System and Organization Controls (SOC) 2 Type 2 Report

Report on Digital Imaging Solutions Inc.'s Description of Its DIS Direct Service

Relevant to Security

Throughout the Period August 1, 2024 to January 31, 2025

Table of Contents

Section I: Independent Service Auditor's Report

To: Digital Imaging Solutions Inc. ("DIS Direct" or "the Company")

Scope

We have examined DIS Direct's accompanying description of its DIS Direct Service found in Section 3 titled “DIS Direct's Description of Its DIS Direct Service Throughout the Period August 1, 2024 to January 31, 2025” (description), based on the criteria for a description of a service organization’s system set forth 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 for the period August 1, 2024 to January 31, 2025, to provide reasonable assurance that DIS Direct's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (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)*.

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

DIS Direct uses a subservice organization for infrastructure and data hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at DIS Direct to achieve DIS Direct's service commitments and system requirements based on the applicable trust services criteria. The description presents DIS Direct's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of DIS Direct'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.

Service Organization’s Responsibilities

DIS Direct 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 DIS Direct's service commitments and system requirements were achieved. In Section 2, DIS Direct has provided the accompanying assertion titled “Assertion of Digital Imaging Solutions Inc. Management” (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. DIS Direct 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 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 engagement.

An examination of a 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 provides 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 report 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 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, DIS Direct's Controls, Service Auditor Tests, and Results of Tests” of this report.

Controls That Were Not Tested During the Period

The Company’s description of its system discusses the following controls implemented and operated during the period August 1, 2024 to January 31, 2025 that were not tested as part of our procedures:

- REQ-8: Upon hire, employees acknowledge that they have read and agree to the Code of Conduct.
- REQ-10: Upon hire, employees acknowledge that they have read and agree to the confidentiality agreement.
- REQ-11: New employees offered employment are subject to background checks prior to their start date.
- REQ-12: New employees complete security awareness training upon hire.
- REQ-30: Access to system components is based on job role, function, and requires a documented access request with manager approval prior to access being provisioned.

- REQ-31: Access to system components is revoked within 24 hours of termination as part of the termination process.
- REQ-50: All incidents related to security are logged, tracked, evaluated, and communicated to affected parties by management until the Company has recovered from the incidents.

During the period August 1, 2024 to January 31, 2025, the Company did not experience the above control activities that would warrant the operation of the controls during the period.

Because the controls described above were not required to operate during the period, we did not test the operating effectiveness of those controls as evaluated using the following trust services criteria (TSC):

- TSC CC1.1: The entity demonstrates a commitment to integrity and ethical values.
- TSC CC1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
- TSC 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.
- TSC 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.
- TSC 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.

Opinion

In our opinion, in all material respects—

a. The description presents the DIS Direct Service that was designed and implemented throughout the period August 1, 2024 to January 31, 2025, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period August 1, 2024 to January 31, 2025, to provide reasonable assurance that DIS Direct's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of DIS Direct's controls throughout the period.
c. The controls stated in the description operated effectively throughout the period August 1, 2024 to January 31, 2025, to provide reasonable assurance that DIS Direct's service commitments and system requirements would be achieved based on the applicable trust services criteria, if complementary subservice organization controls and complimentary user entity controls assumed in the design of DIS Direct's controls operated effectively throughout the period.

Restricted Use

This report is intended solely for the information and use of DIS Direct; user entities of the DIS Direct Service throughout the period August 1, 2024 to January 31, 2025, business partners of DIS Direct subject to risks arising from interactions with the DIS Direct Service, practitioners providing services to such user entities and business partners, prospective 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 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.

- 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.

Laika Compliance LLC

Arlington, Virginia

February 5, 2025

Section II: Assertion of Digital Imaging Solutions Inc. Management

We have prepared the accompanying description in Section 3 titled “DIS Direct's Description of its DIS Direct Service Throughout the Period August 1, 2024 to January 31, 2025” (description), based on the criteria for a description of a service organization’s system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report (AICPA, Description Criteria) (description criteria)*. The description is intended to provide report users with information about the DIS Direct Service that may be useful when assessing the risks arising from interactions with DIS Direct's system, particularly information about system controls that DIS Direct 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 (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)*.

DIS Direct uses a subservice organization for infrastructure and data hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at DIS Direct, to achieve DIS Direct's service commitments and system requirements based on the applicable trust services criteria. The description presents DIS Direct's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of DIS Direct'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, along with controls at DIS Direct, to achieve DIS Direct's service commitments and system requirements based on the applicable trust services criteria. The description presents DIS Direct's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of DIS Direct's controls.

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

- The description presents the DIS Direct Service that was designed and implemented throughout the period August 1, 2024 to January 31, 2025, in accordance with the description criteria.
- The controls stated in the description were suitably designed throughout the period August 1, 2024 to January 31, 2025, to provide reasonable assurance that DIS Direct'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 DIS Direct's controls throughout that period.
- The controls stated in the description operated effectively throughout the period August 1, 2024 to January 31, 2025, to provide reasonable assurance that DIS Direct'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 DIS Direct's controls operated effectively throughout that period.

Our description of the DIS Direct Service discusses the following controls implemented during the period August 1, 2024 to January 31, 2025 that were not required to operate due to non occurrence of the activities:

- REQ-8: Upon hire, employees acknowledge that they have read and agree to the Code of Conduct.
- REQ-10: Upon hire, employees acknowledge that they have read and agree to the confidentiality agreement.
- REQ-11: New employees offered employment are subject to background checks prior to their start date.
- REQ-12: New employees complete security awareness training upon hire.
- REQ-30: Access to system components is based on job role, function, and requires a documented access request with manager approval prior to access being provisioned.
- REQ-31: Access to system components is revoked within 24 hours of termination as part of the termination process.

- REQ-50: All incidents related to security are logged, tracked, evaluated, and communicated to affected parties by management until the Company has recovered from the incidents.

During the period August 1, 2024 to January 31, 2025, DIS Direct did not experience the above control activities that would warrant the operation of the controls during the period.

Digital Imaging Solutions Inc.

Section III: DIS Direct's Description of Its DIS Direct Service Throughout the Period August 1, 2024 to January 31, 2025

Overview of Operations

Digital Imaging Solutions Inc. (“DIS Direct” or “the Company”) is a mail service provider company that offers professional mailing services.

The system description in this section of the report details the DIS Direct Service. Any other Company services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of the subservice organization).

Principal Service Commitments and System Requirements

Service commitments are declarations made by management to customers regarding the performance of the DIS Direct Service. The Master Service Agreement (MSA) includes the communication of the Company's commitments to its customers.

System requirements are specifications regarding how the DIS Direct Service should function to meet the Company’s principal commitments to customers. System requirements are specified in the Company’s policies and procedures, system design documentation, contracts with customers, and in government regulations.

The Company’s principal service commitments and system requirements related to the DIS Direct Service include the following:

Trust Services Category	Service Commitments	System Requirements
Security	DIS Direct will take responsibility for implementing appropriate technical and organizational safeguards to ensure the protection of sensitive information.	• Change Management • Encryption Standards • Identity and Access Management • Security Awareness Training • Security Incident Response • Security Monitoring and Reporting • Threat and Vulnerability Management • Vendor Risk Management

The Components of the System Used to Provide the Service

The boundaries of the DIS Direct Service are the specific aspects of the Company’s infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the DIS Direct Service.

The components that directly support the services provided to customers are described in the subsections below.

INFRASTRUCTURE AND SOFTWARE

The Company utilizes Microsoft 365 to provide the resources to host the DIS Direct Service. The in-scope hosted infrastructure and list of software and ancillary software used to build, support, secure, maintain, and monitor the DIS Direct Service are shown in the table below:

Infrastructure and Software	
Production Tool	**Business Function**
Microsoft Defender for Endpoint	Anti-Malware
SonicWall Firewall	Network Traffic Control

PEOPLE

The Company develops, manages, and secures the DIS Direct Service via separate departments. The responsibilities of these departments involved in the governance, management, operation, security, and use of the DIS Direct Service are defined in the following table:

People	
Group/Role Name	**Function**
Customer Service	Responsible for managing customer relationships and addressing customer issues.
Executive Management	Responsible for overseeing Company-wide activities, establishing and accomplishing goals, and managing objectives.
Sales	Responsible for sales and marketing.

PROCEDURES

Procedures include the automated and manual procedures involved in the operation of the DIS Direct Service. Procedures are developed and documented by the respective teams for a variety of processes. These procedures are drafted in alignment with the overall Information Security Policy and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of the DIS Direct Service:

Procedure	Description
Logical Access	How the Company restricts logical access, provides and removes that access, and prevents unauthorized access.
System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.
Configuration and Change Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk and Compliance	How the Company identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.
Business Continuity and Disaster Recovery (BC/DR)	How the Company identifies the steps to be taken in the event of a disaster to help resume business operations.
Data Classification and Handling	How the Company classifies data included in the service and the procedures for handling the data.
Incident Response Plan	How the Company identifies the steps to be taken in the event of a security incident.

DATA

Data refers to transaction streams, files, data stores, tables, and other outputs used or processed by the Company. Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts. The Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Disk encryption is enabled on workstations.

SYSTEM INCIDENTS

A system event is defined as an occurrence that could lead to the loss of, or disruption to, operations, services, or functions and result in DIS Direct's failure to achieve its service commitments or system requirements. Such an occurrence may arise from actual or attempted access or use by internal or external parties and (a) impair (or potentially impair) the availability, integrity, or confidentiality of information or systems; (b) result in unauthorized disclosure or theft of information or other assets or the destruction of corruption of data; or (c) cause damage to systems. Such occurrences also may arise from the failure of the DIS Direct Service to process data as designed or from the loss, corruption, or destruction of data used by the DIS Direct Service.

On the other hand, a system incident is defined as a system event that requires action on the part of DIS Direct management to prevent or reduce the impact of the event on DIS Direct's achievement of its service commitments and system requirements.

There were no identified significant system incidents that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements from August 1, 2024 to January 31, 2025.

The Applicable Trust Services Criteria and Related Controls

APPLICABLE TRUST SERVICES CRITERIA

The Trust Services Category that is in scope for the purposes of this report is Security.

- **Security:** Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

The common criteria are organized as follows:

1. Control environment: The criteria relevant to how the entity is structured and the processes the entity has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values, qualifications of personnel, and the environment in which they function.
2. Information and communication: The criteria relevant to how the entity communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.
3. Risk assessment: The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.
4. Monitoring activities: The criteria relevant to how the entity monitors the system, including the suitability and design and operating effectiveness of the controls, and acts to address deficiencies identified.
5. Control activities: The criteria relevant to the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.
6. Logical and physical access controls: The criteria relevant to how the entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
7. System operations: The criteria relevant to how the entity manages the operation of a system and detects and mitigates processing deviations, including logical and physical security deviations.
8. Change management: The criteria relevant to how the entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
9. Risk mitigation: The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

This report is focused solely on the Security category.

CONTROL ENVIRONMENT

INTEGRITY AND ETHICAL VALUES

DIS Direct places emphasis on ethics and communication within the organization. Management communicates and oversees the implementation of the Code of Conduct to new and current employees. The Code of Conduct describes employee responsibilities and expected behavior regarding data and information system usage. Employees receive the Code of Conduct upon hire and sign an acknowledgment to confirm that they have received, read, and understand its contents.

DIS Direct commits to the highest level of integrity in dealing with its customers, vendors, and workforce. This commitment to integrity is promulgated with established policies that cover a variety of business and integrity objectives.

As part of the compliance effort, DIS Direct maintains a complete inventory list of all third parties. Such third parties are contractually required to maintain relevant elements of information security policy requirements, and to report cybersecurity incidents, in a timely manner.

OVERSIGHT AND AUTHORITY

The Risk Committee is tasked with governance, oversight, and responsibilities relative to internal control. The Risk Committee includes members that are independent of the internal control function. The Risk Committee meets quarterly and maintains formal meeting minutes.

ORGANIZATIONAL STRUCTURE

DIS Direct's organizational structure provides a framework for planning, executing, and controlling business operations. The organizational structure assigns roles and responsibilities to provide for adequate staffing, efficiency of operations, and the segregation of duties. Roles and responsibilities are formally documented and include responsibilities for the oversight and implementation of the security and control environment. Management has also established authority and appropriate lines of reporting for key personnel. DIS Direct follows a structured onboarding process to assist new employees as they become familiar with processes, systems, policies, and procedures. DIS Direct places emphasis on ethics and communication within the organization.

MANAGEMENT’S PHILOSOPHY AND OPERATING STYLE

DIS Direct's senior management takes a hands-on approach to running the business. Senior management is heavily involved in all phases of the business operations. The senior management team remains in close contact with all personnel and consistently emphasizes appropriate behavior to all personnel and key vendor personnel.

AUTHORITY AND RESPONSIBILITY

Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control.

HUMAN RESOURCES

Upon hire and annually thereafter, all personnel must successfully complete training courses covering basic information security practices that support the functioning of an effective risk management program. The training courses are designed to assist employees in identifying and responding to cybersecurity threats, including social engineering, phishing, pharming, and avoiding inappropriate security practices.

If an employee is found to be violating company policies, additional training is provided, or other disciplinary actions are taken.

Employees with job responsibilities that fall directly within the incident response program have additional requirements to complete technical and job-specific training throughout the year. Additionally, those employees who have direct access to customer and employee data will receive specific training around incident management, information handling, and data protection.

When onboarding new personnel, background checks are performed by DIS Direct management.

INFORMATION AND COMMUNICATION

DIS Direct has an Information Security Policy to ensure that employees understand their individual roles and responsibilities concerning processing, as well as controls to ensure that significant events are communicated in a timely manner. The policy includes formal and informal training programs and the use of email, instant messaging, and other mechanisms to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel when issues are identified. The Information Security Policy helps users understand how their roles and responsibilities relate to the system and the policy is communicated to all users.

DIS Direct has also published documentation that describes the security features of the service, internal security-related processes and controls, and conformity to regulatory requirements.

RISK ASSESSMENT AND MITIGATION

DIS Direct has performed a risk assessment during the design and implementation of the control objectives and related controls described in this report. As part of the risk assessment, DIS Direct identified the threats and vulnerabilities relevant to the security of DIS Direct business operations and rated the risk posed by each identified vulnerability. This rating allowed for the design and implementation of controls to mitigate the most significant risks to the security of DIS Direct's service.

The risk assessment is performed annually, at a minimum, or in response to any major updates to the product, client base, or business plan.

When conducting the risk assessment, DIS Direct first identified threats and vulnerabilities relevant to the security of business operations. For each identified vulnerability, DIS Direct considered:

- The likelihood of impact (i.e., the likelihood of the vulnerability being exploited), and
- The severity of impact (i.e., how damaging an exploitation of the vulnerability would be).

The likelihood and severity of impact estimations were then used to establish a risk ranking for each vulnerability.

MONITORING

The systems within the boundary are configured to prevent and detect vulnerabilities. In addition to prompt reviews of system alerts, management provides monitoring and audit logging in the form of preventive, detective, and corrective reporting. Relevant output from monitoring and detection mechanisms is distributed to executive and management personnel. Anti-malware is enabled on workstations.

The Company utilizes a distributed approach in order to scale the security monitoring function by using a combination of commercially available tools, custom code, and an instant messaging platform. The Company has created a system that provides for the determination of attributions for the most critical security-relevant events and target notifications are sent to the staff with the authority and the context necessary to vet that security alert. The interface of this system allows the targeted staff member to either resolve the security alert if they can do so safely or to escalate to the appropriate team if a response is required.

CONTROL ACTIVITIES

An Information Security Policy has been formally documented and implemented to provide policies and procedures governing the protection of confidential and sensitive information. The Information Security Policy is communicated and distributed to employees upon hire. In the event of a significant change to the Information Security Policy, a communication is sent to all new and existing employees regarding the changes.

The Information Security Policy is reviewed and updated on an annual basis. The Information Security Policy defines information security responsibilities for all personnel. Where security responsibilities apply, roles are related to the policy and procedures that define their activity within their associated responsibilities. Security awareness training is provided to all employees upon hire and on an annual basis thereafter to ensure that personnel understand their security roles and responsibilities.

DIS Direct also communicates security roles and responsibilities to vendors and other third parties. Marketing and contractual materials that describe the services and scope of work provided to clients are documented and maintained to ensure that employees, contractors, vendors, and clients understand their roles and responsibilities.

LOGICAL ACCESS

Access management processes exist so that DIS Direct user accounts are added, modified, or disabled in a timely manner and are reviewed on a quarterly basis. In addition, password configuration settings for user authentication to DIS Direct Service are managed in compliance with DIS Direct's Password Policy which is part of the Information Security Policy.

Users must be approved for logical access by management prior to receiving access to DIS Direct Service. Management authorization is required before employment is offered and access is provided. Users must also be assigned a unique ID before being allowed access to system components. User IDs are authorized and implemented as part of the new hire onboarding process. Access rights and privileges are granted to user IDs based on the principle of least privilege and Role-Based Access Control (RBAC) protocols. Access is limited to that which is required for the performance of job duties for individual users, and generic access by DIS Direct employees is not allowed.

SYSTEM OPERATIONS

An Incident Response Policy has been formally documented and implemented to guide preparation, detection, response, analysis and repair, communication, follow-up, and training for any class of security breach or incident. The responsibilities in the event of a breach, the steps of a breach, and the importance of information security are defined for all employees. The Incident Response Team employs industry-standard diagnosis procedures (such as incident identification, registration and verification, as well as initial incident classification and prioritizing actions) to drive resolution during business-impacting events.

DIS Direct reviews, triages, and communicates all incident alerts to the Incident Response Team to initiate the incident response process. Post-mortems are convened after any significant operational issue, regardless of external impact. Documentation of the investigation is conducted to determine that the root cause is captured and that preventative actions may be taken for the future.

CHANGE MANAGEMENT

A Change Management Policy has been formally documented and implemented to guide the processes of change request, documentation, review, evaluation, approval, scheduling, testing, and implementation. Changes that may affect system availability and system security are communicated to management and any partners who may be affected.

System configuration standards are formally documented and implemented to ensure that all systems and network devices are properly and securely configured. Center for Internet Security (CIS) and National Institute of Standards and Technology (NIST) hardening standards are used as a basis for DIS Direct's system configuration standards.

SOFTWARE DEVELOPMENT

To provide the DIS Direct Service, software, and infrastructure is utilized. However, DIS Direct does not develop software or manage infrastructure to support the in-scope services. Microsoft 365 is responsible for the software development and infrastructure change management for the infrastructure and data hosting services provided to DIS Direct.

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

The Company’s controls related to the DIS Direct Service cover only a portion of overall internal control for each user entity of the DIS Direct Service. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. Therefore, each user entity’s internal control should be evaluated in conjunction with the Company’s controls and the related tests and results described in Section 4 of this report, taking into account the related CUECs identified for the specific criterion. In order for user entities to rely on the controls reported herein, each user entity must evaluate its own internal control environment to determine whether the identified CUECs have been implemented and are operating effectively.

The CUECs presented should not be regarded as a comprehensive list of all controls that should be employed by user entities.

Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls (CUECs)
CC2.1	• User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames. • Controls to provide reasonable assurance that the Company is notified of changes in: ○ User entity vendor security requirements. ○ The authorized user list.
CC2.3	• It is the responsibility of the user entity to have policies and procedures to: ○ Inform their employees and users that their information or data is being used and stored by the Company. ○ Determine how to file inquiries, complaints, and disputes to be passed on to the Company.
CC6.1	• User entities grant access to the Company's system to authorized and trained personnel. • User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.
CC6.6	• Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company.
CC7.4	• User entities are responsible for notifying the Company of any security incidents that are discovered.

SUBSERVICE ORGANIZATION AND COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

The Company uses Microsoft 365 as a subservice organization for infrastructure and data hosting services. The Company's controls related to the DIS Direct Service cover only a portion of the overall internal control for each user entity of the DIS Direct Service. The description does not extend to the infrastructure and data hosting services provided by the subservice organization. Section 4 of this report and the description of the system only cover the Trust Services Criteria and related controls of the Company and exclude the related controls of Microsoft 365.

Although the subservice organization has been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. CSOCs are expected to be in place at Microsoft 365 related to data encryption, physical security, environmental protection and software and infrastructure change management. Microsoft 365 data encryption controls should mitigate the risk of unauthorized access to customer data. Microsoft 365 physical security controls should mitigate the risk of unauthorized access to the hosting facility. Microsoft 365 environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variability. Microsoft 365 change management controls should mitigate the risk of unauthorized changes and discontinued functionality of the infrastructure and data hosting services provided to DIS Direct. DIS Direct does not develop software or manage infrastructure, and as such, software and infrastructure change management is the responsibility of the subservice organization.

The Company management receives and reviews the Microsoft 365 SOC 2 report annually. In addition, through its operational activities, Company management monitors the services performed by Microsoft 365 to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to Microsoft 365 management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the DIS Direct Service to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and related tests and results described in Section 4 of this report, taking into account the related CSOCs expected to be implemented at Microsoft 365 as described below.

Criteria	Complementary Subservice Organization Controls (CSOCs)
CC6.1	• Microsoft 365 is responsible for encrypting data at rest.
CC6.4	• Microsoft 365 is responsible for restricting data center access to authorized personnel. • Microsoft 365 is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC6.5	• Microsoft 365 is responsible for securely decommissioning and physically destroying production assets in its control.
CC7.2	• Microsoft 365 is responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers. • Microsoft 365 is responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • Microsoft 365 is responsible for overseeing the regular maintenance of environmental protections at data centers.
CC8.1	• Microsoft 365 is responsible for software development and infrastructure changes.

SPECIFIC CRITERIA NOT RELEVANT TO THE SYSTEM

There were no specific Security Trust Services Criteria as set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria) that were not relevant to the system as presented in this report.

SIGNIFICANT CHANGES TO THE SYSTEM

There were no changes that are likely to affect report users' understanding of how the DIS Direct Service is used to provide the service from August 1, 2024 to January 31, 2025.

REPORT USE

The description does not omit or distort information relevant to the DIS Direct Service while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to their particular needs.

Section IV: Description of Criteria, DIS Direct's Controls, Service Auditor Tests, and Results of Tests

This SOC 2 Type 2 Report was prepared in accordance with the AICPA Attestation Standards based on the criteria for a description of a service organization’s system set forth 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 for the period August 1, 2024 to January 31, 2025. This section of the report includes 2 tables:

Table 1: DIS Direct Controls Mapped to the Security Criteria

Table 2: Description of Tests of Controls, Service Auditor Tests, and Results of Tests

Table 1: DIS Direct Controls Mapped to the Security Criteria

CC1.0 - Control Environment		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC1.1	**REQ-7** **REQ-8** **REQ-9** **REQ-10** **REQ-11** **REQ-14**	The entity demonstrates a commitment to integrity and ethical values.
CC1.2	**REQ-3** **REQ-4**	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3	**REQ-2** **REQ-4** **REQ-15** **REQ-16**	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4	**REQ-12** **REQ-13** **REQ-14** **REQ-15**	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

CC1.0 - Control Environment		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC1.5	**REQ-7** **REQ-14** **REQ-15**	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

CC2.0 - Information and Communication		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC2.1	**REQ-4** **REQ-19** **REQ-20** **REQ-39**	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
CC2.2	**REQ-2** **REQ-13** **REQ-15**	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
CC2.3	**REQ-5** **REQ-6** **REQ-22**	The entity communicates with external parties regarding matters affecting the functioning of internal control.

CC3.0 - Risk Assessment		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC3.1	**REQ-17** **REQ-18**	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
CC3.2	**REQ-17** **REQ-19** **REQ-58** **REQ-59**	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.

CC3.0 - Risk Assessment		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC3.3	**REQ-17** **REQ-19**	The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4	**REQ-17** **REQ-19**	The entity identifies and assesses changes that could significantly impact the system of internal control.

CC4.0 - Monitoring Activities		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC4.1	**REQ-4** **REQ-19** **REQ-20** **REQ-23**	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
CC4.2	**REQ-4** **REQ-19** **REQ-20** **REQ-23**	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.

CC5.0 - Control Activities		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC5.1	**REQ-17** **REQ-20**	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
CC5.2	**REQ-17** **REQ-20**	The entity also selects and develops general control activities over technology to support the achievement of objectives.

CC5.0 - Control Activities

Criteria	Applicable Control Activities	Criteria Description
CC5.3	REQ-1 REQ-17 REQ-21 REQ-24 REQ-32 REQ-42 REQ-48 REQ-51 REQ-53	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

CC6.0 - Logical and Physical Access

Criteria	Applicable Control Activities	Criteria Description
CC6.1	REQ-25 REQ-26 REQ-28 REQ-33 REQ-34	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.
CC6.2	REQ-29 REQ-30 REQ-31	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.
CC6.3	REQ-29 REQ-30 REQ-31	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.

CC6.0 - Logical and Physical Access		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC6.4	**N/A: The Company's production environment is hosted at third-party data centers, which are carved out for purposes of this report.**	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.
CC6.5	**REQ-32** **REQ-33**	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.
CC6.6	**REQ-27** **REQ-37** **REQ-43**	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7	**REQ-39**	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.
CC6.8	**REQ-38** **REQ-39** **REQ-43**	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

CC7.0 - System Operations		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC7.1	**REQ-19**	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.
CC7.2	**REQ-39** **REQ-43**	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.
CC7.3	**REQ-39** **REQ-48**	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.

CC7.0 - System Operations		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC7.4	**REQ-43** **REQ-48** **REQ-49** **REQ-50**	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
CC7.5	**REQ-48** **REQ-49** **REQ-50** **REQ-58** **REQ-59**	The entity identifies, develops, and implements activities to recover from identified security incidents.

CC8.0 - Change Management		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC8.1	**N/A: The in-scope service uses Microsoft 365 wherein Microsoft 365 is responsible for software development and infrastructure management, hence this criterion is carved out for purposes of this report.**	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

CC9.0 - Risk Mitigation		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC9.1	**REQ-17** **REQ-48** **REQ-49** **REQ-58** **REQ-59**	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2	**REQ-22** **REQ-23**	The entity assesses and manages risks associated with vendors and business partners.

Table 2: Description of Tests of Controls, Service Auditor Tests, and Results of Tests

Control activities and test procedures performed in connection with determining the design and operating effectiveness of controls relative to the applicable Trust Services Criteria are described below.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-1	An Information Security Policy is documented and defines the information security rules and requirements for the service environment. The policy is version controlled, reviewed annually, approved by management, and communicated to authorized users.	Inspected the Information Security Policy and policy repository to determine that an Information Security Policy was documented, defined the information security rules and requirements for the service environment, was version controlled, reviewed annually, approved by management, and communicated to authorized users.	**No exceptions noted.**
REQ-2	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment.	Inspected the Information Security Policy to determine that management had established defined roles and responsibilities to oversee the implementation of the security and control environment.	**No exceptions noted.**
REQ-3	The Risk Committee is tasked with governance, oversight, and responsibilities relative to internal control. The Risk Committee includes members that are independent of the internal control function.	Inspected the Risk Committee charter to determine that the Risk Committee was tasked with governance, oversight, and responsibilities relative to internal control and the Risk Committee included members that were independent of the internal control function.	**No exceptions noted.**
REQ-4	The Risk Committee meets quarterly and maintains formal meeting minutes.	Inspected the Risk Committee meeting minutes for a sample of quarters to determine that the Risk Committee met quarterly and maintained formal meeting minutes.	**No exceptions noted.**
REQ-5	The MSA includes the communication of the Company's commitments to its customers.	Inspected the MSA template to determine that the Company's commitments were communicated to customers.	**No exceptions noted.**
REQ-6	Technical support resources related to system operations are provided on the Company's website.	Inspected the Company's website to determine that technical support resources related to system operations were provided on the Company's website.	**No exceptions noted.**

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-7	The Code of Conduct describes employee and contractor responsibilities and expected behavior regarding data and information system usage.	Inspected the Code of Conduct to determine that it described employee and contractor responsibilities and expected behavior regarding data and information system usage.	**No exceptions noted.**
REQ-8	Upon hire, employees acknowledge that they have read and agree to the Code of Conduct. The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No employees were hired during the period.	Inquired of management and inspected the employee listing to determine that the circumstances that warrant the operation of the control did not occur during the period.	**Not tested. No employees were hired during the period.**
REQ-9	The employee confidentiality agreement prohibits any disclosure of information and other data to which the employee has been granted access.	Inspected the employee confidentiality agreement to determine that it prohibited the disclosure of information and other data to which the employee or contractor had been granted access.	**No exceptions noted.**
REQ-10	Upon hire, employees acknowledge that they have read and agree to the confidentiality agreement. The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No employees were hired during the period.	Inquired of management and inspected the employee listing to determine that the circumstances that warrant the operation of the control did not occur during the period.	**Not tested. No employees were hired during the period.**

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-11	New employees offered employment are subject to background checks prior to their start date. The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No employees were hired during the period.	Inquired of management and inspected the employee listing to determine that the circumstances that warrant the operation of the control did not occur during the period.	**Not tested. No employees were hired during the period.**
REQ-12	New employees complete security awareness training upon hire. The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No employees were hired during the period.	Inquired of management and inspected the employee listing to determine that the circumstances that warrant the operation of the control did not occur during the period.	**Not tested. No employees were hired during the period.**
REQ-13	Employees complete security awareness training annually.	Inspected the training records for a sample of current employees to determine that employees completed security awareness training annually.	**No exceptions noted.**
REQ-14	Managers complete performance appraisals for direct reports annually.	Inspected the performance appraisals for a sample of employees to determine that managers completed performance appraisals for direct reports annually.	**No exceptions noted.**
REQ-15	Job descriptions are documented for employees supporting the service and include authorities and responsibilities in support of the system.	Inspected the job descriptions for a sample of employees supporting the service to determine that job descriptions were documented and included authorities and responsibilities in support of the system.	**No exceptions noted.**
REQ-16	An organization chart is documented and defines the organizational structure and reporting lines.	Inspected the organization chart to determine that an organization chart was documented and defined the organizational structure and reporting lines.	**No exceptions noted.**

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-17	A Risk Management Policy is documented and includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Management Policy to determine that a Risk Management Policy was documented and included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	**No exceptions noted.**
REQ-18	The Company specifies its objectives in its annual risk assessment to enable the identification and assessment of risks related to the objectives.	Inspected the risk assessment results to determine that the Company specified its objectives in its annual risk assessment to enable the identification and assessment of risks related to the objectives.	**No exceptions noted.**
REQ-19	A risk assessment is performed annually. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk assessment results to determine that a risk assessment was performed annually and, as part of this process, threats and changes to service commitments were identified, risks were formally assessed, and the risk assessment included a consideration of the potential for fraud and how fraud may have impacted the achievement of objectives.	**No exceptions noted.**
REQ-20	As part of its annual risk assessment, management selects and develops manual and IT general control activities that contribute to the mitigation of identified risks.	Inspected the risk assessment results to determine that as part of its annual risk assessment, management selected and developed manual and IT general control activities that contributed to the mitigation of identified risks.	**No exceptions noted.**

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-21	A Vendor Management Policy is documented and includes guidance on performing the following vendor management functions: - Requirements for the classification of third-party vendors - Requirements for the assessment of risks resulting from the procurement of third-party services - Annually reviewing critical third-party attestation reports or performing a vendor risk assessment	Inspected the Vendor Management Policy to determine that a Vendor Management Policy was documented and included guidance on performing the following vendor management functions: - Requirements for the classification of third-party vendors - Requirements for the assessment of risks resulting from the procurement of third-party services - Annually reviewing critical third-party attestation reports or performing a vendor risk assessment	**No exceptions noted.**
REQ-22	Formal agreements are in place with critical vendors. These agreements include commitments applicable to that entity.	Inspected the contracts for a sample of critical vendors to determine that formal agreements were in place with critical vendors and the agreements included commitments applicable to that entity.	**No exceptions noted.**
REQ-23	A vendor risk assessment is performed annually for all critical vendors to assess and manage risks associated with the service.	Inspected the vendor risk assessment results for a sample of critical vendors to determine that a vendor risk assessment was performed annually for all critical vendors to assess and manage risks associated with the service.	**No exceptions noted.**
REQ-24	An Access Control Policy is documented and includes guidance for performing the following system access control functions: - Provisioning users - Deprovisioning users - Access reviews and recertification - Restricting access based on separation of duties and least privilege	Inspected the Access Control Policy to determine that an Access Control Policy was documented and included guidance for performing the following system access control functions: - Provisioning users - Deprovisioning users - Access reviews and recertification - Restricting access based on separation of duties and least privilege	**No exceptions noted.**

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-25	Authentication to the following system components requires unique usernames and passwords: - Microsoft 365 - Firewall	Inspected the system configurations and observed login attempts to determine that authentication to the following system components required unique usernames and passwords: - Microsoft 365 - Firewall	**No exceptions noted.**
REQ-26	Passwords for the following system components are configured according to the Password Policy: - Microsoft 365 - Firewall	Inspected the Password Policy and compared to password configurations for the following system components to determine that passwords were configured according to the Password Policy: - Microsoft 365 - Firewall	**No exceptions noted.**
REQ-27	Access to production infrastructure is restricted to authorized users with valid multi-factor authentication (MFA) tokens.	Inspected the MFA configurations to determine that access to production infrastructure was restricted to authorized users with valid MFA tokens.	**No exceptions noted.**
REQ-28	Privileged access to the following system components is restricted to authorized users with a business need: - Microsoft 365 - Firewall	Inspected the system access listings, inquired of management, and compared each user's access privileges to their job role to determine that privileged access to the following system components was restricted to authorized users with a business need: - Microsoft 365 - Firewall	**No exceptions noted.**
REQ-29	Quarterly access reviews are conducted to help ensure that system access is restricted appropriately for the following system components: - Microsoft 365 - Firewall The review is documented, and access is modified or removed where applicable.	Inspected the access review results for a sample of quarters to determine that quarterly access reviews were conducted to help ensure that system access was restricted appropriately, the review was documented, and access was modified or removed where applicable for the following system components: - Microsoft 365 - Firewall	**No exceptions noted.**

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-30	Access to system components is based on job role, function, and requires a documented access request with manager approval prior to access being provisioned. The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No users were provisioned access to system components during the period.	Inquired of management and inspected system access listings to determine that the circumstances that warrant the operation of the control did not occur during the period.	**Not tested. No users were provisioned access to system components during the period.**
REQ-31	Access to system components is revoked within 24 hours of termination as part of the termination process. The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No employees and contractors were terminated during the period.	Inquired of management and inspected the employee and contractor listing to determine that the circumstances that warrant the operation of the control did not occur during the period.	**Not tested. No employees and contractors were terminated during the period.**
REQ-32	A Data Retention and Disposal Policy is documented and includes guidance for the secure retention and disposal of customer data.	Inspected the Data Retention and Disposal Policy to determine that a Data Retention and Disposal Policy was documented and included guidance for the secure retention and disposal of customer data.	**No exceptions noted.**
REQ-33	An inventory of production system assets is maintained by management.	Inspected the production system asset inventory to determine that an inventory of production system assets was maintained by management.	**No exceptions noted.**
REQ-34	Disk encryption is enabled on workstations.	Inspected the encryption configurations for a sample of workstations to determine that disk encryption was enabled on workstations.	**No exceptions noted.**

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-37	A software firewall is enabled on workstations.	Inspected the firewall configurations for a sample of workstations to determine that a software firewall was enabled on workstations.	**No exceptions noted.**
REQ-38	Anti-malware is installed on workstations.	Inspected the anti-malware configurations for a sample of workstations to determine that anti-malware technology was installed on workstations.	**No exceptions noted.**
REQ-39	A log management tool is utilized to monitor and identify security events and trends that may have a potential impact on the Company's ability to achieve its security objectives and generates alerts when security events occur.	Inspected the log management tool dashboard, configurations, and an example alert notification to determine that a log management tool was utilized to monitor and identify security events and trends that may have had a potential impact on the Company's ability to achieve its security objectives and generated alerts when security events occurred.	**No exceptions noted.**
REQ-42	A Vulnerability Management Policy is documented and includes guidance for performing the following vulnerability management functions: - Methods for identifying vulnerabilities and frequency - Assessing the severity of identified vulnerabilities - Prioritizing and implementing remediation or mitigation activities for identified vulnerabilities based on severity and defined timelines	Inspected the Vulnerability Management Policy to determine that a Vulnerability Management Policy was documented and included guidance for performing the following vulnerability management functions: - Methods for identifying vulnerabilities and frequency - Assessing the severity of identified vulnerabilities - Prioritizing and implementing remediation or mitigation activities for identified vulnerabilities based on severity and defined timelines	**No exceptions noted.**
REQ-43	Workstations are patched with a supported Operating System (OS) version to harden workstations against security threats.	Inspected the OS version configurations for a sample of workstations to determine that workstations were patched with a supported OS version to harden workstations against security threats.	**No exceptions noted.**

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-48	An Incident Response Policy is documented and includes guidance for detecting, responding to, and recovering from security events and incidents.	Inspected the Incident Response Policy to determine that an Incident Response Policy was documented and included guidance for detecting, responding to, and recovering from security events and incidents.	**No exceptions noted.**
REQ-49	The incident response plan is tested annually to assess the effectiveness of the incident response program.	Inspected the incident response plan test results to determine that the incident response plan was tested annually to assess the effectiveness of the incident response program.	**No exceptions noted.**
REQ-50	All incidents related to security are logged, tracked, evaluated, and communicated to affected parties by management until the Company has recovered from the incidents. The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No security incidents occurred during the period.	Inquired of management and inspected the security incident repository to determine that the circumstances that warrant the operation of the control did not occur during the period.	**Not tested. No security incidents occurred during the period.**
REQ-51	Hardening standards are documented and include guidance on baseline security requirements for production systems before deployment to the production environment.	Inspected the hardening standards to determine that hardening standards were documented and included guidance on baseline security requirements for production systems before deployment to the production environment.	**No exceptions noted.**
REQ-53	A Change Management Policy is documented and includes guidance for documenting, testing, reviewing, and approving changes to information systems.	Inspected the Change Management Policy to determine that a Change Management Policy was documented and included guidance for documenting, testing, reviewing, and approving changes to information systems.	**No exceptions noted.**

Control #	Applicable Control Activities	Service Auditor’s Tests	Results of Tests
REQ-58	A BC/DR plan is documented to support continuity and recovery of critical services and business processes after unexpected business interruptions.	Inspected the BC/DR plan to determine that a BC/DR plan was documented to support continuity and recovery of critical services and business processes after unexpected business interruptions.	**No exceptions noted.**
REQ-59	The BC/DR plan is tested annually to assess the effectiveness of management's readiness to respond to unexpected business interruptions.	Inspected the BC/DR plan test results to determine that the BC/DR plan was tested annually to assess the effectiveness of management's readiness to respond to unexpected business interruptions.	**No exceptions noted.**