schellman
Quality, above all.

CERTIFICATE OF REGISTRATION

Information Security Management System - ISO/IEC 27001:2013

The Certification Body of Schellman & Company, LLC hereby certifies that the following organization operates an Information Security Management System that conforms to the requirements of ISO/IEC 27001:2013

Brownstein Hyatt Farber Schreck, LLP

for the following scope of registration

The scope of the ISO/IEC 27001:2013 certification covers the information security management system (ISMS) supporting the Brownstein systems and supporting services including Brownstein's IT personnel, staff, attorneys, department directors, executive leadership, applicable system owners, information security policies and procedures, physical controls, client and firm data, and in accordance with the Statement of Applicability, version 1.2, dated February 10, 2021.

which includes the following in-scope location(s) on page 2 of 2

Certificate Number: **1554476-2**

ISO 27001 CERTIFIED by schellman

ANAB ACCREDITED ISO/IEC 17021 MANAGEMENT SYSTEMS CERTIFICATION BODY

UKAS MANAGEMENT SYSTEMS 8685

Authorized by:

Christopher L. Schellman
CEO, Schellman & Company, LLC
4010 W Boy Scout Blvd., Suite 600
Tampa, Florida 33607, United States
www.schellman.com

Issue Date	Original Registration Date	Expiration Date	Certificate Version
April 5, 2021	February 21, 2020	February 20, 2023	Version 2

CONDITIONS & LIMITATIONS:

1. The aforementioned organization has a perpetual responsibility to maintain compliance with ISO/IEC 27001:2013 during the period of certification.
2. This certificate is subject to the satisfactory completion of annual surveillance audits by Schellman & Company, LLC
3. ISO/IEC 27001:2013 compliance audits are not designed to detect or prevent criminal activity or other acts that may result in an information security breach. As such, this certification should not be construed as a guarantee or assurance that an organization is unsusceptible to information security breaches.
4. The information in this document is provided "AS IS", without warranties of any kind. Schellman & Company, LLC expressly disclaims any representations and warranties, including, without limitation, the implied warranties of merchantability and fitness for a particular purpose.
5. This certificate is the property of Schellman & Company, LLC and is bound by the conditions of contract. The authenticity of this certificate can be validated by contacting Schellman & Company, LLC

In-Scope Location(s)

Location	Function / Role
410 17th Street Suite 2200 Denver, Colorado 80202 United States	Headquarters and Main Location of the ISMS and its Owners
1155 F Street NW Suite 1200 Washington, District of Columbia 20004 United States	Operations
100 North City Parkway Las Vegas, Nevada 89106 United States	Operations
2049 Century Park East Los Angeles, California 90067 United States	Operations
1021 Anacapa Street Santa Barbara, California 93101 United States	Operations

Brownstein

Information Security Management System Manual

Purpose

The purpose of this document is to provide an overview of the ISO 27001:2013 implementation at Brownstein Hyatt Farber Schreck (Brownstein).

1. Context of the Organization (Clause 4)

1.1 Understanding the Organization and Its Context

Brownstein has determined and documented the external and internal issues that are relevant to the Information Security Management System(ISMS)in the Scoping Statement. The ISMS Scope must be reviewed at least annually, and any needed changes approved.

1.2 Understanding the Needs and Expectations of Interested Parties

Brownstein has determined and documented the interested parties relevant to the ISMS and the requirements of those parties in the Scoping Statement. The Risk Management Committee (RMC) will review the needs and expectations of all interested parties at least annually and approve any needed changes.

1.3 Determining the Scope of The Information Security Management System

Brownstein has determined the boundaries of the ISMS and established a scope. The requirements of the issues in §4.1 have been considered and the requirements of relevant parties in §4.2 in determining the scope of the ISMS have been documented in the ISMS Scoping Statement.

1.4 Information Security Management System

Brownstein has established, implemented and must continually maintain the ISMS as documented in the ISMS Scoping Statement.

2. Leadership (Clause 5)

2.1 Leadership and Commitment

Top management must be committed to the establishment of an effective ISMS and demonstrates this commitment in the following ways:

A documented library of information security policies with clearly defined objectives.

An ISMS that is operational within the business units and processes within its scope. The objectives of the ISMS are to:

- Provide a framework for clear communication of top management's commitment to the successful operation and improvement of the ISMS and meeting the objectives of the ISP.
- Identify and provide the resources needed to establish, maintain and improve the ISMS.

- Provide direction and support with regards to information security, business requirements, relevant laws and regulations and client security requirements.
- Establish a viable management framework for ISMS implementation, ongoing operation, and consequently, effective information security within the firm's ISMS boundary.
- Ensure employees, vendors, and contractors understand their responsibilities and are suitable to protect Brownstein's interests and clients' information.
- Manage external service providers and other vendors to ensure compliance with information security requirements.
- Ensure the proper protection of Brownstein's assets.
- Prevent unauthorized physical or logical access or damage to sensitive information or information processing facilities and offices.
- Ensure compliance with applicable International, Federal, State, and local laws, regulations and guidelines.
- Ensure compliance with client-mandated security requirements for storing, processing and transmitting sensitive information.
- Ensure appropriate integrity of information, data and data systems through monitoring, logging, auditing user activity.
- Ensure an appropriate level of security awareness for all employees.
- Ensure the continuity of the firm's most critical business functions, services, and enabling IT systems in the event of a disruption.
- Ensure ongoing monitoring and measurements of the selected controls selected to achieve desired risk management outcomes.

2.3 Policy

Top management has established a documented library of information security policies that provides a high-level description of Brownstein's policy, objectives, and approach to information security. The RMC will review the library information security policies at least annually and as needed submit recommendations for updates as may be necessary to the firm.

2.4 Organizational Roles, Responsibilities, And Authorities

Top management must ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated. The RMC has the authority to make all necessary decisions with regards to; ISMS organization, roles and responsibilities assignments to relevant people and business units, and to routinely collect reports sufficient to monitor the performance of the ISMS in meeting the objectives as stated above.

3. Planning (Clause 6)

3.1 Actions to Address Risks and Opportunities

Brownstein has engaged professional services to assist with ISMS establishment and to improve the firm's information security posture. Such improvement is achieved through a risk-based approach to identify methods, controls, and metrics that will ensure the effective operation of the ISMS.

The RMC must maintain at least annually a documented Risk Assessment Methodology, Risk Assessment, Risk Treatment Plan, and a Statement of Applicability as a list of selected controls. The RMC must also review and approve needed changes to policies and procedures at least annually.

3.2 Information Security Objectives and Planning to Achieve Them

Brownstein has established objectives as stated above that are consistent with the documented library of information security policies. The objectives are measurable, risk-based, and communicated to interested parties. These objectives as well as the implemented security controls will be reviewed, evaluated and approved at least annually.

Brownstein must establish ISMS information security objectives which will be reviewed at least annually by the RMC. The objectives will be updated as necessary and documented in the RMC meeting minutes and this manual. ISMS Metrics must be gathered and maintained to provide evaluation requirements and criteria. Objectives must be communicated to employees through the initial onboarding process and annual Security Awareness Training.

4. Support Clause 7

4.1 Resources

The RMC has the authority to allocate company resources as needed to establish, implement, maintain, and improve this ISMS. Resource requirements must be evaluated and adjusted by the RMC as needed, at least annually. Decisions regarding resource adjustments must be documented in meeting minutes.

4.2 Competence

The competence of the personnel implementing the ISMS is left to the discretion of the RMC. The Chief Security Officer (CISO) is responsible for determining the experience, education and background that personnel must have to be deemed competent in Information Security Management Systems and Management Systems Auditing.

The CISO will be responsible for monitoring and measuring control effectiveness, risk management effectiveness and ensuring compliance.

4.3 Awareness

To improve the competence of the firm as a whole, all employees of Brownstein must be aware of the documented library of information security Policies. In addition, Brownstein should make employees aware of their contribution to the effectiveness of the ISMS and the benefits of improved information security performance. Brownstein employees must also be aware of the consequences of not conforming with the requirements set by the ISMS program.

Awareness of the documented library of information security polices is accomplished through the following:

- New employees receive Security Awareness Training as a part of the onboarding process.
- All employees receive Security Awareness Training at least annually.

- Employees with specialized roles receive training that aligns with the work they are responsible for.

Additionally, the RMC may enhance security awareness through additional training, notifications, testing and other means as appropriate.

4.4 Communication

The RMC has the authority to communicate on topics related to information security.

The RMC may designate or assign responsibility for communication on matters both routine and unexpected. Improvements to the ISMS and the status of these improvements should be approved, implemented, and tracked by the RMC in compliance with its charter. CISO is the Brownstein ISMS point of contact.

When communicating, the following guidance must be followed:

- What to communicate: Changes to policies, procedures, regulations, laws, risks, vendor requirements or operating environment;
- When to communicate: As approved by the RMC. Emergence, requirement or incident, the CISO has the authority to communicate as necessary either internally or externally. If the CISO exercises this authority, they will notify the RMC as soon as is practical;
- With whom to communicate: Internal or external stakeholders as appropriate. Corporate-sensitive information must not be communicated to external stakeholders unless required by contractual obligation, regulation or best business practice;
- Who shall communicate: The RMC Chair or Senior Management shall be the primary points of communication with internal and external stakeholders. In the event neither is available, the next senior member will take responsibility, provided that person is in a corporate officer position.
- Process: Communication with external stakeholders will be via email to ensure a record of the communication. Telephone calls, if necessary, should be used to clarify emails and not issue new information. Communications with internal stakeholders will be via email or other means as necessary. In accordance with ISMS-related policy. UNDER NO CIRUMSTANCES WILL SOCIAL MEDIA BE USED TO COMMUNICATE ISMS-RELATED INFORMATION, INCIDENTS OR STATUS.

4.5 Documented Information

Documentation required by the ISO 27001 standard, the ISMS, and the related information security policies and procedures, are governed by Brownstein Change Management Procedures. The RMC will review and approve needed changes at least annually.

5. Operation (Clause 8)

5.1 Operational Planning and Control

The RMC owns all of the processes of the ISMS and is responsible for all changes made to the ISMS.

Decisions made that affect change to the ISMS and the controls selected must be documented in meeting minutes or tickets submitted for approval according to the Change Management Process.

5.2 Information Security Risk Assessment

Brownstein has determined that a risk-based approach to information security works best for the firm and will conduct a Risk Assessment at least annually. The RMC may initiate additional assessments as deemed necessary and will define the scope of each as needed.

Risk Assessments are conducted according to the Brownstein Risk Assessment Methodology policy. The RMC will review and approve needed changes to the methodology at least annually.

5.3 Information Security Risk Treatment

Brownstein will create a plan in the Risk Treatment Plan to reduce risks in necessary processes when the current risk exceeds the accepted risk threshold.

A Risk Treatment Plan is documented per the Brownstein Risk Assessment Methodology. The RMC must review and approve needed changes to the methodology at least annually.

6. Performance evaluation (Clause 9)

6.1 Monitoring, Measurement, Analysis and Evaluation

Brownstein has determined the necessary metrics to evaluate the effectiveness of the ISMS. The selected metrics, applicable control objectives, methods of measurement, frequency of reporting, report owner, criteria for analysis and reporting channels are documented in the Brownstein ISMS Metrics. The RMC will review and approve needed changes to the program at least annually.

6.2 Internal Audit

The RMC is responsible for auditing the ISMS. An Internal Audit Program must be developed in accordance with ISO 27001 requirements, and this function will be outsourced for independence purposes. Audits of physical and environmental controls at each office will be conducted by the CISO or the CIO. The RMC will review and approve any needed changes to the program at least annually.

6.3 Management Review

Brownstein's Senior Management has chartered the RMC to review the ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness. Internal audits will be used to measure the ISMS effectiveness to ISO 27001 standards and conformance to business needs. Internal audits will be conducted before certification and annual surveillance audits.

The organization relies upon the CISO and CIO to plan and implement the internal ISMS audit program. Internal ISMS audits should be planned using a risk-based approach that considers Brownstein's drivers for implementing ISO 27001, InfoSec goals and objectives,

current and planned architecture, the most current Risk Assessment, and technical operating environment which includes implemented security controls and the approved ISMS metrics.

Only qualified personnel and third parties should be used to conduct internal ISMS audits. Acceptable certifications include ISO 27001 Lead Auditor, Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), or Certified ISO 27001 Lead Implementer. Appropriately qualified persons will not be permitted to perform internal ISMS audits for any part of the ISMS they implemented either partially or in whole.

Internal ISMS audit results must be delivered and briefed to the RMC. The RMC chair must ensure internal audits are maintained in the ISMS repository that is in compliance with the firm's procedures for maintaining ISMS-related information.

The RMC Meeting Agenda and Minutes must be performed to document its oversight responsibilities. Meetings are scheduled at least annually. The Senior Security Manager will review the meeting minutes template at least annually and make any needed changes to ensure completeness and applicability.

Internal ISMS auditors must document the ISMS records' compliance to the ISO 27001 standard and recommend items for corrective action and continuous improvement to ensure ISMS records are in concert with the standard as well as approved policies and procedures.

7. Improvement (Clause 10)

7.1 Nonconformity and Corrective Action

The RMC has established a Corrective Action Plan (CAP) process to address audit findings.

A non-conformity is defined as the absence of, or the failure to implement and maintain, one or more ISMS requirements and are categorized as either minor or major.

When a non-conformity is identified, it must be categorized as either major or minor. Lesser identified issues will be considered as "observations".

Non-conformities will be identified through the audit process and controlled through the Corrective Action Plan (CAP) process. In the event of a non-conformity, the CAP will include a Root Cause Analysis (RCA) with the underlying causative condition clearly identified and approved by the RMC. Additionally, the root cause will be used to determine if similar situations exist in other areas and mitigating/corrective actions implemented to preclude the potential for recurrence of the non-conformity.

Findings must be formally identified, recorded and tracked from identification through resolution. Non-conformities will be corrected in accordance with the respective CAP.

Any temporary measures will be attributed a milestone date and all milestone dates, completion dates and status must be reviewed and approved by the RMC with such review annotated in the committee's meeting minutes. The Senior Security Manager will report to the RMC when all corrective actions have been implemented.

All non-conformities, both open and closed, will be maintained in a consolidated log with the ISMS-related documentation in the ISMS Repository. A brief overview of the information

may be used in the CAP Log in lieu of complete redundancy between the CAP itself and the information in the log. The RMC will review and approve corrective actions and any needed program changes annually.

7.2 Continual Improvement

To achieve continuous improvement, the RMC solicits inputs from interested parties on a routine basis. The CISO and CIO will review such inputs at least annually or as necessary depending upon the nature of the input.

Revision History

Date	Initials	Changes Made	Revision #
4/1/19	AC	Initial Draft	
5/13/19	DL	Final	1.0
12/1/20	DL	Annual review. No changes made.	2.0
2-22-21	DL	Reformatted to match Policy format, Updated revision Dates and version. Added Confidential Footer	2.1
04/16/21	DL / EL	Annual Review. No Changes made.	2.1