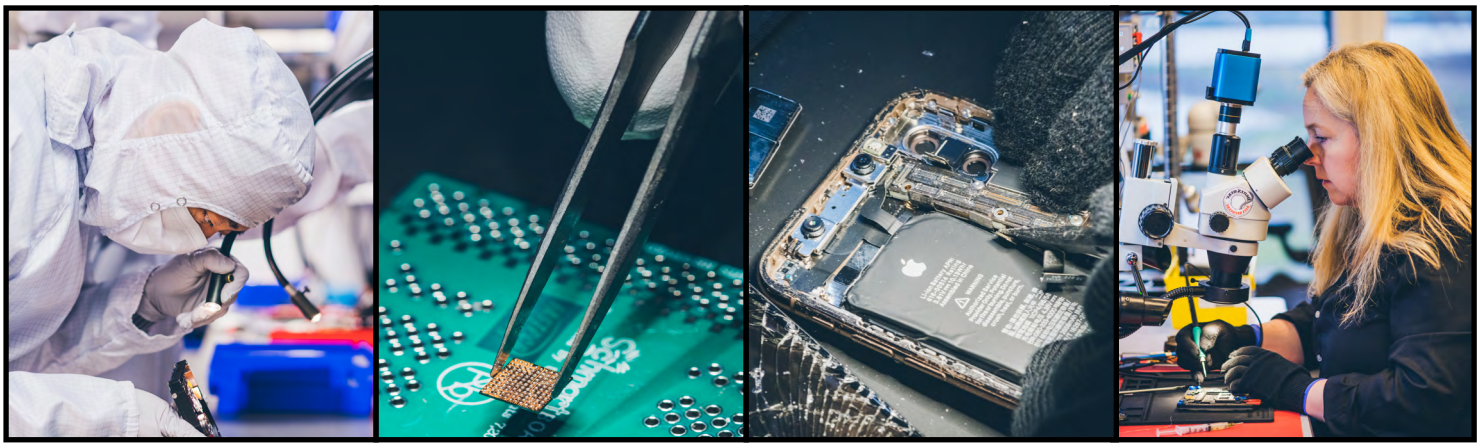
Who Can You Trust With Your Data?

The vetting process of a third-party data recovery service provider is the most critical step in preventing a breach.



Vet DriveSavers Data Recovery

This page is intentionally blank.

The Big Picture

Possible data breach must be a consideration anywhere critical data can be accessed. If your data recovery service provider's network is hacked and critical customer data is accessed, your company could be liable.

The National Institute of Standards and Technology (NIST) recommends that third-party data recovery service providers be properly vetted before turning over data storage equipment to them for recovery.

If a data storage device has failed resulting in lost or corrupted digital data, few organizations have the internal resources to recover that data, especially in the case of a mechanical failure. The device must be sent to a data recovery vendor. These devices often hold critical IP, financial databases, accounting files, email exchanges, customer records, PCI, PII and PHI. Therefore, data recovery organizations must be classified as high-risk vendors. However, **most of the data recovery industry does not meet best practice standards to ensure data security.**

Why Vet

If an organization does not perform due diligence before engaging the services of a data recovery vendor, it runs the risk of a data breach. **This can result in damage to an organization's reputation and have serious financial ramifications.** The good news is that changes to internal policies and procedures combined with contractual changes with third-party businesses handling the organization's data will mitigate the risk posed by this security gap.

Certified Secure Data Recovery

Since 1985, DriveSavers has completed more than 500,000 data recoveries and we support over 20,000 business partners worldwide. More importantly, **DriveSavers is the only data recovery company in the industry that undergoes an annual SSAE 18 SOC 2 Type II audit, offering the highest level of data security available.**

The SOC 2 Type II audit assures that every aspect of the facility and network are certified secure to protect personal and confidential data. SOC 2 Type II is the most stringent and extensive security audit administered, verifying that our data hosting control objectives and control activities are in place, suitably designed, enforced and operating effectively to achieve all desired security control objectives.

This annual independent audit of the previous year's operations verifies our qualifications to handle enterprise-class recoveries and support those customers who must maintain compliance with data privacy and data security regulations such as:

- NIST (National Institute of Standards & Technology) SP 800.34 (Rev.1)
- HIPAA (Health Insurance Portability and Accountability Act)
- FERPA (Family Educational Rights and Privacy Act)
- SOX (Sarbanes-Oxley Act of 2002)
- GLBA (Gramm-Leach-Bliley Act of 1999)
- GDPR (General Data Protection Regulation)

Enclosed you will find the necessary documentation exhibiting proof of DriveSavers unmatched data security. This document is updated annually and certificates may be in the process of recertification. 9/20/23

This page is intentionally blank.

Table of Contents

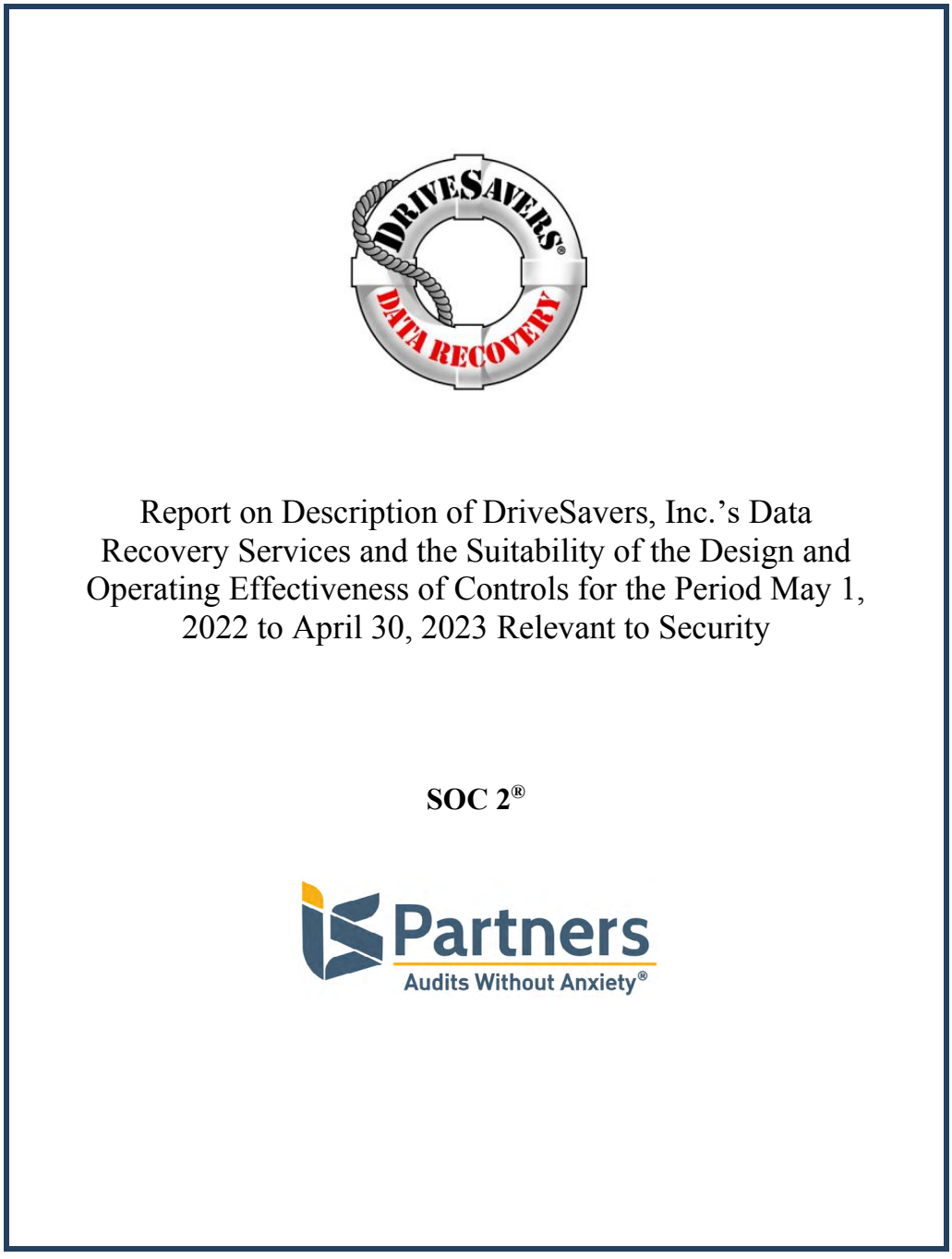
Please Click the on the Interactive Links.

This page is intentionally blank.

SOC 2 Type II Certification

IS Partners Audit Report

IS Partners SOC 2 Type II audit: DriveSavers undergoes an annual SOC 2 Type II audit of its internal data hosting and processing controls to guarantee that our data recovery services uphold the stringent data security and privacy protocols mandated by the corporate clients and government agencies we serve.
These annual audits are conducted by control-oriented professionals from IS Partners, an independent firm with experience in accounting, auditing and information security. At the end of each annual audit period, a successive twelve-month "look back" audit begins, and an updated report is generated reflecting the dates for which records were reviewed. The "look back" period is reflected in the dates on the report.



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

IS Partners, LLC
1668 Susquehanna Road
Dresher, PA 19025

215.675.1400 main office
215.259.7928 fax
ispartnersllc.com

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.

IS Partners, LLC
1668 Susquehanna Road
Dresher, PA 19025

215.675.1400 **main office**
215.259.7928 **fax**
ispartnersllc.com

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

IS Partners, LLC
1668 Susquehanna Road
215.675.1400 main office
215.259.7928 fax

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

215.675.1400 main office
215.259.7928 fax

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.

The IS Partners Audit Report is updated annually. If you would like the complete report, click here.

HIPAA PROGRAM POLICY CERTIFICATION

Executive Summary

Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Omnibus rules, providers have an obligation to assure their Business Associates are complying with these regulations. *DriveSavers Data Recovery* engaged *WiRED* Security Incorporated to provide an independent review of their corporate information security policies. The purpose of this review was to ensure that *DriveSavers Data Recovery* in its role as a Business Associate (BA) meet the compliance requirements imposed by HIPAA. The scope of this engagement included reviewing and updating corporate information security policies as required, to meet this objective.

Information security best practices were used along with the objectives set forth under HIPAA to conduct this assessment. The assessment was done to ensure that the language and processes used would meet regulatory requirements and safeguard sensitive health information.

The policy assessment team looked at *DriveSavers Data Recovery's* policies and compared them (gap analysis) to policies used by similar organizations and healthcare industry vetted templates that align with HIPAA. The assessment fully covered the topics listed below to ensure they would be compliant with HIPAA regulations:

- Security Risk Assessment and Risk Management
- Appropriate Information Technology (IT) Systems and Services
- An Assigned Security Official with Documented Responsibilities
- Workforce security and verification of proper access to ePHI
- Information Access Management
- Workstation Use
- Device and Media Controls
- Encryption and Decryption
- Access Controls
- Integrity

Executive Summary Conclusion

The DriveSavers Data Recovery information security policies meet the demonstrated requirements and obligations as required for its role as a Business Associate under HIPAA compliance rules. Their information security policies show that they are committed to providing a secure computing environment and provide reasonable protection for the data that is entrusted to them by their clients and business partners.

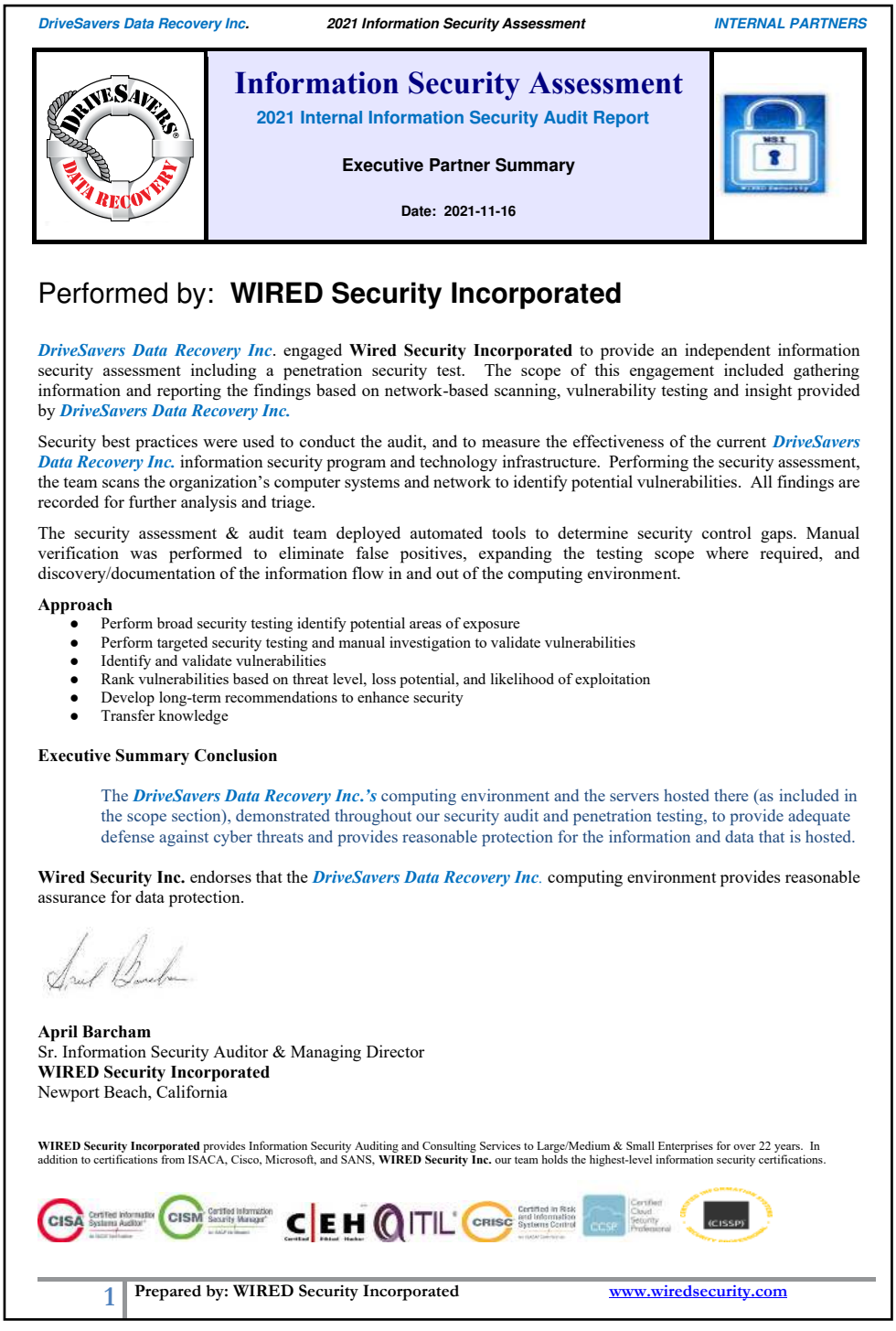
WIRED Security ***endorses*** that *DriveSavers Data Recovery* corporate information security policies meet the demonstrated requirement and obligations as required for its role as a Business Associate under HIPAA compliance.

Peter Brown
Principal Information Security Consultant
WIRED Security Incorporated
Newport Beach, California

WIRED Security Incorporated provides Information Security Auditing and Consulting Services to Large/Medium & Small Enterprises for over 17 years. In addition to certifications from ISACA, Cisco, Microsoft, and SANS, *WIRED* Security consultants hold the highest level information security certifications, including CISSP, CISM, CISA and CEH.

Network Security Audit

DriveSavers undergoes annual security audits on its perimeter and network systems. These audits are conducted by a team of independent information security and technology consultants from WIRED Security, Inc., to ensure that adequate controls and safeguards are in place for safely hosting data belonging to our customers. A thorough review of our Business Continuity Plan, Information Security Policy and the SOC 2 Type II audit documentation is performed. DriveSavers has deployed a full "Defense-in-Depth" network. All hardware and software used by DriveSavers has multiple industry certifications including, but not limited to, NIST, NEBS level 3, ICSA, NSS and FIPS. The DriveSavers computing network environment (as tested) has an excellent ability to avoid information security breaches.



DriveSavers Data Recovery Inc. *2021 Information Security Assessment* *INTERNAL PARTNERS*

Information Security Assessment

2021 Internal Information Security Audit Report

Executive Partner Summary

Date: 2021-11-16

Performed by: **WIRED Security Incorporated**

DriveSavers Data Recovery Inc. engaged **Wired Security Incorporated** to provide an independent information security assessment including a penetration security test. The scope of this engagement included gathering information and reporting the findings based on network-based scanning, vulnerability testing and insight provided by ***DriveSavers Data Recovery Inc.***

Security best practices were used to conduct the audit, and to measure the effectiveness of the current ***DriveSavers Data Recovery Inc.*** information security program and technology infrastructure. Performing the security assessment, the team scans the organization's computer systems and network to identify potential vulnerabilities. All findings are recorded for further analysis and triage.

The security assessment & audit team deployed automated tools to determine security control gaps. Manual verification was performed to eliminate false positives, expanding the testing scope where required, and discovery/documentation of the information flow in and out of the computing environment.

Approach

- Perform broad security testing identify potential areas of exposure
- Perform targeted security testing and manual investigation to validate vulnerabilities
- Identify and validate vulnerabilities
- Rank vulnerabilities based on threat level, loss potential, and likelihood of exploitation
- Develop long-term recommendations to enhance security
- Transfer knowledge

Executive Summary Conclusion

The ***DriveSavers Data Recovery Inc.'s*** computing environment and the servers hosted there (as included in the scope section), demonstrated throughout our security audit and penetration testing, to provide adequate defense against cyber threats and provides reasonable protection for the information and data that is hosted.

Wired Security Inc. endorses that the ***DriveSavers Data Recovery Inc.*** computing environment provides reasonable assurance for data protection.

April Barcham
Sr. Information Security Auditor & Managing Director
WIRED Security Incorporated
Newport Beach, California

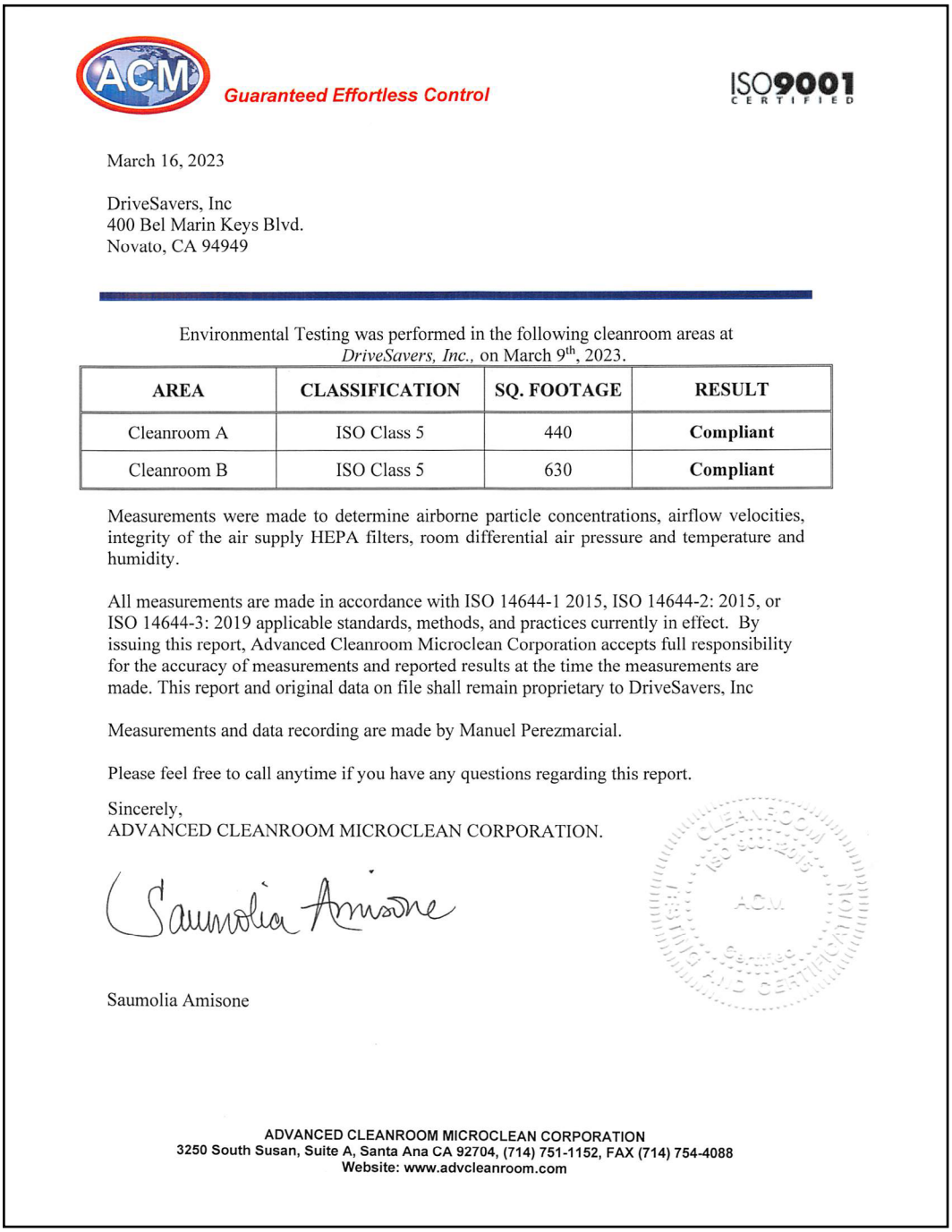
WIRED Security Incorporated provides Information Security Auditing and Consulting Services to Large/Medium & Small Enterprises for over 22 years. In addition to certifications from ISACA, Cisco, Microsoft, and SANS, **WIRED Security Inc.** our team holds the highest-level information security certifications.

1 **Prepared by: WIRED Security Incorporated** www.wiredsecurity.com

Certified ISO Class 5 Cleanroom

DriveSavers has installed the largest and most technologically-advanced, ISO-certified data recovery Cleanroom environment in the industry. This pristine environment protects drives and data from airborne contaminants maximizing recovery success rates. Sealed drive mechanisms can be opened in accordance with the specifications of all leading hardware and storage device manufacturers without voiding the original warranty.

CPS Controlled Environment Testing Report



ACM *Guaranteed Effortless Control*

ISO9001 CERTIFIED

March 16, 2023

DriveSavers, Inc
400 Bel Marin Keys Blvd.
Novato, CA 94949

Environmental Testing was performed in the following cleanroom areas at *DriveSavers, Inc.*, on March 9th, 2023.

AREA	CLASSIFICATION	SQ. FOOTAGE	RESULT
Cleanroom A	ISO Class 5	440	**Compliant**
Cleanroom B	ISO Class 5	630	**Compliant**

Measurements were made to determine airborne particle concentrations, airflow velocities, integrity of the air supply HEPA filters, room differential air pressure and temperature and humidity.

All measurements are made in accordance with ISO 14644-1 2015, ISO 14644-2: 2015, or ISO 14644-3: 2019 applicable standards, methods, and practices currently in effect. By issuing this report, Advanced Cleanroom Microclean Corporation accepts full responsibility for the accuracy of measurements and reported results at the time the measurements are made. This report and original data on file shall remain proprietary to DriveSavers, Inc

Measurements and data recording are made by Manuel Perezmarcial.

Please feel free to call anytime if you have any questions regarding this report.

Sincerely,
ADVANCED CLEANROOM MICROCLEAN CORPORATION.

Saumolia Amisone

Saumolia Amisone

ADVANCED CLEANROOM MICROCLEAN CORPORATION
3250 South Susan, Suite A, Santa Ana CA 92704, (714) 751-1152, FAX (714) 754-4088
Website: www.advcleanroom.com

Cleanroom Test Scope

DriveSavers, Inc. Test Date: 03/09/23 Previous Test Date: 01/21/22

CLEANROOM A CERTIFICATED OF COMPLIANCE

Test Mode:	At-Rest	
Airflow Type:	Non-Unidirectional	
Test Date:	03/09/23	
Next Test Date:	03/2024	
Class:	ISO14644-1: **5**	LIMIT AT 0.5 UM = 3,520

CLEANROOM A **Meet** the Requirements per ISO 14644-1 Class **5**, at 0.5 um particle size.

DriveSavers, Inc. Test Date: 03/09/23 Previous Test Date: 01/21/22

CLEANROOM B CERTIFICATED OF COMPLIANCE

Test Mode:	At-Rest	
Airflow Type:	Non-Unidirectional	
Test Date:	03/09/23	
Next Test Date:	03/2024	
Class:	ISO14644-1: **5**	LIMIT AT 0.5 UM = 3,520

CLEANROOM B **Meet** the Requirements per ISO 14644-1 Class **5**, at 0.5 um Particle size.

Initials MP Date 16Mar23

IT Industry Training and Certifications

DriveSavers has been recovering data and restoring peace of mind since 1985, and has completed more than 500,000 data recoveries worldwide. We also support over 20,000 business partners and our engineers are trained and certified to handle the most challenging data recovery cases.

IT Industry Certifications

Apple – Certified Macintosh Technician (ACMT)

CompTIA A+ Certified

CompTIA Network+ Certified

PC3000 Certified

U.C. Berkeley– Telecommunications Engineering Certified

U.S. Navy – Micro Miniature Soldering Certified

U.S. Government –Security Standards and Specifications

WinHex – FileSystems Revealed

IT Industry Training

FreeNAS Administration Training

Knowledgetek – Solid-State Drive (SSD) Technology

Microclean Solutions – Corporate Cleanroom Training

SANS Institute

VMware – vSphere: Install, Configure, Manage

Custom Security Protocol Options

DriveSavers offers the highest possible security protocols to meet the stringent requirements of corporations and government agencies and can customize a security protocol to meet the security level you require.

- Devices acquired using forensic best practices
- Media is kept in a Class 5 Mosler Safe during non-working hours
- No copies of your data are kept on site after your recovery is complete
- Two separate copies of the recovered data shipped via two different methods
- Procedures are documented and adhered to for handling sensitive or encrypted data
- Chain of custody protocols provided upon receipt of return
- Confidentiality agreement endorsed

To view all certifications and new additions visit: www.drivesaversdatarecovery.com/proof

DriveSavers Security Compliance Contacts

At the heart of our certified secure data recovery environment is a “defense-in-depth” network, verified in our SOC 2 Type II auditing process to be “a formidable defense” for the information and data that it hosts.

Michael Cobb

Chief Information Security Officer, Facility Security Officer

1.415.591.7772 direct
1.415.382.8000 x126

mike.cobb@drivesavers.com

Rocky Trono

Government Account Executive, Strategic Alliances Manager

1.415.766.9026 direct
1.415.382.8000 x113

rocky.trono@drivesavers.com

Companies Worldwide Trust DriveSavers

DriveSavers Data Recovery
1.800.440.1904—Toll Free
1.415.382.2000—Local
1.888.440.2404—International
DriveSavers.com