Report on Description of 3H Corporate Services, LLC Corporate and Insurance Licensing Services System and the Suitability of the Design of Controls as of December 31, 2021 Relevant to Security

SOC 2®

Partners
Audits Without Anxiety®

TABLE OF CONTENTS

I. INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of 3H Corporate Services, LLC:

Scope

We have examined 3H Corporate Services, LLC's ("3HCS") and affiliates (3H Agent Services, Inc., 3H Tax Filing Services, LLC, and Creative Compliance Software Solutions, LLC) accompanying description entitled "Description of 3H Corporate Services, LLC's Corporate and Insurance Licensing Services System" ("description") as of December 31, 2021, 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 of controls stated in the description as of December 31, 2021, to provide reasonable assurance that 3H Corporate Services, LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to security ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

3H Corporate Services, LLC uses subservice organizations for infrastructure hosting and VPN software in support of the Corporate and Insurance Licensing Services System. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at 3H Corporate Services, LLC, to achieve 3H Corporate Services, LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents 3H Corporate Services, LLC's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of 3H Corporate Services, LLC's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, 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 3H Corporate Services, LLC, to achieve 3H Corporate Services, LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents 3H Corporate Services, LLC's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of 3H Corporate Services, LLC's controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service organization's responsibilities
3H Corporate Services, LLC is responsible for its service commitments and system requirements and for designing and implementing controls within the system to provide reasonable assurance that 3H Corporate Services, LLC's service commitments and system requirements were achieved. 3H Corporate Services, LLC has provided the accompanying assertion entitled "3H Corporate Services, LLC's Management Assertion" ("assertion") about the description and the suitability of the design of controls stated therein. 3H Corporate Services, LLC 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 the design 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 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 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
- 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
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent limitations
The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design 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.

Other matters
We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion
In our opinion, in all material respects:

a. The description presents 3H Corporate Services, LLC's Corporate and Insurance Licensing Services System that was designed and implemented as of December 31, 2021, in accordance with the description criteria.
b. The controls stated in the description were suitably designed as of December 31, 2021, to provide reasonable assurance that 3H Corporate Services, LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of December 31, 2021, and if subservice organizations and user entities applied the complementary controls assumed in the design of 3H Corporate Services, LLC's controls as of December 31, 2021.

Restricted use
This report is intended solely for the information and use of 3H Corporate Services, LLC, user entities of 3H Corporate Services, LLC's Corporate and Insurance Licensing Services System as of December 31, 2021, business partners of 3H Corporate Services, LLC subject to risks arising from interactions with the Corporate and Insurance Licensing Services System, 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
Dresher, Pennsylvania
January 12, 2022

IS Partners, LLC
1668 Susquehanna Road
Dresher, PA 19025

215.675.1400 main office
215.259.7928 fax
ispartnersllc.com

II. SERVICE ORGANIZATION'S ASSERTION

3H Corporate Services, LLC's Management Assertion

We have prepared the description entitled "Description of 3H Corporate Services, LLC's Corporate and Insurance Licensing Services System" (the "description") as of December 31, 2021, 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 Corporate and Insurance Licensing Services System that may be useful when assessing the risks arising from interactions with 3H Corporate Services, LLC's system, particularly information about system controls that 3H Corporate Services, LLC has designed and implemented 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*).

3H Corporate Services, LLC uses subservice organizations for infrastructure hosting and VPN software in support of the Corporate and Insurance Licensing Services System. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at 3H Corporate Services, LLC, to achieve 3H Corporate Services, LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents 3H Corporate Services, LLC's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of 3H Corporate Services, LLC's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at 3H Corporate Services, LLC, to achieve 3H Corporate Services, LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents 3H Corporate Services, LLC's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of 3H Corporate Services, LLC's controls.

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

a. the description fairly presents the Corporate and Insurance Licensing Services System that was designed and implemented as of December 31, 2021, in accordance with the description criteria.

b. the controls were suitably designed to provide reasonable assurance that 3H Corporate Services, LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of December

31, 2021, and if subservice organizations and user entities applied the complementary controls assumed in the design of 3H Corporate Services, LLC's controls as of December 31, 2021.

III. DESCRIPTION OF 3H CORPORATE SERVICES, LLC'S CORPORATE AND INSURANCE LICENSING SERVICES SYSTEM

Background

3HCS was founded by Gary Harker to assist and guarantee that entrepreneurs and business owners comply with State and Federal Laws. As a corporate attorney, Gary has advised business clients on all issues involving corporate formation, governance, and business operations and transactions. He brings over 20 years of legal, regulatory, corporate, and general business experience to 3HCS.

3HCS is focused on providing exceptional corporate and insurance licensing services.

Business:

- Business Formation
- Qualifications/ Incorporations
- Trade Name Registrations
- Annual Reports
- Document Retrieval
- Dissolution/ Withdrawals
- Consulting

Licensing:

- Purchasing Group Registrations and Annual Filings
- Applications
- Renewals
- Maintenance
- Consulting
- Creative Compliance Software Solutions

Principal Service Commitments and System Requirements

Creative Compliance takes the security and privacy of its customers seriously. Therefore, the company has chosen to undergo a SOC 2 examination that includes the SOC 2 trust services category of security.

Creative Compliance makes the following security and privacy-related commitments to its customers:

- Anything posted to 3H is private to their organization.
- The company will only use third-party services to store and process customer data that have been security reviewed and approved, and clearly communicated to customers.
- The company will use the latest and most secure encryption methods for all data in transit and at rest. Passwords will never be stored in plaintext.
- Customer data is processed only to provide the contracted services, it is never sold to third-parties or used for advertising or marketing purposes.

- The company maintains incident response plans. These are reviewed annually, communicated internally, and to customers.

The company has implemented policies, procedures, technical controls, and automation to ensure that these commitments are met.

Components of the System

Infrastructure
Managed Services use a local network server used to administer access to 3H employees. The server is housed in the 3H Office located in Saratoga Springs, NY. Access to the server is maintained in a locked room and access to the room is restricted to authorized personnel only. Backups are hosted offsite and encrypted using a third-party provider.

Creative Compliance is hosted in the 3H Datacenter. The 3H Datacenter is operated by the IS Team with limited authorized access. The datacenter uses alarms to monitor unauthorized access to the rented space. 3H uses state of the art fire suppression and maintains diesel generators to ensure that assets are protected and readily available in the event of a power outage. The 3H datacenter is in Saratoga Springs, NY. 3H uses vendors to house and encrypt backups at an offsite location.

Software
All software developed in-house by 3H is subject to secure system design, coding and testing standards that incorporate appropriate information security controls. All development work shall exhibit a separation between production, development, and test environments, and have a defined separation between development/test and production environments unless prohibited by licensing restrictions or the CTO grants an exception. All applications/programs access paths utilized in development or testing, other than formal user access paths, must be deleted or disabled before software is moved into production and the development process must be documented from the initiation phase, through implementation and ongoing maintenance and security considerations must be noted and addressed through each phase.

People
3HCS/Creative Compliance Software Solutions currently has 15 employees. The CEO oversees the managers/VPs of the departments, and all employees also have direct access to the CEO if needed.

Gary Harker, Esq.
Founder, Managing Principal
Gary is the Founder and Managing Principal of 3H Corporate Services, LLC based in Saratoga Springs, New York. He started 3H in 2003 and is considered one of the foremost experts in Insurance Regulatory Compliance in the U.S. He is a Licensed Attorney and currently serves as regulatory counsel for several entities within the insurance services sector as well as overseeing the day-to-day operations of 3H. Gary received his law degree from the University of Lancaster and an LL.M. in corporate law from the University of Edinburgh.
Beth Harker

Principal
Beth has been a principal with 3H since 2008. She oversees all aspects of Surplus Lines filings, and statutory agent representation for 3H. She has a deep understanding of all the 3H companies and her analytical skills have been instrumental in creating systems and efficiencies across the companies. She has a Bachelor of Science in Business Administration from the University of Florida, graduating with honors as a member of Phi Kappa Phi, and an M.B.A. from the University of Edinburgh.

Richard Richbart
Chief Technology Officer and Software Architect
Rich is the CTO of 3H and the Software Architect of the 3H Compliance Management System, ComplyINS Hub. An accomplished Information Technology Specialist, Rich founded the award-winning local technology firm Spa.Net in 1994. His extensive knowledge and experience in managing technology businesses, data center design and data center administration has earned him recognition as a prominent technology leader in the area. He joined the 3H team full time in 2019 after spending the previous two years working as a Special Consultant developing the ComplyINS application. Rich has sat on many local and national technology boards and has consulted as Technology Specialist and Network Architect to a wide range of government, education and nonprofit.

Katie Vianese
Vice President, Licensing Compliance
Katie is the head of 3H's Licensing Compliance Division. She has been with 3H for over 10 years and is an expert in all types of general and specialty licensing, including but not limited to Surplus Lines, TPA, MGA, Reinsurance, and Premium Finance. She is a *cum laude* graduate of Boston College.

Darrell Belch, Esq.
Vice President, Corporate Compliance
Darrell is a Vice President, Corporate Compliance and a member of the 3H licensing compliance team. Darrell is a licensed attorney and joined 3H in early 2019. Darrell supports both the licensing and corporate divisions and assists with legal research on various topics. Darrell holds a B.S. in Exercise Science from the University at Buffalo. Darrell worked for Manulife Financial in their Boston office and ZC Sterling (Qbe Insurance Group) and as an operations supervisor in their Raleigh office. A native of Saratoga Springs, Darrell returned to the Capitol area in 2004 and earned a J.D. with a concentration in Intellectual Property from Albany Law School.

Anastasia Welsh
Associate Project Manager
Anastasia Welsh is an Associate Project Manager at 3H. She started working in both 3H’s corporate and licensing divisions in 2016 and now focuses exclusively on licensing. She has extensive experience with producer and surplus lines licensing as well as surplus lines policy reporting. Anastasia received her B.A. at Mercyhurst University, graduating as a member of the Nu Delta Alpha Dance Honors Society, with a concentration in Dance Choreography/ Performance and Business Arts Administration.

Domenic D'Andrea
Product Support Manager
Domenic joined the team in January 2020, he oversees product support also working closely with the team on improvements, enhancements to the software and various projects. He also oversees the data center and office IT.

Previously employed for 20 years at SPA.NET, he performed IT support for both software and hardware for local business. Services included networking, web services, email setup, and support computer repair and virus removal. He worked several software companies as onsite tech for local government software, orthopedic and dental software companies.

Data
3H Corporate Services, LLC has an Information Classification scheme in place that allows staff to identify information that must be encrypted when being sent out of the business. The details are as follows:

- Confidential – Includes information such as advice given to clients, minutes of client meetings, client's strategy documentation, client finances or client personal employee or member details (up to and including name, address, NI, bank details)
- Internal – Includes information such as internal memos, ongoing project information or minutes of internal meetings
- Public – Includes information such as marketing brochures, client or company details or other information already available in the public domain

Procedures

Change Management

Change Management refers to a formal process for making changes to 3HCS's systems. The goal of change management is to increase awareness and understanding of proposed changes across an organization and ensure that all changes are made in a thoughtful way that minimize negative impact to services and customers.

This divisional policy applies to all changes to management, IT, and software development.

All changes to 3HCS must follow a structured process to ensure appropriate planning and execution.

By 3HCS definition there are three types of changes: (a) a Standard Change, (b) a Normal Change (of low, medium, or high risk), and (c) an Emergency Change.

Risk Assessment Process

Monitoring and reviewing the risk management process for the organization involves:

1. Determining whether each risk previously identified is still relevant to the organizational area

2. Reviewing the assessments given to likelihood and consequences for each risk
3. Reviewing the risk rating
4. Reviewing the adequacy of existing systems and controls to manage risk and
5. Reviewing the treatment strategies that previously have been considered and are currently being implemented.

Monitoring and review of risk are synchronized with normal business control processes; that is, at the occurrence of business performance benchmarking (e.g., quarterly). This process allows for the effective revision of previously identified risks, and associated treatment strategies being implemented for their mitigation, and provides the opportunity to determine and undertake the risk assessment process for any new risks which should be included.

HR Practices

3HCS seeks to ensure all employees are effectively and efficiently introduced to their new positions and the relevant policies, systems, and processes of 3HCS to perform and develop in their roles. 3HCS intends to comply with all federal and state regulations regarding the on-boarding of new employees.

After the acceptance of the position, HR will begin the on-boarding process to ensure a successful on-boarding experience.

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

3H Corporate Services, LLC's management has established a system of internal controls aligned with the integrated framework established by the Committee of Sponsoring Organizations (COSO). Management's approach to addressing the various components of the COSO integrated framework is described below.

Control Environment

Management Philosophy

Creative Compliance is committed to providing superior, best in class, service in all aspects of the business. The company is founded upon values of honesty, integrity, selflessness, and modesty, which form the foundation of success. Creative Compliance strives to accomplish important work and focus on great results. 3HCS is a team, highly aligned yet loosely coupled to allow flexibility. Employees are the most important asset, promoting corporate culture and the success of 3HCS.

Risk Assessment Process

A risk assessment is performed annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments, policies, and procedures are identified and the risks are formally assessed.

Monitoring and reviewing the risk management process for the organization involves:

- Determining whether each risk previously identified is still relevant to the organizational area
- Reviewing the assessments given to likelihood and consequences for each risk
- Reviewing the risk rating
- Reviewing the adequacy of existing systems and controls to manage risk, and
- Reviewing the treatment strategies that previously have been considered and are currently being implemented

Information and Communication Systems

Information security is the protection of information against accidental or malicious disclosure, modification, or destruction. Information is an important, asset of 3HCS that must be managed with care. All information has value to the Organization. However, not all this information has equal value or requires the same level of protection. Access controls are put in place to protect information by controlling who has the right to use different information resources and by guarding against unauthorized use. Formal procedures must control how access to information is granted and how such access is changed. This policy also mandates a standard for the creation of strong passwords, their protection, and frequency of change.

Monitoring Controls

3HCS uses a combination of products for monitoring control, AVG antivirus for email and endpoint protection, Zyxel firewall security software for monitoring network traffic and an extra layer of security. To monitoring patching, 3HCS uses Vulnerability Manager Plus.

Information Technology Processes and Controls

Personnel Security
User access control must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. These must be agreed upon by the CTO. Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

Access within software applications must be restricted using the security features built into the individual product. The IT department of the software application is responsible for granting access to the information within the system. The access must:

- Be compliant with the User Access Management policy and the Password policy.
- Be separated into clearly defined roles.
- Give the appropriate level of access required for the role of the user.
- Be unable to be overridden (with the admin settings removed or hidden from the user).
- Be free from alteration by rights inherited from the operating system that could allow unauthorized higher levels of access.
- Be logged and auditable.

Physical access cards are managed by building security staff. Access card usage is logged.

Physical Security and Environmental Controls
The office building is alarmed with key fob access and video monitoring.

3H information systems are physically secured. Access to IT equipment is restricted to only those whose responsibilities require they maintain the equipment or infrastructure primarily the CTO or his assigns. Dedicated space is committed to company server(s) and IT equipment and camera monitored. Physical documents containing Class IV2 data are shredded, and other documents securely disposed of along with unwanted information system components.

Data center access is via keycard for suite access, with video surveillance performed by the landlord. Data room access is enabled by a key and is restricted to two people.

Change Management
Change Management refers to a formal process for making changes to 3HCS's systems. The goal of change management is to increase awareness and understanding of proposed changes across an organization and ensure that all changes are made in a thoughtful way that minimize negative impact to services and customers.

System Monitoring
3H practice is to protect against unauthorized access use, disclosure, disruption, modification, or destruction of 3H information systems through implemented policies, procedures, and controls to protect data including technical measures to detect, respond and mitigate damage from a cyberattack. Controls include data encryption; malware defenses including anti-virus, anti-spyware, and host-based IDS features; security software management including software network management; email and web browser protection utilizing spam-filtering tools and blocking malicious web domains. Additional controls include managing the security configuration of network infrastructure devices (firewalls, routers and switches); inventory and control of hardware assets; managing operational use of ports, protocols and services on managed network devices; managing the security configuration of servers, workstations and portable devices (laptops, tablets, smart phones); control and management of application and system lifecycles to prevent systems and accounts from being leveraged; controlled use of administrative privileges on computers, applications and the network; wireless access controls; maintenance, monitoring and analysis of audit logs; and incident response and management.

Problem Management
The integrity and confidentiality of business information and availability of information systems are critical to 3H's viability. In the event of a potential or suspected breach of 3H information systems or information security the CTO must be alerted. The following is a non-exhaustive list of events that trigger reporting:

- Suspected compromise of PII (social security numbers, account numbers, etc.).
- Suspected compromise of Login Credentials (username, password, etc.).
- Suspected virus, malware, or Trojan infection.
- Loss or theft of any device (company used or personal devise that contains company information).
- Any attempt by a person to obtain a user's password over the telephone or by email.
- Misplaced portable device that contain PII.
- Accidental unauthorized email of PII.

In the event of a Security Breach involving 3H client Non- Public Information (Class IV Data4) notice will be provided to the client immediately upon determination of the Security Breach. 3H's data backup is designed to ensure discovery of key network servers, email application data bases, webpages, and servers.

Data Backup and Recovery
3H's data backup is designed to ensure discovery of key network servers, email application data bases, webpages, and servers. Data stored on information systems including servers, Exchange mailbox stores, telephone systems, and FIRM's cloud-based platform will be backed

up daily. Logged information generated from each back up will be checked for errors. The CTO or his assign will identify problems and take any necessary corrective action to reduce risk. Random test restores will be done regularly to verify backups have been successful, and the CTO or his assign will maintain records demonstrating review of logs and test scores. Prior to the retirement or disposal of media, the CTO or his assign will ensure that the media no longer contains active backup images and that the media's former contents cannot be read or recovered by an unauthorized party. Documentation must be kept and undated.

Business Continuity – Cybersecurity Disruptive Event

A cybersecurity disruptive event includes ransomware or other cyberattack, environment catastrophes, hardware or software failures or building accessibility which cause a malfunction of 3H Information System such as a network outage or power failure. The objective of the plan is to respond to the disruptive event as quickly as possible to return 3H to business as usual as quickly as possible. Preventing loss of 3H resources including hardware, data, and physical IT assets, minimizing related IT downtown, and keeping the business running are cybersecurity business plan priorities.

Disclosure of Security Incidents

3H Corporate Services, LLC did not identify any system incidents as of December 31, 2021, that: (a) were the result of controls that were not suitably designed, or (b) otherwise resulted in a significant failure in the achievement of one or more of the Company's service commitments and system requirements.

V. SUBSERVICE ORGANIZATIONS

3H Corporate Services, LLC uses subservice organizations to help support its Corporate and Insurance Licensing Services system. The scope of this report does not include the controls and related Trust Services Criteria at the subservice organizations. The following is a description of the services provided by each subservice organization and the controls that are expected to be implemented:

Subservice Organization	Services Provided
Carbonite	Infrastructure Hosting
LogMeIn, Inc.	VPN Software

The following table presents controls that are assumed to be implemented by the subservice organization, which 3H Corporate Services, LLC has identified as necessary to achieve certain Trust Services Criteria stated in the system description.

Applicable Trust Services Criteria	Subservice Organization Controls Expected to be Implemented to Meet the Applicable Trust Services Criteria
CC2.3 – COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	• Feature updates or any major changes to the services provided must be communicated to clients in a timely manner. • Incidents or security breaches of any kind are communicated to clients in a timely manner.
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.	• Client data is stored on a separate network to mitigate the impact during a security breach. • All client data at rest is to be encrypted. • Any client data sent through public means must be encrypted. • All client data is replicated at an offsite location in the event of a system failure. This allows the organization to access client information and ensure a smooth customer experience.
CC6.6 – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	• Firewalls are placed on the perimeter of the network to monitor for and block any unwanted network traffic. • Firewalls should be configured with a default deny-all rule and only allow traffic in through exception. • Firewall configuration settings are reviewed on a quarterly basis and updated as necessary.

Monitoring of Subservice Organizations

3H Corporate Services, LLC monitors its subservice organizations throughout the year by evaluating security bulletins that may address potential issues from Carbonite and LogMeIn. Additionally, a vendor risk assessment is performed for all vendors on a periodic basis that have access to confidential data or impact the security of the system. Management investigates issues and confirms that subservice organizations are meeting the service expectations of 3H Corporate Services, LLC.

VI. COMPLEMENTARY USER ENTITY CONTROLS

3H Corporate Services, LLC's controls surrounding the Corporate and Insurance Licensing Services System were designed with the assumption that certain controls would 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 auditors should consider whether the following controls have been placed in operation at user organizations:

- Client organizations are responsible for understanding and complying with their contractual obligations to 3H Corporate Services, LLC, as well as 3H Corporate Services, LLC's privacy policy and terms of service.

- Client organizations are responsible for communicating any incident or security breach that could affect the services provided by 3H Corporate Services, LLC.

- Client organizations are responsible for communicating any law or industry changes that could affect the services provided by 3H Corporate Services, LLC.

VII. INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF CONTROLS

The trust services criteria relevant to *Security* address the need for information and systems to be protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

Security refers to the protection of

i. information during its collection or creation, use, processing, transmission, and storage, and

ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

CONTROL ENVIRONMENT

CC1.1: ***The entity demonstrates a commitment to integrity and ethical values.***

Control No.	***Control Activity***
CC 1.1.1	Management monitors employees' compliance with the code of conduct through monitoring of performance and employee complaints.
CC 1.1.2	Personnel are required to read and accept the employee handbook annually, which is housed at their ADP (payroll online account) and includes the code of conduct and cybersecurity policy.
CC 1.1.3	Personnel must pass a criminal background check before they may be hired by 3H or third-party vendors hired by the entity.

CC1.2: ***The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.***

Control No.	***Control Activity***
CC 1.2.1	The Security Steering Committee Charter includes roles and responsibilities relevant to security.
CC 1.2.2	The Security Steering Committee that provides visibility into the enterprise security program.
CC 1.2.3	3H evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revises these when necessary to help meet changing commitments and requirements.

CC1.3: ***Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.***

Control No.	***Control Activity***
CC 1.3.1	Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors.
CC 1.3.2	3H evaluates its IT organizational structure as part of the business planning.

CC1.4: ***The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.***

Control No.	***Control Activity***
CC 1.4.1	3H hiring procedures include a comprehensive screening of candidates for key positions and consideration of whether the educational requirements match the job requirements. Background screening policies requires background checks to be performed on all new employees.
CC 1.4.2	Job descriptions provide for security roles where applicable and are drafted in line with 3H policies and standards, including the information security policy.

CC1.5: ***The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.***

Control No.	***Control Activity***
CC 1.5.1	Roles and responsibilities are defined in written job descriptions.
CC 1.5.2	3H evaluates its IT organizational structure as part of the business planning.

COMMUNICATION AND INFORMATION

CC2.1: ***The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.***

Control No.	***Control Activity***
CC 2.1.1	3H performs an assessment at least monthly to identify key information system processes that process relevant data into information to support internal control.
CC 2.1.2	3H performs a vulnerability assessment semi-annually to identify the required internal controls for key information systems, which help to achieve the entity's service commitments and system requirements.

CC2.2: ***The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.***

Control No.	***Control Activity***
CC 2.2.1	Policy and procedures documents for significant processes that address system requirements are available on the intranet.
CC 2.2.2	Personnel are required to attend annual security, confidentiality, and privacy training.
CC 2.2.3	Personnel are required to read and accept the code of conduct and the statement of confidentiality and privacy practices upon hire and annually thereafter.

CC2.3: ***The entity communicates with external parties regarding matters affecting the functioning of internal control.***

Control No.	***Control Activity***
CC 2.3.1	3H's system description is outlined in various documents including standard operating procedures, employee agreements, security procedures and various other policies and procedures.

RISK ASSESSMENT

CC3.1: ***The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.***

Control No.	*Control Activity*
CC 3.1.1	A risk assessment is performed annually. As part of this process, threats to security are identified and the risk from these threats is formally assessed.
CC 3.1.2	Security processes and procedures are revised by the Security Officer based on the assessed threats.
CC 3.1.3	Data owners annually review data access rules and request modifications based on defined security requirements and risk assessments.
CC 3.1.4	Whenever new data is captured or created, the data is classified based on security policies.
CC 3.1.5	Propriety of data classification is considered as part of the change management process.

CC3.2: ***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.***

Control No.	***Control Activity***
CC 3.2.1	3H has a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.
CC 3.2.2	During the risk assessment and management process, risk management office personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.

CC3.3: ***The entity identifies and assesses changes that could significantly impact the system of internal control.***

Control No.	***Control Activity***
CC 3.3.1	The Finance department reviews internal controls relating to fraud management on an as-needed basis. Risk and controls matrices are updated according to internal findings by the Finance department.

CC3.4: ***The entity identifies and assesses changes that could significantly impact the system of internal control.***

Control No.	***Control Activity***
CC 3.4.1	A risk assessment is performed annually. As part of this process, threats to security are identified and the risk from these threats is formally assessed.
CC 3.4.2	Security processes and procedures are revised by the security officer based on the assessed threats.

MONITORING ACTIVITIES

CC4.1: ***The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.***

Control No.	*Control Activity*
CC 4.1.1	Logging and monitoring software is used to collect data from system infrastructure components and endpoint systems and used to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity or service requests. This software sends a message to the operations center and security organization and automatically opens a priority incident or problem ticket and change management system record item.
CC 4.1.2	Operations and security personnel follow defined protocols for resolving and escalating reported events.
CC 4.1.3	A risk assessment is performed annually. As part of this process, threats to security are identified and the risk from these threats is formally assessed.

CC4.2: ***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.***

Control No.	***Control Activity***
CC 4.2.1	Security processes and procedures are revised by the security officer based on the assessed threats.
CC 4.2.2	All security deficiencies rated as serious threats are reported to senior management.

CONTROL ACTIVITIES

CC5.1: ***The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.***

Control No.	***Control Activity***
CC5.1.1	A risk assessment is performed periodically. As part of this process, threats to security are identified, and the risk from these threats is formally assessed.
CC5.1.2	Data owners periodically review data access rules and request modifications based on defined security requirements and risk assessments.

CC5.2: ***The entity also selects and develops general control activities over technology to support the achievement of objectives.***

Control No.	***Control Activity***
CC5.2.1	Remediation plans are proposed, and implementations are monitored.

CC5.3: ***The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.***

Control No.	***Control Activity***
CC5.3.1	Policies are stated in the Customer Cyber Security Policy and the Employee Handbook.

Supplemental Criteria: 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.***

Control No.	*Control Activity*
CC6.1.1	Secure log on. Each user logon is unique with permissions only for their own records. Dual authentication required on new devices or web browsers.
CC6.1.2	Login sessions are terminated after three unsuccessful login attempts. LogMeIn (VPN) software is used to permit remote access by authorized users. Users are authenticated by the LogMeIn VPN server through specific “client” software and user ID and passwords.

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.***

Control No.	***Control Activity***
CC6.2.1	User password frequency is set to 90 days.
CC6.2.2	Access to the network requires approval from the appropriate management personnel prior to being granted access.

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.***

Control No.	***Control Activity***
CC6.3.1	When an employee is terminated, all passwords are reset or the user logon it deleted including any cloud software access.
CC6.3.2	Password controls are set on the Server in Group Policy for the active directory.

CC6.4: ***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.***

Control No.	***Control Activity***
CC6.4.1	Data center access is via key card for suite access, and video surveillance is performed by the landlord. Data room access is enabled by key and is restricted to two people.
CC6.4.2	Physical access cards are managed by building security staff. Access card usage is logged. Logs are maintained and reviewed by building security staff.

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.***

Control No.	***Control Activity***
CC6.5.1	In the Cyber Security Policy, data disposal will use best practices.

CC6.6: ***The entity implements logical access security measures to protect against threats from sources outside its system boundaries.***

Control No.	***Control Activity***
CC6.6.1	Login sessions are terminated after three unsuccessful login attempts. LogMeIn (VPN) software is used to permit remote access by authorized users. Users are authenticated by the LogMeIn VPN server through specific "client" software and user ID and passwords.
CC6.6.2	Firewall reports are emailed daily.

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.***

Control No.	***Control Activity***
CC6.7.1	When transmitting any PI information to a client we create a secure SharePoint instance for the client, then remove the data and share.
CC6.7.2	Log-on sessions are encrypted using industry standard https using secure certificates.

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.***

Control No.	***Control Activity***
CC6.8.1	AVG antivirus in installed on computers, and network antivirus runs on the firewall.

Supplemental Criteria: 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.***

Control No.	*Control Activity*
CC7.1.1	Logging and monitoring software (AVG and zyzel router security package) is used to collect data from system infrastructure components and endpoint systems and used to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity or service requests. This software sends a message to the operations center and security organization.
CC7.1.2	Using AVG, zyzel router security software and vulnerability management software to run continual security and vulnerability assessments (daily and weekly logs).

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.***

Control No.	***Control Activity***
CC7.2.1	Carbonite is used for offline backup, monthly checks on backing up, and quarterly testing of restoring sample documents.

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.***

Control No.	***Control Activity***
CC7.3.1	AVG antivirus reports and firewall router reports are emailed daily and evaluated by the information security team.

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.***

Control No.	***Control Activity***
CC7.4.1	Users are provided instructions for communicating potential security breaches to the information security team. The information security team logs incidents reported through phone calls, support email and website form to log online ticketing (Hub Spot).

CC7.5: ***The entity identifies, develops, and implements activities to recover from identified security incidents.***

Control No.	***Control Activity***
CC7.5.1	Users are provided instructions for communicating potential security breaches to the information security team, employees are provided instructions in the Employee Handbook and customers are provided instructions through the Cybersecurity Policy. The information security team logs incidents reported through online form submission, email, and phone.

Supplemental Criteria: Change Management

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.***

Control No.	*Control Activity*
CC8.1.1	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 3H's risk management process and relevant risk management data is updated to reflect the planned incident and problem resolution.
CC8.1.2	Changes to system infrastructure and software are developed and tested in a separate development or test environment before implementation into production.

Supplemental Criteria: Risk Mitigation

CC9.1: ***The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.***

Control No.	*Control Activity*
CC9.1.1	A risk assessment is performed annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments, policies, and procedures are identified, and the risks are formally assessed.

CC9.2: ***The entity assesses and manages risks associated with vendors and business partners.***

Control No.	***Control Activity***
CC9.2.1	The risk management program includes the use of insurance to minimize the financial impact of any loss events.
CC9.2.2	The entity has documented and communicated security policies that define the information security rules and requirements for the service environment.
CC9.2.3	The entity has clauses in its agreements with vendors and business partners to terminate relationships when necessary.
CC9.2.4	Vendor and business partner access is removed upon termination through a termination checklist, and access is revoked within 24 hours as part of the termination process.