> <p>Business continuity plans, including restoration of backups, are tested annually.</p>
164.312(a)(2)(iii) Automatic Logoff (A)	<b>CC6.0</b>	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Workstations that have access to customer account data are placed into password protected sleep mode when systems are unattended for a predetermined time.
164.312(a)(2)(iv) Encryption & Decryption (Stored) (A)	<b>CC6.0</b>	Implement a mechanism to encrypt and decrypt electronic protected health information (ePHI).	Workstations that have access to customer account data are placed into password protected sleep mode when systems are unattended for a predetermined time.

Section	Criteria	Safeguard Description	Datacate Control Activity
164.312(b) Audit Controls	<b>CC6.0</b>	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information (ePHI).	<p>Annual user profile and access reviews are performed by domain administrator. The review includes a review of all active users, including employees and contractors.</p> <p>Monitoring and alarming are configured by Datacate security teams to identify and notify management of incidents when thresholds are crossed on key security and operational metrics including system performance, suspicious user activity, unauthorized changes to security protocols, and data center environmental stability. Issues, if any, are routed through incident management for resolution.</p>
164.312(c)(1) Integrity	<b>CC1.0</b> <b>CC6.0</b>	Implement policies and procedures to protect electronic protected health information (ePHI) from improper alteration or destruction.	<p>Datacate does not have direct access to ePHI.</p> <p>Datacate corporate office access is restricted through badge access cards which are distributed only after all required background investigations are completed.</p> <p>Physical access to the data center is authorized by the customer point of contact (POC). Access cards are provisioned by Datacate personnel based on authorized request from the customer point of contact (POC).</p> <p>Physical access to the Datacate facility is restricted and authorized. Physical access reviews are performed annually. The review includes active Datacate employees. Upon customer request, Datacate will provide a data center electronic access usage report.</p> <p>Visitors must be signed in by an employee before a temporary badge that authorizes them can be issued. All visitors must be escorted by an entity employee when visiting facilities where sensitive system and system components are maintained and operated.</p> <p>Physical security measures in place are listed in section CC6.0.</p>
164.312(c)(2) Mechanism to Authenticate ePHI (A)	<b>N/A</b>	Implement electronic mechanisms to corroborate that electronic protected health information (ePHI) has not been altered or destroyed in an unauthorized manner.	Not applicable – Datacate user entities are responsible for the integrity of electronic protected health information (ePHI).

Section	Criteria	Safeguard Description	Datacate Control Activity
164.312(d) Person or Entity Authentication	<b>CC6.0</b>	Implement procedures to verify that a person or entity seeking access to electronic protected health information (ePHI) is the one claimed.	<p>Datacate does not have direct access to ePHI.</p> <p>Physical access to the data center is authorized by the customer point of contact (POC). Access cards are provisioned by Datacate personnel based on authorized request from the customer point of contact (POC).</p> <p>Physical access to the Datacate facility is restricted and authorized. Physical access reviews are performed annually. The review includes active Datacate employees. Upon customer request, Datacate will provide a data center electronic access usage report.</p> <p>Visitors must be signed in by an employee before a temporary badge that authorizes them can be issued. All visitors must be escorted by an entity employee when visiting facilities where sensitive system and system components are maintained and operated.</p> <p>Physical security measures in place are listed in section CC6.0</p>
164.312(e)(1) Transmission Security	<b>CC6.0</b>	Implement technical security measures to guard against unauthorized access to electronic protected health information (ePHI) that is being transmitted over an electronic communications network.	Datacate network devices are configured to restrict access to authorized ports trusted IP addresses when authenticating to infrastructure systems. Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters. Monitoring and alarming are configured by Datacate security teams to identify and notify management of incidents when thresholds are crossed on key security and operational metrics including system performance, suspicious user activity, unauthorized changes to security protocols, and data center environmental stability. Issues, if any, are routed through incident management for resolution.
164.312(e)(2)(i) Integrity Controls (A)	<b>N/A</b>	Implement security measures to ensure that electronically transmitted electronic protected health information (ePHI) is not improperly modified without detection until disposed of.	Not applicable – Datacate user entities are responsible for the integrity of electronic protected health information (ePHI).

Section	Criteria	Safeguard Description	Datacate Control Activity
<p>164.312(e)(2)(ii) Encryption (Transmission) (A)</p>	<p><b>CC6.0</b></p>	<p>Implement a mechanism to encrypt electronic protected health information (ePHI) whenever deemed appropriate.</p>	<p>Note: User entity is responsible for sending data to Datacate via a secure connection and/or the data should be encrypted.</p> <p>The Datacate system is authenticated through SSL-protected endpoints both from the internet and within the internal system infrastructure. This includes SSL defined points of connectivity to protect communications between customer portal users and their connection with the Datacate system.</p>