Lilac, LLC DBA DiplomaSender
SOC 3
2020

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

April 1, 2019 To March 31, 2020

Table of Contents

SECTION 1

ASSERTION OF LILAC, LLC DBA DIPLOMASENDER MANAGEMENT

ASSERTION OF Lilac, LLC DBA DiplomaSender MANAGEMENT

May 7, 2020

We are responsible for designing, implementing, operating, and maintaining effective controls within Lilac, LLC DBA DiplomaSender's ('DiplomaSender' or 'the Company') Documentation Repository Application Services System throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that DiplomaSender's service commitments and system requirements relevant to Security and Confidentiality (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in "Lilac, LLC DBA DiplomaSender's Description of Its Documentation Repository Application Services System throughout the period April 1, 2019 to March 31, 2020" and identifies the aspects of the system covered by our assertion.

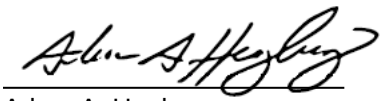
We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that DiplomaSender's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity and Privacy* (AICPA, *Trust Services Criteria*). DiplomaSender's objectives for the system in applying applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "Lilac, LLC DBA DiplomaSender's Description of Its Documentation Repository Application Services System throughout the period April 1, 2019 to March 31, 2020".

DiplomaSender uses Microsoft Azure ('Azure' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at DiplomaSender, to achieve DiplomaSender's service commitments and system requirements based on the applicable trust services criteria. The description presents DiplomaSender's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of DiplomaSender's controls. The description does not disclose the actual controls at the subservice organization.

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

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

We assert that the controls within the system were effective throughout the period April 1, 2019 to March 31, 2020 to provide reasonable assurance that DiplomaSender's service commitments and system requirements were achieved based on the applicable trust services criteria.



Adam A. Hughey
President
Lilac, LLC DBA DiplomaSender

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Lilac, LLC DBA DiplomaSender:

Scope

We have examined Lilac, LLC DBA DiplomaSender's ('DiplomaSender' or 'the Company') accompanying description of Documentation Repository Application Services System titled "Lilac, LLC DBA DiplomaSender's Description of Its Documentation Repository Application Services System throughout the period April 1, 2019 to March 31, 2020" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that DiplomaSender's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

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

Service Organization's Responsibilities

DiplomaSender 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 DiplomaSender's service commitments and system requirements were achieved. DiplomaSender has provided the accompanying assertion titled "Assertion of Lilac, LLC DBA DiplomaSender Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. DiplomaSender 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 Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of 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 stated therein were suitably designed and operated 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.

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

- 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 operate 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 report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and 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.

Opinion

In our opinion, management's assertion that the controls within DiplomaSender's Documentation Repository Application Services System were suitably designed and operating effectively throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that DiplomaSender's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

The SOC logo for Service Organizations on DiplomaSender's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of DiplomaSender, user entities of DiplomaSender's Documentation Repository Application Services during some or all of the period April 1, 2019 To March 31, 2020, business partners of DiplomaSender subject to risks arising from interactions with the Documentation Repository Application Services, and those who have sufficient knowledge and understanding of the complementary user entity controls and 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.

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

A-LIGN ASSURANCE

Tampa, Florida
May 7, 2020

SECTION 3

LILAC, LLC DBA DIPLOMASENDER'S DESCRIPTON OF ITS DOCUMENTATION REPOSITORY APPLICATION SERVICES SYSTEM THROUGHOUT THE PERIOD APRIL 1, 2019 TO MARCH 31, 2020

OVERVIEW OF OPERATIONS

Company Background

Lilac, L.L.C., dba DiplomaSender (DS) began operations in 2011 and during the last 9 years has accumulated and is now managing data for the High School Equivalency (HSE) population for twenty-one jurisdictions. Currently, DS inventories over 8 million physical test taker records (Analog) These are organized, inventoried and stored in DS's private climate controlled secure warehouse located in Oklahoma. In addition to Analog, there are approximately 120 million digital test taker records (Digital). Digital are managed in the Azure Cloud Service, this includes: SQL Databases, File Storage, Security Center, Data Encryption, and Geosynchronous Co-location.

Digital records are verified during the initial migration into the databases and then undergo a second tier of verification. As data is added and updated each record is validated and rechecked. This is a continual process and is integral to the DS data maintenance procedure. The resulting datasets are available online through a self-service management system. The DS HSE portal offers four broad user categories: 3rd Party Vendor, Test Taker, Test Center Administration, and HSE Administration. Using the DS website, a variety of options are available to test takers allowing them to view the testing history; view sample diplomas, transcripts, and certification letters (documents); and order complimentary and replacement documents.

DS is currently providing services in the states of: Alaska, California, Colorado, Delaware, District of Columbia, Idaho, Indiana, Iowa, Massachusetts, Maine, Michigan, Mississippi, Nevada, New Mexico, North Carolina, Ohio, Oklahoma, Pennsylvania, Tennessee, West Virginia, and Wyoming (States). Some states have authorized two or more publishers to administer the HSE and DS manages the multiple publisher (MP) data sets and the resulting DOCUMENTS in those states In all states the documents are customized and in MP states there are multiple transcripts specific to the publisher and the test series (Pre-02, 02, 2014).

Description of Services Provided

DS provides Documentation Repository Application Services. The company was founded in 2011 in Oklahoma.

DS's core service is the management and cleanup of HSE high-stakes testing data for contracted state partners. DS provides the following to the clients and the constituents:

- Management of electronic record data provided by:
    - Client states
    - HSE publishers
- Management of analog records provided by client states
- Digitization of analog records into combined database
- Fulfilment of initial issuance of earned credential and transcript
- Fulfillment of duplicate document requests by:
    - Academic record holder
    - Third-party approved agency
    - Government approved agency
- Management of transaction history and logs for each academic record

Information is shared with user entities by a secured website, telephone, and secure electronic exchange via Slack and FTP.

Principal Service Commitments and System Requirements

DS designs its processes and procedures related to data management of academic records to meet its objectives for its academic record accessibility and document distribution services. Those objectives are based on the service commitments that DS makes to user entities, the laws and regulations that govern the provision of academic record accessibility and document distribution services, and the financial, operational, and compliance requirements that DS has established for the services. The academic record accessibility and document distribution services of DS are subject to the security and privacy requirements of the Family Educational Rights and Privacy Act (FERPA), as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which DS operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

Security principles within the fundamental designs of the data management of academic records are designed to permit system users to access the information they need based on the role in the system while restricting them from accessing information not needed for the roles. Use of encryption technologies to protect customer data both at rest and in transit.

DS establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in DS's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how collaborators are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the data management of academic records.

Components of the System

Infrastructure

Primary infrastructure used to provide DS's Documentation Repository Application services system includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Cloud	Azure Selected	Hosts website, database, and storage
Firewall	Azure	Managed by Microsoft

Software

Primary software used to provide DS's Documentation Repository Application services system includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Azure SQL	N/A	Microsoft SQL Server hosted in Azure
Azure Web App		Website hosted in Azure

Primary Software		
Software	**Operating System**	**Purpose**
Azure Storage		Cloud storage hosted in Azure

People

DS has a staff of approximately 30 collaborators organized in the following functional areas:

- Leadership. Executives, Directors, and company administrative support staff, such as legal, compliance, internal audit, training, contracting, accounting, finance, and human resources
- Contact Center
- IT. Help desk, IT infrastructure, IT networking, IT system administration, software systems development and application support, information security, and IT operations personnel manage electronic interfaces and business implementation support and telecom
    - The help desk group provides technical assistance to users
    - The infrastructure, networking, and systems administration staff typically has no direct use of the data management of academic records. Rather, it supports DS' IT infrastructure, which is used by the software. A systems administrator will deploy the releases of the data management of academic records and other software into the production environment
    - The software development staff develops and maintains the custom software for DS. This includes the data management of academic records, supporting utilities, and the external websites that interact with the data management of academic records. The staff includes software architect and developers, database architect and administrator, and software quality assurance
    - The Microsoft Azure information security staff supports the data management of academic records indirectly by monitoring internal and external security threats and maintaining current antivirus software
    - The Microsoft Azure information security staff maintains the inventory of IT assets
    - IT operations in collaboration with Microsoft Azure manage the user interfaces for the data management of academic records. This includes processing user entity-supplied membership and eligibility files, producing encounter claims files, and other user-oriented data (capitation files, error reports, remittance advice, and so on)

Data

Data, as defined by DS, constitutes the following:

- Academic record file data
- Transaction data
- Electronic interface files
- Output reports
- Input reports
- System files
- Error logs

Academic record processing is initiated by the automatic export from each publisher. Additional information is entered into the system automatically and manually through analog record review and digitization.

Output reports are available in electronic PDF, comma-delimited value file exports, or electronically from the website. The availability of these reports is limited by job function. Reports delivered externally will only be sent using a secure method— secure FTP, or secure websites—to educational providers, testing facilities, and governments or managed providers using DS-developed websites or over connections secured by trusted security certificates. DS uses Slack to encrypt communication exchanges with government, testing centers, and educational providers.

Processes, Policies and Procedures

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

Physical Security

Wholly occupied company facilities are protected by walls and permanently locked doors around the entire perimeter. The facility has a designated reception area which is accessed when hosted by a DS collaborator and is monitored by security cameras recording 24 hours per day. Access to the reception area is always locked. Visitors, seeking access, press a buzzer to attract the attention of a collaborator who authenticates the identity and releases the lock. The door may also be unlocked through the use of an access card/ID that has been assigned general access to the facility. Access beyond the reception area is controlled through the access card system.

All remaining exterior ingress doors are restricted to users possessing an access card/ID that has been assigned access to use the door. Access is restricted through the use of access control lists. Collaborators and vendors granted access cards are assigned to roles based on the job responsibilities.

Visitors check in with the receptionist or security guard stationed in the reception area. Visitors must present a valid, government-issued photo ID. The visitor's name, employer, and purpose for visit are recorded in a visitor log and his or her visit must be approved by a DS collaborator who is authorized to sign non-collaborators into the facility. The visitor is escorted throughout the duration of his or her visit.

Upon a collaborator's termination of employment, the HR generates an access deletion record on the last day of employment. This record is routed to the access administrators for deletion. In addition, terminated collaborators turn over access cards/IDs during the exit interview. These cards are then sent via tracked shipping to physical security for recording and destruction. On a monthly basis, the director of IT runs a report detailing access cards with deleted access that have not been recorded as returned. The director investigates all missing cards and documents the resolution in the event management system.

DS utilizes Azure for cloud hosting services at the multiple facilities. See 'Subservice Organizations' section below for detailed controls.

Logical Access

DS uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists.

All resources are managed in the asset inventory system and each asset is assigned an owner.

Collaborators and approved vendor personnel sign on to the DS network using an Active Directory user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Active Directory. Passwords must conform to defined password standards and are enforced through Active Directory. These settings are part of the configuration standards, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts.

Collaborators access DS services through the Internet using the SSL functionality of the web-browser. These customer collaborators must supply a valid user ID and password to gain access to the website. Passwords must conform to password configuration requirements configured on the web server. The ability to recall backups is restricted to authorized IT personnel.

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify, and respond to incidents on the network.

DS monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. DS evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Database performance
- Cloud storage
- Network bandwidth

DS has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. DS staff validate that all patches have been installed and if applicable that reboots have been completed. and procedures used to provide the services.

Computer Operations - Backups

Customer data is backed up and monitored by Azure for completion and exceptions. In the event of an exception, Azure systems perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job depending on customer indicated preference within the documented work instructions.

Backup infrastructure and on-site backup tape media are physically secured in locked cabinets and/or caged environments within the third-party data centers. The backup infrastructure resides on managed networks logically secured from other networks. The ability to recall backups is restricted to authorized IT personnel.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify, and respond to incidents on the network.

DS monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. DS evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Disk storage
- Network bandwidth

DS has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and DS system owners review proposed operating system patches to determine whether the patches are applied. Customers and DS systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. DS staff validate that all patches have been installed and if applicable that reboots have been completed. and procedures used to provide the services.

Change Control

DS maintains documented change control policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

DS has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and DS system owners review proposed operating system patches to determine whether the patches are applied. Customers and DS systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. DS staff validate that all patches have been installed and if applicable that reboots have been completed.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Administrative access to the firewall is restricted to authorized collaborators.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure. In the event that a primary system fails, the redundant system is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by DS. The third-party vendor’s approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications, and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed in real time by Qualys. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the DS system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized collaborators may access the system from the Internet through the use of DS’s secure website. Collaborators are authenticated through the use of a two-factor authentication system.

Boundaries of the System

The scope of this report includes the Documentation Repository Application services system performed in the Norman, Oklahoma facility.

This report does not include the cloud hosting services provided by Azure at the Central US (Iowa), East US (Virginia), East US 2 (Virginia), South Central US (Texas), and West US (California) regional facilities.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Incident in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Criteria Not Applicable to the System

All Common and Confidentiality criterion were applicable to the DS Documentation Repository Application services system.

Subservice Organizations

This report does not include the cloud hosting services provided by Azure at the Central US (Iowa), East US (Virginia), East US 2 (Virginia), South Central US (Texas), and West US (California) regional facilities.

Subservice Description of Services

Azure is a cloud computing platform for building, deploying and managing applications through a global network of Microsoft and third-party managed datacenters. It supports both Platform as a Service and Infrastructure as a Service cloud service models and enables hybrid solutions that integrate cloud services with customers' on-premises resources.

Complementary Subservice Organization Controls

DS's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to DS's services to be solely achieved by DS control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of DS.

The following subservice organization controls should be implemented by DS to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - Azure		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors.
		Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors.

Subservice Organization - Azure		
Category	**Criteria**	**Control**
		Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		The datacenter facility is monitored 24x7 by security personnel.

DS management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, DS performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

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

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

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