Report on Description of DriveSavers, Inc.'s Data Recovery Services and the Suitability of the Design and Operating Effectiveness of Controls for the Period May 1, 2022 to April 30, 2023 Relevant to Security

SOC 2®

TABLE OF CONTENTS

I. INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of DriveSavers, Inc.:

Scope
We have examined DriveSavers Inc.'s ("DriveSavers" or "Company") accompanying description of its Data Recovery Services titled "Description of DriveSavers, Inc.'s Data Recovery Services" throughout the period May 1, 2022 to April 30, 2023 ("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 May 1, 2022 to April 30, 2023, to provide reasonable assurance that DriveSavers' 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*).

DriveSavers uses a subservice organization to provide managed IT services in support of its system. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at DriveSavers, to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents DriveSavers' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of DriveSavers' 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 DriveSavers, to achieve DriveSavers' service commitments and system requirements based on the applicable trust services criteria. The description presents DriveSavers' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of DriveSavers' 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
DriveSavers 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 DriveSavers' service commitments and system requirements were achieved. DriveSavers has provided the accompanying assertion titled "DriveSavers' Data Recovery Services" ("Description of DriveSavers, Inc.'s Data Recovery Services") about the description and the suitability of design and operating effectiveness of controls stated therein. DriveSavers 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. We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

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.

Description of tests of controls
The specific controls we tested and the nature, timing and results of those tests are presented in section VII.

Opinion
In our opinion, in all material respects,

a. The description presents DriveSavers' Data Recovery Services that was designed and implemented throughout the period May 1, 2022 to April 30, 2023, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period May 1, 2022 to April 30, 2023, to provide reasonable assurance that DriveSavers' 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 subservice organizations and user entities applied the complementary controls assumed in the design of DriveSavers' controls throughout that period.

c. The controls stated in the description operated effectively throughout the period May 1, 2022 to April 30, 2023, to provide reasonable assurance that DriveSavers' 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 DriveSavers' controls operated effectively throughout that period.

Restricted use
This report, including the description of tests of controls and results thereof in section VII, is intended solely for the information and use of DriveSavers, user entities of DriveSavers' Data

Recovery services during some or all of the period of May 1, 2022 to April 30, 2023, business partners of DriveSavers subject to risks arising from interactions with the Data Recovery services, 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.

IS Partners, LLC

IS Partners, LLC
Dresher, Pennsylvania
August 21, 2023

IS Partners, LLC
1668 Susquehanna Road
Dresher, PA 19025

215.675.1400 main office
215.259.7928 fax
ispartnersllc.com

II. DRIVESAVERS' MANAGEMENT ASSERTION

We have prepared the accompanying description of DriveSavers, Inc.'s ("DriveSavers" or "Company") Data Recovery services titled "Description of DriveSavers, Inc.'s Data Recovery services" throughout the period May 1, 2022 to April, 30, 2023 ("description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria"). The description is intended to provide report users with information about the Data Recovery services that may be useful when assessing the risks arising from interactions with DriveSavers' system, particularly information about system controls that DriveSavers 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*).

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

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

a) The description presents DriveSavers' Data Recovery services that was designed and implemented throughout the period of May 1, 2022 to April 30, 2023, in accordance with the description criteria.
b) The controls stated in the description were suitably designed throughout the period May 1, 2022 to April 30, 2023 to provide reasonable assurance that DriveSavers' 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 subservice organizations and user entities applied the complementary controls assumed in the design of DriveSavers' controls throughout that period.
c) The controls stated in the description operated effectively throughout the period May 1, 2022 to April 30, 2023, to provide reasonable assurance that DriveSavers' 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 DriveSavers' controls operated effectively throughout that period.

III. DESCRIPTION OF DRIVESAVERS, INC.'S DATA RECOVERY SERVICES

Company Background

Founded in 1985, DriveSavers Data Recovery Inc. (DriveSavers) is a data recovery firm serving all forms of businesses that require data recovery. DriveSavers provides trusted and proven data recovery technology solutions including recovery of RAID, NAS, SAN, tape and multi-disk systems.

Overview of the Services Provided

DriveSavers provides data recovery firm serving all forms of businesses that require data recovery. Their dedicated team of experienced enterprise engineers combines proprietary software and hardware tools with multi-terabyte systems to achieve amazing results, even from storage devices with mechanical failure or physical damage. The following manufacturers prefer DriveSavers for the recovery of their servers and storage devices: Dell, HP/Compaq, and Apple. Leading manufacturers authorize DriveSavers to open sealed drive mechanisms without voiding the original warranty.

Specific service offerings include:

Service Offering(s)	Service Description
Data recovery of	• RAID • NAS • SAN • TAPE • MULTI-DISK • CD • DVD • REMOVABLE MEDIA - THUMB DRIVES • HANDHELD (PDA's / IPODS / CELL PHONES / TABLETS) • DESKTOPS • LAPTOPS • DIGITAL CAMERAS • DIGITAL ARTS RECOVERY • FILE LEVEL AND DISK LEVEL ENCRYPTED DATA

DriveSavers has established a relationship with the following business partners for delivery of services:

Vendor Name	Service(s) Provided
Computer Services, Inc. (CSI)	Managed IT Services Provider

Products/services obtained from third-party business partners related to delivery of DriveSavers products/services to clients are supported by documentation outlining services provided by third party.

Data Type(s)
Electronic data involved with the delivery of DriveSavers Data Recovery, Inc.'s products/services is primarily public information. The exception to this statement is income information that is provided on the form 4506-T and social security verifications form both of which are completed by the consumer.

Principal Service Commitments and System Requirements

DriveSavers designs its processes and procedures related to its data recovery services to meet its clients' objectives. Those objectives are based on the service commitments that DriveSavers makes to user entities, the frameworks and methodologies that define sustainability measurement and reporting requirements, regulatory requirements that govern the provision of sustainability services, and the financial, operational, and compliance requirements that DriveSavers has established for the services.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other client 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 system that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role;
- Use of encryption technologies to protect client data both at rest and in transit;
- Confidentiality provisions regarding proprietary technical and business information of both DriveSavers and its customers;
- Staffing, hardware and software necessary to develop and operate all service and operations systems;
- Responsible for resolving inquiries made by user entities in accordance with the terms agreed to in the Master Services Agreement (MSA) and applicable schedules;
- Attainment of various Key Performance Indicators ("KPIs") and,
- Service level and performance requirements relating to system uptime.

In achieving its service commitments and system requirements, DriveSavers has implemented various controls to ensure Security such as:

- Centralize privilege management, adhering to the principle of least privilege,
- Monitor, alert, and raise actions to the service in real time,
- Apply a defense-in-depth approach with security controls,
- Protect data in transit and at rest with encryption, tokenization, and access control,
- Geographically separated data centers with controlled physical security,
- Vulnerability management program designed to identify and correct vulnerabilities within the environment in a timely manner,
- Incident response program designed to minimize the impact of incidents and protect resources, and

DriveSavers establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in DriveSavers' system policies and procedures, system design documentation, and Master Service Agreements with clients. 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 employees 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 DriveSavers' software services.

This report covers the system boundaries of the DriveSavers' system servers, applications and databases, including specific aspects of the service organization's infrastructure, software, people, procedures and data necessary to provide its services.

Components of the System
The system is comprised of the following five components:

- Infrastructure (systems and networks)
- Software (web application & utilities)
- People (Engineers, IT project managers, Product Manager)
- Procedures (automated and manual)
- Data (transactions streams, files, databases, and storage)

The following sections of this description define each of these five components comprising DriveSavers' system and other relevant aspects of DriveSavers' control environment, risk assessment process, information and communication systems, and monitoring controls.

Infrastructure

Facility
DriveSavers, Inc. maintains a secured headquarters in Novato, California. The facility is physically secured and environmentally controlled with card access badges, closed circuit television cameras, temperature and humidity controls, fire prevention and suppressions systems, intruder alarms and backup electrical power. DriveSavers is Department of Defense (DOD) Certified.

Building Security
All exterior doors remain locked at all times. DriveSavers employees are issued access control cards or FOBs to enter the building. Access to internal areas is granted on an as needed basis based upon employee's job function.

Visitors
All external entrances are locked, requiring visitors to DriveSavers Data Recovery Inc. to utilize a camera- controlled Intercom system to request access to the facility. All visitors must sign in at the reception deck and be issued a visitor's badge. Visitors are escorted by DriveSavers Data Recovery Inc. Services staff while onsite. Visitors are required to sign out when leaving the facility.

Restricted Areas
Within the building, the lab areas and IT network computer room have been designated as "Restricted" and require an additional level of security to access the area. All access points to Restricted Areas requiring proximity card access are logged.

Equipment
All equipment used in support of production operations is located within DriveSavers Data Recovery Inc. Services and managed by internal personnel resources. On an as-needed basis, hardware vendors will provide on-site and/or remote support and assistance for troubleshooting and ongoing maintenance activities. Categories of equipment include the following:

Communications Equipment
Routers, switches and other communication devices are installed within DriveSavers Data Recovery Inc. Services to manage data traffic internally within the facility and incoming/outgoing data transmissions.

Server(s)
Servers utilized by DriveSavers Data Recovery Inc. for production processing are a combination of physical servers and virtual servers utilizing VMWare / HyperV. Additional and replacement servers are purchased by DriveSavers Data Recovery Inc. from Fortune500 manufacturers.

User Computing Device(s)
Desktop and laptop workstations owned by DriveSavers Data Recovery Inc. Services are used for production processing purposes.

Network

Circuits
Connection to the Internet is dependent on following methods:

- T-1
- Cable

DriveSavers Data Recovery Inc. maintains redundant communications to the Internet for failover purposes. This redundant connection enters the server room through diverse communication channels.

Internal (Production) Network
Access to the internal network occurs via a wired connection based on TCP/IP protocol. DriveSavers Data Recovery Inc. Services maintains a network of wired routers, firewalls, switches, load balancers and VPN appliances providing network connectivity to five separate networks. DriveSavers Data Recovery Inc. has not implemented a wireless network for production or guest services.

Security Devices

Firewall
Connections to and from DriveSavers Data Recovery Inc. Services' networks are protected by firewalls that are hosted and managed internally.

DMZ
A demilitarized zone (DMZ) is used to separate publicly accessible servers from the trusted network. These DMZs only allow authorized traffic to pass in and out of the DMZ.

Remote Access
Capability to connect to the DriveSavers Data Recovery Inc. network remotely is accomplished via third- party software that creates a secure VPN tunnel.

Employees
DriveSavers Data Recovery Inc. employees that have a business need to connect remotely are required to establish the connection via a VPN session. Employees must obtain approval from the business unit manager of DriveSavers Data Recovery Inc. prior to being authorized to access the network remotely. Access is controlled by a security group in Active Directory. Employees are required to enter their username and password when initiating the VPN and provide an MFA authentication code.

Vendors
Remote access to the DriveSavers Data Recovery Inc. network is limited to the specific named vendor users. Access is controlled by DriveSavers Data Recovery Inc. and is only given when needed. Once the security system vendor is finished access is removed again.

Software

Software Administration

Software Inventory
DriveSavers Data Recovery Inc. has identified all business-critical applications including product name, developer, license number and related terms and maintains this information in a central repository.

License Administration
A copy of the executed license agreement is maintained by the IT Manager who is also responsible for ensuring compliance with license terms and use rights.

Maintenance / Support
Maintenance of Microsoft applications is included as part of the software licensing agreement.

Operating System(s) Software

Overview
Similar to equipment, operating system software that has been installed on production servers is administered by internal personnel resources. On an as-needed basis, software vendors will provide remote support and assistance for troubleshooting and software updates/patches.

Servers
DriveSavers Data Recovery Inc. Services has implemented and maintains current vendor supported operating system for Microsoft Windows server to support production and nonproduction operations.

User Computing Device(s)
Microsoft Windows operating system software has been installed on desktop and laptop workstations in support of production and nonproduction operations.

Security Software
Security software has been installed on servers and workstations to protect data and the underlying infrastructure from unauthorized access and activity within production and nonproduction systems and includes but is not limited to the following:

- Anti-Virus/Malware
- Intrusion Detection/Intrusion Prevention
- Event Monitoring
- Event Alerting
- Centralized Logging
- Web Filtering

System Utilities
Utilities to support production systems include but are not limited to the following:

- System Performance and Availability Monitoring Software
- Backup Software
- User Authentication & Identification (Physical & Logical)

People

DriveSavers Data Recovery Inc. Services Employees
DriveSavers Data Recovery Inc. has a staff of 85 full- and part-time employees that are assigned to various roles within the organization. Overall, the President is responsible for administration of DriveSavers Data Recovery Inc.

DriveSavers Data Recovery Inc. personnel resources that are assigned to one of the following functional business areas:

Business Function(s)	Responsibility
Information Technology	Oversees the installation and maintenance of the computer network and infrastructure
Data Recovery	Performs the data recovery of client's information
Security Compliance	Makes sure business is conducted in full compliance with all laws and regulations and maintains a safe and secure environment
Shipping	Arranges the collection and shipping of storage media from various courier services

IT Support Service
IT Support staff is responsible for troubleshooting issues reported by internal users, business partners and clients. The DriveSavers Data Recovery Inc. Help Desk is staffed from 6:00 AM through 5:00 PM Pacific Time, Monday through Friday, and no weekend staffing. Issues that are reported outside of this schedule are reviewed by IT personnel and prioritized and reacted to base on severity and the DriveSavers Data Recovery Inc. to the business.

Contracted Personnel
DriveSavers Data Recovery Inc. Services supplements current staff with contracted personnel resources when: 1) unique skills are not resident within DriveSavers Data Recovery Inc. Services or 2) deadlines cannot be met with existing employees.

Data

Client Data Administration

Data Classification
Data follows a classification schema that describes the security and handling of data.

Classifications include:

Classification	Description
Confidential	All customers' data is treated as confidential.

Overview
The company transmits and receives all client data externally via courier services for receiving and sending data using encryption technology whenever possible.

Processes and Procedures

Procedures related to Order Fulfillment Services are described in a sequence relevant to the Trust Principles and Criteria in scope of this engagement including:

Systems Security
Management has developed and communicated procedures relevant to systems security to employees, clients and external business partners to restrict logical access to the DriveSavers Data Recovery Inc. Services system. Procedures are reviewed annually by functional business area leads with changes approved by management. These procedures cover the following key elements of systems security:

- Selection, documentation, and implementation of security controls related to:
  - Network(s)/Security Device(s)/Server(s)/Workstation(s)
  - Database(s)/Application System(s)
  - Facilities
- Systems Security Configuration/Patching
- Managing Systems User Account Access
- Monitoring Systems Security-related Activity

IV.

IV. OTHER RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION SYSTEMS, AND MONITORING CONTROLS

Control Environment

Organization Structure

The organization structure of DriveSavers provides the overall framework for establishing, directing, and monitoring strategic objectives. The overall hierarchy and individual reporting relationships have been established to support and promote operational independence between functions areas of the organization and underlying roles and responsibilities.

Management Philosophy

DriveSavers operates in an industry where risk management, control, and reputation are critical. The company has instituted policies and programs to promote an appropriate control environment in support of customer needs. The primary elements of DriveSavers control environment are demonstrated by management's philosophy and operating style; management's integrity and ethical values; the method of assignment of authority, responsibility and close supervision; human resources, skills and commitments to competence; information risk management; and the company's organizational structure, reporting mechanisms and segregation of duties; management's controls for monitoring and following up on performance, including the results of internal controls procedures; and management's response to various external influences that affect the company's operations such as examinations by independent third parties.

Strategic Planning

The control environment sets the tone of the organization, influencing the control consciousness of all personnel. It is the foundation for all other components of internal control, providing discipline and structure. Through the control environment, management influences the way business activities are structured, objectives are established, and risks are assessed. It influences control activities, information and communication systems, and monitoring procedures. DriveSavers managerial culture instills a companywide attitude of integrity, security, and control consciousness, and sets a positive "tone at the top". Management has established methods that foster shared values and teamwork in pursuit of these objectives.

Risk Assessment

DriveSavers has placed into operation an annual risk assessment program to identify and manage risks that could affect DriveSavers ability to properly control its assets and to serve its customers. This program requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address and mitigate those risks. Company meetings include a discussion of these matters. DriveSavers has identified various internal and external risk factors. DriveSavers has assessed the probable impact of the events in their probability of occurrence and has implemented various measures designed to manage those risks. Risks that are considered during management's formal and informal risk assessment activities may include consideration of the following events:

- Changes in operating environment
- New personnel

- New or changed information systems
- Rapid growth/decline
- New business models, products, or activities
- Corporate restructurings
- Expanded operations

Information and Communication

DriveSavers has implemented various methods of communication to help ensure employees understand their individual roles and internal controls, and to facilitate the timely dissemination of significant events. Time sensitive information is communicated directly to employees and via e-mail. Employees are required to adhere to DriveSavers policies and procedures to ensure that records and other documents are maintained accurately, securely and completely. DriveSavers facilitates the effective flow of information through key business performance metrics and system related metrics. There is also an "open door" policy that allows employees direct access to the management team.

Upper management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. This includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to an appropriate higher level within the company. DriveSavers management believes that open communication channels help ensure that exceptions are reported and acted on. For that reason, formal communication tools such as organization charts and acceptable use policies are in place. Management's communication activities are made electronically, verbally, and through the actions of management.

Monitoring Controls

Monitoring requires a clear understanding of processes and their relationships to key risks, progress towards addressing the highest rated risks, and ongoing risk assessment and effectiveness of managing risk. DriveSavers management performs monitoring activities in order to continuously assess the quality of internal controls over time. Monitoring activities are used to initiate corrective actions through department meetings, client conference calls, and informal notifications. Monitoring activities are conducted on a continuous basis and necessary corrective actions are taken as required to correct deviations from company policy and procedures.

Management's close involvement in operations helps to identify significant variances from expectations regarding internal controls. Upper management immediately evaluates the specific facts and circumstances related to any suspected control breakdowns. A decision for addressing any control weaknesses is made based on whether the incident was isolated or requires a change in the company's procedures or personnel.

Additionally, DriveSavers personnel monitor the quality of internal control and operating performance as a normal part of their business activities. Key business metrics and IT metrics are maintained to facilitate this monitoring process. Exceptions and deviations to normal business activity are reviewed by management and sufficiently resolved. Management strives to provide accurate information and tools to employees to facilitate compliance with policies and procedures that help manage risk.

Control Activities

Policy Statements, Standards & Procedures

DriveSavers has established operating policies and procedures for use by employees. The management committee maintains policies and procedures related to system administration, use, controls and operating procedures. Policies and procedures are updated as warranted and appropriate personnel are notified when policy or procedure has changed.

Personnel Administration

Management of DriveSavers Data Recovery Inc. has a strong commitment to recruit, develop, and retain competent personnel to execute the business plan to achieve business and control objectives. Most staff positions are filled through general solicitation or employee referrals. Management positions are commonly filled through employee performance growth and referrals. Employment with DriveSavers Data Recovery Inc. is "at will" and is stated in the employment application.

Candidates for open positions are interviewed and hired based on their qualifications to satisfy the requirements of the position as outlined in the job description. DriveSavers Data Recovery Inc. maintains documentation for each employee in a personnel file including:

- Identification of Department
- Employment Application
- Background Check Consent Form/Results
- Acknowledgement of receipt of the Employee Handbook including Workplace Rules

Employee Separation

DriveSavers Data Recovery Inc. has established a checklist that identifies steps associated with the employee termination process. The checklist addresses both voluntary resignations and involuntary terminations. Completion of the checklist and all separation related activities is the responsibility of the business unit manager including notifying IT to disable/remove user accounts, retrieving physical security access devices and DriveSavers Data Recovery Inc.-owned technology assets.

Contracted/Temporary Personnel

Contracted and temporary personnel resources used to satisfy short-term staffing needs and specific project requirements must be approved by the project manager and HR department.

System(s) Development & Change Management

DriveSavers requires that internal changes to its systems be documented and approved by management. Changes are scheduled to reduce disruptions. The individual migrating the change into production is approved by management. Documentation of changes and associated authorizations are retained in a centralized location for ease of administration. Internal changes are moved to production by authorized personnel. Management reviews the access to production systems for appropriateness of personnel.

System(s) Account Management

DriveSavers maintains corporate policies, procedures, and controls to facilitate logical security. The company performs a risk assessment to identify potential business and security risks and implements measures to reduce the risks. There is a Corporate Code of Conduct that each employee

signs, along with policies for security, confidentiality, nondisclosure, and acceptable use of systems. There are security administration procedures that require management's authorization for any add, change, and delete of user accounts. Segregation of IT duties is achieved by the ongoing review of employee access rights. DriveSavers employees are authorized by management to access information of their systems and their clients' systems based upon their job requirements. Best practices are employed by DriveSavers for password administration. Passwords are confidential, not shared, are complex, and must be changed after a prescribed time period. Passwords are required to have a sufficient number of characters. Default passwords are changed. DriveSavers uses a virtual private network (VPN) and firewalls for secure access through the Internet. Remote users are authorized by management.

Data Backup and Recovery

DriveSavers uses automated systems for scheduling tasks such as backups. Backups are taken on a nightly basis, with the backup media stored in a secure off-site facility. Backup logs are monitored to ensure completeness of processing. The company periodically tests the backup media to facilitate its recoverability.

Physical Security and Environmental Controls

The facility is physically secured and environmentally controlled with card access badges, closed circuit television cameras, temperature and humidity controls, fire prevention and suppressions systems, intruder alarms and backup electrical power. DriveSavers is Department of Defense (DOD) Certified.

Security Monitoring & Response

Remote user access is logged and reviewed monthly. DriveSavers monitors their security stringently. Intrusion prevention and detection systems are installed and continuously monitored. Security alerts are identified, escalated, and communicated. Remedial action is taken if necessary. DriveSavers employs automated preventative controls to minimize disruptions from computer viruses and spyware. The network is periodically assessed by an independent third party for system configuration errors and vulnerabilities. Additionally, DriveSavers external audit team completes regular self-assessments of DriveSavers controls.

Problem Management / Notification

DriveSavers computers at the headquarters are processing their operations on a 24/7/365 basis. Processes are in place to minimize interruptions in service. A help desk is maintained via the MAC and PC engineering group, along with a system that tracks the status and resolution of calls to the help desk and reported problems.

Changes to the System During the Period

There were no changes that are likely to affect report users' understanding of how the DriveSavers Data Recovery system is used to provide the service during the period from May 1, 2022, through April 30, 2023.

Disclosure of Security Incidents **–** DriveSavers has a well-established incident management program that consists of a documented incident response program.

The company diligently responds to alerts received from various monitoring tools deployed at the perimeter of the network, within the network and applications. Throughout the period, DriveSavers investigated all incidents related to its systems and applications performance and security controls. These incidents were promptly responded to and mitigated.

None of the incidents led to an actual data breach or were significant enough to trigger external communications. Examples of such incidents include file integrity monitoring false positives due to configuration changes (by design) and malware detected and immediately quarantined on a workstation.

V. SUBSERVICE ORGANIZATIONS

DriveSavers uses subservice organizations to perform certain functions that support the delivery of services. The scope of this report does not include the controls and related Trust Services Criteria at the subservice organization. The following is a description of the services provided by the subservice organization and the controls that are expected to be implemented:

Subservice Organization	Services Provided
Computer Services, Inc. (CSI)	Managed IT Services Provider

Below are the applicable trust services criteria that are impacted by the subservice organization and the controls expected to be implemented at the subservice organizations to meet the applicable criteria:

Applicable Trust Services Criteria	Subservice Organization Controls Expected to be Implemented to Meet the Applicable Trust Services Criteria
CC 3.1 ***The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.***	• An assessment of DriveSavers' risks is performed and conducted on an annual basis.
CC 3.2 ***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.***	• An assessment of DriveSavers' risks is performed and conducted on an annual basis.
CC 4.1 ***The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.***	• Monitoring alerts from the independent third party are reviewed by the chief information security officer on a daily basis.
CC 6.4 ***The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.***	• Environmental controls for the protection of DriveSavers' servers hosting the DriveSavers Recovery Services.
CC 7.1 ***To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.***	• Internal and external vulnerability scans are performed annually and reviewed by management.

Monitoring of Subservice Organizations

To help ensure that DriveSavers maintains security controls regarding the security of its data, DriveSavers performs on-going monitoring of its subservice organizations. The process includes obtaining and reviewing the annual independent audit reports (SOC2) provided by the subservice organization, which detail the controls in place to mitigate the risk associated with engaging with the subservice organizations

Relationships with critical vendors are reviewed on an on-going basis and are managed by the Company's IT vendor process.

VI. COMPLEMENTARY USER ENTITY CONTROLS

DriveSavers' controls were designed with the assumption that certain complementary controls will be placed in operation at user organizations. In certain instances, the application of specific controls at user organizations is necessary to achieve certain trust services criteria included in this report.

The following list outlines controls that should be in operation at user organizations to complement the controls listed in section VII. The list does not represent a comprehensive set of all controls that should be employed by user organizations. User organizations' auditors should consider whether the following controls have been placed in operation at user organizations:

Clients are responsible for:

- Understanding and complying with their contractual obligations to DriveSavers.
- Ensuring the confidentiality of any user IDs and passwords given to DriveSavers.
- Maintaining their own system(s) of record.
- Determining whether DriveSavers security infrastructure is appropriate for its needs and for notifying the service organization of any requested modifications.
- Complying with DriveSavers Data Recovery Inc. process.
- Developing their own disaster recovery and business continuity plans that address their inability to access or utilize DriveSavers services.
- Defining backup schedules and backing up their data.
- Providing redundant infrastructure as needed.
- Defining and implementing operating system, application, and database controls.

VII. INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria References
DS-1	Access to the DriveSavers' network and tools is approved by the IT manager or the chief information security officer.	Obtained and inspected a completed access request for a randomly selected new hire and determined that access to the DriveSavers network and tools was approved by the IT manager or the Chief Information Security Officer.	No exceptions noted.	CC6.1
DS-2	All employees (full-time, part-time, and/or contractor) must pass an initial criminal background check before being employed.	Obtained and inspected a completed background check for a randomly selected sample of new hire and determined all employees must pass an initial criminal background check before being employed.	No exceptions noted.	CC1.1
DS-3	An assessment of DriveSavers' risks is performed on an annual basis, and documented procedures, processes, and controls for reducing the identified risks.	Obtained and inspected the annual risk assessment and determined that the assessment was performed on an annual basis. Obtained and inspected the Information Security policies and determined that procedures, processes and controls were documented for reducing the identified risks.	No exceptions noted.	CC3.1, CC3.2, CC9.1
DS-4	Annual access review of employees' access is performed to verify employee is still active and access is restricted based on job functions.	Obtained and inspected the access review ticket and determined that annual access reviews of employee's access was performed to verify employee is still active and access is restricted based on job functions.	No exceptions noted.	CC6.3
DS-5	Antivirus software is configured to receive updated virus signatures in real-time.	Observed and inspected the antivirus configurations and determined that antivirus signatures were updated in real-time.	No exceptions noted.	CC6.8
DS-6	Antivirus software is installed on workstations, laptops, and servers supporting such software.	Obtained and inspected the installed antivirus software for sampled workstations and determined that antivirus software was installed on workstations, laptops, and servers supporting such software.	No exceptions noted.	CC6.8, CC7.1

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria References
DS-7	Application Development changes are documented, tested, and approved.	Obtained and inspected the List of all Application Changes during the period and determined that the Application Development Changes were documented, tested, and approved.	No exceptions noted.	CC8.1
DS-8	At Monthly Management Meetings, the need for additional resources and skills are discussed in order to achieve business objectives.	Obtained and inspected a sample of meeting minutes and determined that at the Monthly Management Meetings, the need for additional resources and skills were discussed in order to achieve business objectives	No exceptions noted.	CC1.4, CC3.3
DS-9	At the Monthly Management Meetings, management discuss the monthly statistics from the IT service provider.	Obtained and inspected a sample of meeting minutes and determined that at the Monthly Management Meetings, management discuss the monthly statistics from the IT service provider.	No exceptions noted.	CC2.1, CC7.1
DS-10	At the Monthly Management Meetings, management evaluates the detail graphs and spreadsheets about the business operations and performances.	Obtained and inspected a selection of management meeting minutes and determined that management evaluates the detail graphs and spreadsheets about the business operations and performances.	No exceptions noted.	CC3.3
DS-11	At the Monthly Management Meetings, management evaluates the need for changes and re-alignment of the organization structure and reporting.	Obtained and inspected a selection of meeting minutes and determined that at the Monthly Management Meetings, management evaluated the need for changes and re-alignment of the organization structure and reporting.	No exceptions noted.	CC1.2, CC1.3, CC3.3
DS-12	Backout plans are established for each infrastructure change if the event of a failure.	Obtained and inspected ticket information for a selection of system changes during the audit period and determined that back out plans were established for each implementation in the event of a failure.	No exceptions noted.	CC8.1

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria References
DS-13	Backup alerts are monitored to ensure the completeness of the backup process.	Obtained and inspected the backup schedules and alerts for different critical systems and determined that backup alerts were monitored to ensure the completeness of the backup process.	No exceptions noted.	CC7.2
DS-14	Backup frequency (e.g. daily, weekly, and monthly) and type (e.g. full or incremental) of backup is performed using an automated system.	Obtained and inspected the backup schedules for different critical systems and determined that the backup frequency and type of backup was performed using an automated system.	No exceptions noted.	CC7.2
DS-15	Backup media are encrypted during creation.	Observed and inspected the backup encryption too and determined that backup media are encrypted during creation.	No exceptions noted.	CC6.7
DS-16	Change requests are logged in the ticketing system and tracked through to implementation.	Observed and inspected the Change Ticketing Tool and determined that Change requests were logged in the ticketing system and tracked through to implementation.	No exceptions noted.	CC8.1
DS-17	Changes are moved into production only by authorized individuals once approval of tests and implementation plans are obtained. Developers do not maintain access to deploy their own changes.	Observed and inspected the Application Development Segregation of Duties procedures in action and determined that changes are moved into production only by authorized individuals once approval of tests and implementation plans were obtained.	No exceptions noted.	CC8.1
DS-18	DriveSavers conducts an annual review of all security policies and procedures.	Obtained and inspected the Company's Information Security policy and Operational Meeting minutes and determined that DriveSavers conducts and annual review of all security policies and procedures.	No exceptions noted.	CC1.5, CC5.3

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria References
DS-19	DriveSavers' employees attend annual security awareness training and policy compliance. Record of attendance is retained through a tracking tool.	Obtained and inspected the training agenda for annual training and determined it included security awareness topics. Obtained and inspected the training tracking document and determined that all employees attended annual security awareness training.	No exceptions noted.	CC1.4
DS-20	DriveSavers has its organizational structure, reporting lines, authorities, and responsibilities defined in an organization chart.	Obtained and inspected the Organizational Chart and determined that DriveSavers' has its organizational structure, reporting lines, authorities, and responsibilities defined in an organization chart.	No exceptions noted.	CC1.3
DS-21	DriveSavers has provided descriptions of the drive recovery service(s) and plan(s) that DriveSavers offers on its external website.	Observed and inspected the content of the external website and determined that description of the drive recovery service(s) and plan(s) were on the external website.	No exceptions noted.	CC2.3
DS-22	DriveSavers performs an annual review of user accounts to confirm all personnel require access to perform their job functions. The annual review is performed to verify employees are still active.	Obtained and inspected the Physical Access Review and determined DriveSavers performed an annual review of user accounts to confirm all personnel require access to perform their job functions. The annual review was performed to verify employees are still active.	No exceptions noted.	CC6.1
DS-23	DriveSavers' security commitments regarding the service are included in the statement of work.	From a sample of customers during the audit period, obtained and inspected evidence of signed Statement of Work and determined DriveSavers' security commitments regarding the service are included in the statement of work.	No exceptions noted.	CC2.3
DS-24	During the ongoing risk assessment process and the periodic planning and budgeting processes, infrastructure, data, software, and procedures are evaluated for needed changes.	Obtained and inspected the risk assessment results and determined that changes to infrastructure, data, software, and procedures were documented in the annual IT Risk Assessment.	No exceptions noted.	CC3.4, CC9.1

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria References
DS-25	Employee access to protected resources is created or modified based on an authorized request from management.	Obtained and inspected request access documentation for a selection of new hires during the reporting period and determined that access was approved based on an authorized request by management.	No exceptions noted.	CC6.2, CC6.3
DS-26	Entity policies prohibit the transmission of sensitive information over the Internet or other public communications paths (for example, e-mail) unless it is encrypted.	Obtained and inspected the DriveSavers' Information Security Policy and determined that Entity policies prohibit the transmission of sensitive information over the Internet or other public communications paths (for example, e-mail) unless it is encrypted.	No exceptions noted.	CC6.7
DS-27	Every employee has a unique user account name and a password on the domain.	Obtained and inspected a user listing from the domain and determined that every employee had a unique user account name and a password on the domain.	No exceptions noted.	CC6.1
DS-28	Every employee has a unique user account name and a password to the CRM application.	Obtained and inspected user listing from the CRM application and determined that every employee had a unique user account and a password on the CRM application.	No exceptions noted.	CC6.1
DS-29	External access by employees is permitted through an encrypted virtual private network (VPN) connection using multi-factor authentication to gain access to the domain.	Observed and inspected the user listing and determined that employees used encrypted VPN connections to connect externally. Observed and inspected the VPN-MFA Configurations and determined that employees utilized multi-factor authentication to connect externally.	No exceptions noted.	CC6.1, CC6.6
DS-30	External points of connectivity are protected by the firewall configurations in place.	Observed and inspected the Network Firewall in place and determined that external points of connectivity were protected by the firewall configurations in place.	No exceptions noted.	CC6.6

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria References
DS-31	External users are informed of incidents in a timely manner and advised of corrective measure to be taken on their part.	Obtained and inspected the Information Security policy and determined external users were informed of incidents in a timely manner and advised of corrective measure to be taken on their part. Inquired with management and determined that no security incidents occurred during the audit period.	Unable to Conclude.	CC7.4
DS-32	For high severity incidents, a root cause analysis is prepared and reviewed by operations management. Based on the root cause analysis, change requests are prepared and the entity's risk management process and relevant risk management data is updated to reflect the planned incident and problem resolution.	Obtained and inspected the Information Security policy and determined that in the event of high severity incidents, a root cause analysis was prepared and reviewed by operations management. Inquired with management and determined that no security incidents occurred during the audit period.	Unable to Conclude.	CC7.5
DS-33	For items assessed, the risk assessment includes identification of business criticality; data sensitivity; relevant threats assessed; inherent and residual risk for each threat assessed; and identification of relevant business impact areas for each threat (financial, legal, compliance, reputation, and operations).	Obtained and inspected the IT Risk Assessment and determined that for items assessed, the risk assessment included identification of: business critically, data sensitivity, relevant threats assessed, inherent and residual risk for each threat assessed, and identification of relevant business impact areas for each threat.	No exceptions noted.	CC9.1
DS-34	Hard drives on laptops are encrypted.	Obtained and inspected the sample of laptops and determined that the hard drives were encrypted.	No exceptions noted.	CC6.7
DS-35	Identified risks are rated using a risk evaluation process and ratings are reviewed by management annually.	Obtained and inspected a sample of meeting minutes and determined that at the Monthly Management Meetings, identified risks are rated using a risk evaluation process and ratings are reviewed by management.	No exceptions noted.	CC3.1

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria References
DS-36	Identified risks are rated using a risk evaluation process and ratings are reviewed by management at the Monthly Management Meeting.	Obtained and inspected a sample of meeting minutes and determined that at the Monthly Management Meetings, identified risks are rated using a risk evaluation process and ratings are reviewed by management.	No exceptions noted.	CC3.2, CC3.3
DS-37	Infrastructure change requests must be reviewed and approved by the management. Changes are prioritized by management.	Obtained and inspected a list of server changes and determined that Infrastructure change requests must be reviewed and approved by the management. Changes are prioritized by management.	No exceptions noted.	CC8.1
DS-38	Internal and external vulnerability scans are performed annually by an independent third party. The reports from the scans are reviewed by management.	Obtained and inspected the internal and external vulnerability scans and determined that Internal and external vulnerability scans are performed annually by an independent third party. Obtained and inspected the internal and external vulnerability scan review tickets and determined that internal and external scans were reviewed by management.	No exceptions noted.	CC5.1, CC5.2, CC7.1
DS-39	Job postings outline the minimum experience and training requirements for the posting.	Obtained and inspected job postings for all positions and determined that minimum experience and training requirements are defined.	No exceptions noted.	CC1.4
DS-40	Management approval to add, change, or remove access to a user account (i.e. employee, temporary employee, and/or contractor) is required. The user account access is consistent with the level required to perform the daily job duties.	Obtained and inspected request access documentation for a selection of new hires during the reporting period and determined that access was approved. Obtained and inspected a request access documentation for a selection of terminations and determined that access was removed.	No exceptions noted.	CC6.2, CC6.3, CC6.5

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria References
DS-41	At monthly management meetings, management evaluates the effectiveness of the Company's IT controls.	Obtained and inspected a sample of meeting minutes and determined that at the Monthly Management Meetings, management evaluated the effectiveness of the Company's IT controls.	No exceptions noted.	CC2.1, CC3.2, CC3.3, CC3.4, CC4.1, CC4.2, CC5.1, CC5.2
DS-42	Management monitors internal analytics on Company metrics on an on-going basis.	Observed and inspected the Company Metrics Monitoring Tool and determined that management monitors internal analytics on Company metrics on an on-going basis.	No exceptions noted.	CC2.1
DS-43	Monitoring alerts from the independent third party are reviewed by the chief information security officer. Daily reports are provided via e-mail.	Obtained and inspected a sample of Monthly Managed Services reports and determined that the monitoring alerts from the independent third party were reviewed by the Chief Information Security Officer.	No exceptions noted.	CC4.1, CC7.1, CC7.3
DS-44	Notification of physical access to the facility by visitors is sent to all employees.	Obtained and inspected a notification of a visitor to the facility to determine that a notification was sent to all employees.	No exceptions noted.	CC6.4
DS-45	On emergency changes, associated documentation and approvals are required after the change has been implemented.	Obtained and inspected the Change Management policy and determined that a policy around emergency changes was documented and established. Inquired of management and determined that no emergency changes occurred during the audit period.	Unable to conclude.	CC8.1

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria References
DS-46	Operations personnel follow defined protocols in the Information Security Policy for evaluating reported events.	Obtained and inspected the Information Security policy and determined policies and procedures were documented and established for evaluating reported events.	No exceptions noted.	CC7.3, CC7.4, CC7.5
DS-47	Password settings have been configured to include complex passwords, a sufficient minimum number of password characters, invalid login restriction, and automatic change password after a set time.	Observed and inspected the domain password policy and determined that password settings were configured to include complex passwords, a sufficient minimum number of password characters, invalid login restriction, and automatic change password after a set time. Observed and inspected the CRM Application Password Configuration and determined that password settings are configured to include complex passwords, a sufficient minimum number of password characters, invalid login restriction, and automatic change password after a set time.	No exceptions noted.	CC6.2
DS-48	Personnel are required to read and accept the approved policies and procedures upon their hire.	Obtained and inspected signed acknowledgement form for a selection of new hires and determined personnel were required to read and accept the approved policies and procedures upon their hire.	No exceptions noted.	CC1.1, CC2.2
DS-49	Personnel are required to read and accept the code of conduct upon their hire.	Obtained and inspected acknowledgement forms for a selection of new hires during the reporting period and determined that employees read and accepted the code of conduct. Obtained and inspected the DriveSavers' Acceptable Use policy and determined that Code of Conduct was included in the form.	No exceptions noted.	CC1.1, CC5.3

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria References
DS-50	Personnel are required to read and accept the corporate Acceptable Use policy upon their hire.	Obtained and inspected signed Acceptable Use form for a selection of new hires and determined personnel were required to read and accept the approved policies and procedures upon their hire.	No exceptions noted.	CC1.1
DS-51	Personnel are required to read and sign nondisclosure of information agreement upon their hire.	Obtained and inspected a signed non-disclosure agreement for a selection of new hires and determined personnel were required to read and sign non-disclosure of information agreement upon their hire.	No exceptions noted.	CC2.2
DS-52	Personnel follow defined protocols outlined in the Information Security Policy for escalating reported security events.	Obtained and inspected the Information Security Policy and determined that personnel follow defined protocols outlined for escalating reported security events.	No exceptions noted.	CC4.1
DS-53	Physical Access to employees is administered based on the roles and responsibilities of the employee.	Obtained and inspected a list of employees with access to DriveSavers with proximity cards and determined that physical access to employees is administered based on the roles and responsibilities of the employee.	No exceptions noted.	CC6.4
DS-54	Physical access to sensitive areas of the facility is reviewed by management on an annual basis.	Obtained and inspected the review of user access and determined that Physical access to sensitive areas of the facility was reviewed by management on an annual basis.	No exceptions noted.	CC6.4
DS-55	Policies include encryption requirements based on data classification.	Obtained and inspected the Information Security policy and determined encryption requirements based on data classification was documented and established.	No exceptions noted.	CC6.7

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria References
DS-56	Privileged access to the CRM application is restricted solely to users with Database administration responsibilities.	Observed and inspected the user listing from the CRM application and determined that privilege access to the CRM application was restricted based on Database administration responsibilities.	No exceptions noted.	CC6.1
DS-57	Privileged access to the domain is restricted solely to users with IT responsibilities.	Observed and inspected the user listing from the domain and determined privileged access to the domain was restricted solely to users with IT responsibilities.	No exceptions noted.	CC6.1
DS-58	Procedures documents for problem management processes, which include responsibility for reporting problems (and the process for doing so).	Obtained and inspected the Information Security Policy and determined that a problem management process, which include responsibility for reporting problems is in place.	No exceptions noted.	CC2.2, CC2.2, CC7.2
DS-59	Resolution of security events (incidents or problems) is reviewed at the monthly management meeting.	Obtained and inspected the Monthly Manager Meeting Minutes and determined that resolution of security events was reviewed at the monthly management meeting.	No exceptions noted.	CC7.3
DS-60	Roles and responsibilities of the board, management, users, vendors, and others are defined in the Information Security Policy.	Obtained and inspected the Information Security Policy and determined that the Roles and responsibilities of the board, management, users, vendors, and others were defined.	No exceptions noted.	CC1.2, CC1.3, CC1.5

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria References
DS-61	Shared user accounts are prohibited within the domain/CRM without a valid business case.	Observed and inspected the list of admins and the admin type access on the CRM application with the name of the account and determined that shared user accounts are prohibited within the CRM without a valid business case. Observed and inspected the domain admins and the domain admins type access on the domain with the name of the account and determined that Shared user accounts were prohibited withing the domain without a valid business case. Obtained and inspected the list of all user accounts names on the domain and all user accounts on the CRM application and determined that shared user accounts were prohibited within the domain and CRM without a valid business case.	No exceptions noted.	CC6.2
DS-62	Spam filter software is implemented to prevent system vulnerabilities and malicious code.	Observed and inspected the filter software configuration and determined that spam filter software was implemented to prevent system vulnerabilities and malicious code.	No exceptions noted.	CC6.8
DS-63	The Card-based access system logs all attempts to enter the facility.	Observed and inspected the security logs and determined that card-based access system logged all attempts to enter the facility.	No exceptions noted.	CC6.4
DS-64	The Company's Information Security Policy is available to all employees via the Company's HR Wiki.	Observed and inspected the Company HR Wiki and determined that the Company's Information Security Policy was available to all employees via the Company's HR Wiki.	No exceptions noted.	CC2.2
DS-65	The Information Security Policy outlines sanctions for employee misconduct.	Obtained and inspected the Information Security Policy and determined that DriveSavers' outlines sanctions for employee misconduct.	No exceptions noted.	CC5.3

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria References
DS-66	The Information Security Policy outlines the Executive Committee responsibilities to oversee the strategic direction, plans, budgets, and the daily operations of the company.	Obtained and inspected the Information Security Policy and determined that the Executive Committee responsibilities to oversees the strategic direction, plans, budgets, and the daily operations of the company were outlined.	No exceptions noted.	CC1.2, CC1.3
DS-67	Transmission of Company data requires an encrypted connection (TLS, SFTP, SSL, etc...)	Observed and inspected the TLS procedures in place and determined that transmission of company data requires an encrypted connection.	No exceptions noted.	CC6.7
DS-68	Upon termination, a notification of a terminated employee for whose access is to be removed is sent to the help desk. The notification is used to remove physical and logical access.	Obtained and inspected service tickets for a sample of terminated employees and determined that physical and logical access was removed after notification was sent from the help desk.	No exceptions noted.	CC6.2, CC6.3, CC6.5
DS-69	Upon termination, physical access is termination in a timely manner.	Obtained and inspected service tickets for a sample of terminated employees and determined upon termination, physical access was terminated in a timely manner.	No exceptions noted.	CC6.4, CC6.5
DS-70	Users are required to provide proper identification prior to password reset.	Obtained and inspected all password resets during the reporting period and determined that users were required to provide proper identification prior to password reset.	No exceptions noted.	CC7.2
DS-71	Vendor due diligence documentation is collected on an annual basis to evaluate the managed services provider(s) ability to support the organization.	Obtained and inspected due diligence documentation collected from the managed service provider and determined that the managed service provider was evaluated on an annual basis.	No exceptions noted.	CC9.2
DS-72	Visitors must be signed in by an employee before access to high security areas is granted.	Observed and inspected the visitor sign in process and determined visitors must be signed in by an employee before access to high security areas is granted.	No exceptions noted.	CC6.4

AICPA Trust Services Criteria Reference Table

Criteria	Criteria Description	Control Activity
CC1.0 Control Environment		
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	DS-1; DS-2; DS-3; DS-4
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	DS-5; DS-6; DS-7; DS-8
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	DS-8; DS-9; DS-10
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	DS-3; DS-11; DS-12
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	DS-9; DS-11; DS-13
CC2.0 Communication and Information		
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	DS-14; DS-15
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	DS-15; DS-16; DS-17; DS-18
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	DS-19; DS-20
CC3.0 Risk Assessment		
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	DS-21; DS-22
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	DS-21; DS-22; DS-23; DS-24; DS-25; DS-26
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	DS-21; DS-22

Criteria	Criteria Description	Control Activity
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	DS-27; DS-28; DS-29
CC4.0 Monitoring Activities		
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	DS-35; DS-36; DS-37
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	DS-8; DS-30; DS-35; DS-36; DS-62
CC5.0 Control Activities		
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	DS-30
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	DS-32; DS-33
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	DS-8; DS-13; DS-18; DS-27; DS-68
CC6.0 Logical and Physical Access Controls		
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	DS-65; DS-76; DS-77
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.	DS-31; DS-34; DS-64
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.	DS-31; DS-34; DS-63

Criteria	Criteria Description	Control Activity
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	DS-51; DS-52; DS-53; DS-54
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	DS-72; DS-73; DS-74
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	DS-50; DS-71
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	DS-44; DS-45; DS-46; DS-47
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	DS-44; DS-45; DS-47
CC7.0 System Operations		
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	DS-41; DS-42; DS-43
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	DS-8; DS-39; DS-58
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	DS-59; DS-60
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.	DS-61; DS-62
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	DS-20; DS-59; DS-60; DS-61
CC8.0 Change Management		

Criteria	Criteria Description	Control Activity
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	DS-48; DS-49; DS-90; DS-91
CC9.0 Risk Mitigation		
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	DS-38; DS-39; DS-40; DS-58
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	DS-14

VIII. ADDITIONAL INFORMATION PROVIDED BY THE INDEPENDENT SERVICE AUDITOR

Selection Criteria for Specific Tests

In selecting tests of the operating effectiveness of controls, we considered the

a) nature of the items being tested,
b) the types and adequacy of available evidential matter,
c) the nature of the trust services criteria to be achieved, and
d) the expected efficiency and effectiveness of the test.

Types and Descriptions of the Tests of Operating Effectiveness

Various testing methods are used to assess the operating effectiveness of controls during the examination period. The table below describes the various methods that were employed in testing the operating effectiveness of controls that are in place at the Company.

Testing Procedure	Description
Inquiry	Inquired of appropriate personnel and corroborated with management.
Observation	Observed the application or existence of the specific control as represented.
Inspection	Inspected documents and records indicating performance of the control.
Reperformance	Reperformed the control, or processing of the application control, for accuracy of its operation.

Procedures for Assessing Completeness and Accuracy of Client-Provided Information ("CPI")

For tests of controls requiring the use of CPI (for example, controls requiring system-generated populations for sample-based testing), we performed a combination of the following procedures where possible, based on the nature of the CPI, to address the completeness, accuracy, and integrity of the data or reports used:

a) inspect the source of the CPI,
b) inspect the query, script, or parameters used to generate the CPI,
c) tie data between the CPI and the source, and/or
d) inspect the CPI for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity.

In addition to the above procedures, for tests of controls requiring management's use of CPI in the execution of the controls (for example, periodic reviews of user access listings), we inspected management's procedures to assess the validity of the CPI source and the completeness, accuracy, and integrity of the data or reports.