Information Security Standards for Allstate Suppliers (ISSAS)

This ISSAS is aligned to the National Institute of Standards and Technology for the Cyber Security Framework ("NIST") and the International Organization for Standardization 27000 family of standards ("ISO"). The ISSAS pertains to the scope of the services provided by the Supplier to Allstate. Additional security requirements not included in this document may be specified in the Agreement or in an applicable Statement of Work or Schedule.

I. Definitions

Allstate means Allstate Insurance Company and its affiliates, as applicable.

Asset means an Allstate or Supplier owned major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, non-electronic media, a logically related group of systems, or information.

Cloud Technology means any externally hosted technology offering which enables on-demand Network access to a shared pool of configurable computing resources (*e.g.*, software as a service, platform as a service, and infrastructure as a service).

Computer means any desktop or laptop, mobile device (e.g., mobile phone, Smartphone, tablet), server, network, and/or storage device that, (i) is involved in the performance of the Services, (ii) may be used to access a Network or an Environment, or (iii) may access or store ISSAS Information.

Environment means any computing architecture or system (logical or physical), including but not limited to cloud, development, testing, staging, production and/or backup application, to which Supplier is provided access to, or is used to provide Services by the Supplier.

Facilities means (i) any offices, data centers or all other locations (whether owned or managed by Allstate, an Allstate agency, Supplier or Supplier's third party) from which ISSAS Information, Environments or Networks may be accessed or (ii) any permanent or non-permanent location handling or storing Allstate Assets.

ISSAS Information means any information provided by or obtained on behalf of Allstate including physical or electronic data that contains Personally Identifiable Information, Protected Health Information (PHI), as defined in 45 CFR 160.103), Non-Public Information as defined in 23 NYCRR Part 500.01(g), Material Non-Public Information, and Allstate Trade Secrets.

Personally Identifiable Information means information that identifies, relates to, describes, is capable of being associated with or could reasonable be linked, directly or indirectly with a particular individual, device or household.

Material Non-Public Information (MNPI) means information that has NOT been disseminated by a method that is reasonably designed to provide broad, non-exclusionary distribution of the information to the public, and there is a substantial likelihood that, considering all of the surrounding facts and circumstances, a reasonable investor would consider material to an investment decision.

Multi-factor authentication (MFA) means authentication through verification of at least two of the following types of authentication factors: (i) knowledge factors, such as a password; (ii) possession factors, such as a token; or (iii) inherence factors, such as a biometric characteristic.

Network means any Allstate network to which Supplier is provided access in connection with the performance of Services under the Agreement and/or any Supplier network that may access or store ISSAS Information.

Security Incident means (i) any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt, or misuse Services, ISSAS Information, a Network, an Environment, or information stored on such Environment; (ii) any event in which any Personally Identifiable Information may have been lost, or accessed, acquired, used or disclosed without authorization by law; and/or (iii) any other breach in the protection of such Personally Identifiable Information, including any breach of the Personally Identifiable Information obligations in the Agreement.

Services shall have the same meaning ascribed to it in the Agreement, provided that if "Services" is not defined in the Agreement, "Services" means the products, services, or access and use of Supplier's software and/or hosted services provided by Supplier to Allstate under the Agreement or any applicable schedule or statement of work thereto.

Supplier shall have the same meaning ascribed to it in the Agreement, provided that if "Supplier" is not defined in the Agreement, for purposes of this ISSAS, "Supplier" means the counterparty providing Services to Allstate hereunder.

Trade Secrets include any valuable commercial information that provides a business with an advantage over competitors who do not have that information. Examples of Trade Secrets include, but are not limited to, inventions, ideas, compilations of data, formulas, plans, patterns, processes, programs, tools, techniques, mechanisms, or devices not generally known or readily ascertainable by the public and used by a business to make itself more successful.

II. Standard Security Requirements.

Supplier will maintain the following enterprise controls for any Networks and/or Computers that may access Allstate Networks, Environments and/or ISSAS Information.

A. Risk Assessment and Treatment

Supplier will implement and maintain a formalized risk governance plan, policy, and a continuous risk assessment process demonstrating Supplier's ability to identify, quantify, prioritize, and mitigate risks.

Each risk governance plan will, at a minimum, include Supplier conducted risk assessments on a no less than annual basis to identify any potential risks associated with the then current cybersecurity landscape.

Supplier will provide Allstate with documentation outlining such policies and procedures upon request. During the term of the Agreement, Supplier will not amend or modify any policies or procedures in a manner that diminishes the security controls previously in effect.

Supplier will maintain policies and procedures as part of Supplier's overall information security program to assess and manage risk associated with Supplier's third parties. This will include processes that encompass risk ranking, risk assessment and remediation of risks. This program will be in place prior to the effective date of the Agreement, and continually be in force with such third-parties and made available to Allstate upon request.

B. Security Policy

Supplier will provide management direction and support for information security in accordance with business requirements and applicable laws and regulations. Supplier will set a clear policy direction in line with business objectives and demonstrate support for and commitment to information security through the issue, acceptance and maintenance of a written information security policy across the organization. This policy will be based on Supplier's risk assessment and address the following areas:

1. information security;
2. data governance, classification and retention;
3. asset inventory, device management and end of life management;
4. access controls, including remote access and identity management;
5. business continuity and disaster recovery planning and resources;
6. systems operations and availability concerns;
7. systems and network security and monitoring;
8. security awareness and training;
9. systems and application security and development and quality assurance;
10. physical security and environmental controls;
11. customer data privacy;
12. vendor and third-party service provider management;
13. risk assessment;
14. incident response and notification; and
15. vulnerability management.

C. Organizational Security

Supplier will at all times have a security function with clearly defined information protection roles, responsibilities and accountability.

D. Asset and Information Management

Supplier will implement a formalized asset management program, which includes a data classification process – a process for documenting and maintaining an inventory of hardware, software and information assets. The documentation relevant to each asset will include an organizational owner who is responsible for the asset throughout its life cycle.

1. Encryption: Supplier's information security policy will ensure all ISSAS Information is encrypted when in transit or at-rest using industry standard encryption methods.
2. Supplier will have processes and procedures in place to protect and track ISSAS Information during physical transportation to prevent unauthorized access and/or disclosure.
3. ISSAS Information will not be stored by the Supplier on portable storage devices such as flash drives, USBs, or external hard drives. Supplier will have controls such as Mobile Device Management (MDM) or equivalent to restrict the use of portable storage devices or mobile communication devices.
4. When no longer required to satisfy the scope of work under the Agreement or to meet legal requirements, Supplier will promptly return ISSAS Information to Allstate or destroy it in accordance with the most current NIST standard of destruction and sanitization (*e.g.*, NIST SP 800-88).
5. For purposes of this Agreement, each environment in which Supplier stores ISSAS Information is considered a production Environment, subject to the requirements of this ISSAS. Supplier will not store ISSAS Information in Environments, such as testing, that do not meet such requirements.

E. Human Resources Security

Supplier will establish and maintain formal policies for human resources security for all personnel, including officers, employees and contractors, including:

1. conducting appropriate and allowable background screening;
2. acknowledgement of the Supplier's privacy, security awareness, information security and risk policies at onboarding and at least annually thereafter; and
3. formal information security and privacy training at onboarding and at least annually thereafter, including social engineering exercises.

F. Physical and Environmental Security

Supplier will restrict physical access to data and systems by utilizing an industry standard layered security approach that includes cameras, access logs, and badge or key/PIN controlled entries and exits. Environmental security controls including, but not limited to, climate control, fire suppressants and backup power will also be in place at all Facilities containing ISSAS Information.

G. Operations Management

Supplier will maintain documented operating procedures to ensure the effective management, operation, integrity and security of their information systems and data. This will be incorporated in the following programs and processes:

1. Supplier will ensure the most relevant, up-to-date, tested, and approved patches are installed for all Supplier Computers and systems.
2. Supplier will utilize an industry standard change management program for the implementation of all changes. Where appropriate, change management procedures will include vulnerability testing, penetration testing, and audit of controls prior to execution of change.

H. Access Control

Supplier will ensure control and governance of its personnel's access to ISSAS Information, as well as its systems, Networks, Computers, and Facilities.

1. Access provisioning to Supplier Environments, Networks, and ISSAS Information will adhere to the principle of least privilege, defined as the practice of allowing only authorized users the minimum level of access required to perform their respective job functions.
2. All access rights must be managed through a centralized process/system ensuring:
    a. All accessed requested are reviewed and approved prior to the granting or removal of access;
    b. A system is in place for the logging and review of access provisioning; and
    c. Separation of Duties is established so no person or team has sole control over access provisioning.
3. Supplier will, at minimum annually, review all user access privileges and remove or disable accounts or access that are no longer needed.
4. Supplier will ensure that its password controls meet industry best practices and follow internal policies for personnel who have access to systems or Environments with ISSAS Information.

5. Access to any Supplier Cloud Technology, Computer, Environment, or Network that stores or has access to ISSAS Information from the Internet must be secured with MFA.
6. Access to Supplier's privileged accounts must require MFA.
7. Supplier will protect system access from unauthorized boot procedures.
8. Supplier will ensure role-based access provisioning at both the user level and client level.

I. Secure Development

Supplier will implement software security policies, standards and procedures to ensure that stakeholders, business owners and internal governing bodies have a common understanding of business practices and risk management expectations. Supplier will follow an industry standard systems development life cycle ("SDLC") process to confirm secure coding practices are utilized during development.

Supplier's SDLC will include security best practices within the key development phases of the application. This includes code reviews of applications using industry standards, such as Open Web Application Security Project (OWASP).

Supplier will ensure that all web-facing applications are developed with controls in place for input validation.

J. Compliance

Supplier will implement procedures that ensure compliance with Supplier's legal, regulatory, statutory and/or contractual obligations related to any information security or privacy requirements and will cooperate and assist Allstate with any of Allstate's compliance obligations as it relates to the ISSAS Information. If the Supplier is providing Services subject to any additional legal requirements or regulations Supplier must also adhere to those requirements; including without limitation any legal requirements or regulations that were not contemplated at the time of contracting.

K. Mobile Device Management

If ISSAS Information is accessible through mobile devices, Supplier will utilize and follow an industry standard mobile device management policy which includes capabilities such as remote-wipe, encryption of data, and password protection.

L. Network Security

Supplier will maintain documented operating procedures and technological controls to ensure the effective management, operation, and security, of Supplier's Networks. Supplier will maintain, and provide to Allstate upon request, an up-to-date network diagram, including all data interfaces for secure data transmissions. This program will consist of, but is not limited to, the following security controls: (i) threat detection and prevention, (ii) network activity logging and monitoring; (iii) network segmentation; (iv) network intrusion detection and prevention; (v) host intrusion detection and prevention; and (vi) firewalls.

If Supplier uses wireless networks, Supplier will use industry standard wireless encryption protocols when the Supplier's access points provide access into systems and hardware where ISSAS Information can be accessed or stored.

M. Logging and Monitoring

Supplier will comply with relevant security best practices for the monitoring and logging of its Cloud Technology, Computers, Environments, Networks, Facilities, and Environments. Logs will be kept for the duration that is required by applicable law or Supplier's record retention policy, whichever is longer.

N. Threat Management

Supplier will scan its Environment(s) for known security vulnerabilities and threats at least monthly and remediate identified vulnerabilities according to a documented timeline. Supplier shall conduct, at minimum annually, a penetration test of each of their Environments, and provide a summary of the results of those test(s) to Allstate.

O. System Hardening

Supplier will ensure that a formalized process is in place for securely building, configuring, hardening, and managing Supplier Environments, including Supplier Cloud Technology, as well as hardware, software, or any devices used to connect to the Allstate network or installed in any Allstate environment.

P. Cloud Security

If Supplier hosts cloud Services internally, or through a third-party Cloud Service Provider (CSP) Supplier will comply with all requirements set forth below:

1. User access to ISSAS Information must be granted through federated IDs. Supplier's administrator's access to the solution will be through SSO with MFA, in addition to IP whitelisting.
2. Encryption will be managed solely by Allstate or Supplier, meaning such that Cloud Technology service CSP personnel must do not have access to ISSAS Information.
3. Supplier will ensure role-based access provisioning at both the user level and client level.

III. Security Incident Management and Reporting

A. Incident Management Program

Supplier will have an incident management program, including a written incident response plan, to ensure an effective and consistent process for identifying, managing, and controlling a Security Incident. Such incident management program must be in line with best practices for the applicable industry. The written incident response plan must include, but is not limited to, the following for different types of events, including ransomware events:

1. Proactive measures to investigate and mitigate disruptive events and ensure operational resilience, including but not limited to incident response, business continuity and disaster recovery plans;
2. Clear guidelines and channels for Supplier employees to follow to escalate concerns about data security and potential Security Incident;
3. Internal processes for responding to a Security Incident;
4. Goals of the incident response plan;
5. Definition of clear roles, responsibilities and levels of decision making authority;
6. External and internal communications and information sharing;
7. Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
8. Documentation and reporting regarding Security Incidents and related incident response activities
9. Recovery from backups; and
10. Updates to the incident response plan as necessary.

B. Reporting Security Incidents

1. Supplier will immediately investigate any reported or suspected Security Incident(s) and will take reasonable steps to mitigate the effects and minimize damage resulting from the Security Incident(s).
2. Supplier must call and email Allstate to report any Security Incident immediately or no later than 24 hours after becoming aware of a Security Incident, regardless of its impact to ISSAS information. Supplier must provide Allstate with detailed information related to the Security Incident. Supplier must be prepared to provide detailed and frequent updates, as requested by Allstate.
3. Any Security Incident involving access to Personal Information or Confidential Information of Allstate shall be considered Confidential Information of both parties. Supplier shall fully cooperate with Allstate should Allstate decide to investigate the Security Incident. If a Security Incident involves any Personal Information, then if requested by Allstate, Supplier will assist Allstate with any Allstate communications including communications with the media, any affected Persons (by press release, telephone, letter, website or any other method of communication), and any regulatory authorities. The content and method of any such communications will be determined by Allstate at Allstate's sole discretion.
4. Allstate maintains a Security Operations Center that is continuously staffed. Security Incident(s) must be reported within 24 hours of awareness via one of the following methods:

   Email: cyber@allstate.com
   Phone: (888) 248-2488

5. In the event of a Security Incident, Supplier will be expected to share all relevant information and evidence as reasonably requested by Allstate. This information may include indicators of compromise, relevant logs, forensic and third-party reports, and an overview of Supplier's process for eradication and remediation.

Provided that all data relevant to the Security Incident remains intact, Supplier may redact proprietary information from the logs.

6. Allstate reserves the right to use an Allstate designated third-party supplier to conduct forensic investigation of the Security Incident, at Allstate's expense.

C. Security Incident Communications

1. Other than pursuant to a valid request from law enforcement or otherwise required by law, Supplier may not make any statements regarding the Security Incident(s) and its impact to Allstate to any third party (*e.g.*, the media, Allstate customers) without the explicit written authorization of Allstate.
2. In its response to the Security Incident, Supplier must meet all appliable legal requirements. Additionally, where legal notification is required, notification will be completed by the Supplier at Supplier's expense, in collaboration with Allstate. If directed by Allstate, credit monitoring must also be provided at Supplier's expense. In instances where notification is not legally required, upon Allstate's request, notification and credit monitoring may be provided at Supplier's expense.

IV. Additional Requirements

A. Security Communications and Assessment

1. Supplier will provide to Allstate contact information of person(s) at Supplier Allstate may contact in relation to any information security issues or Security Incidents.
2. Supplier will notify Allstate of any material change to an Environment that hosts ISSAS Data, including but not limited to re-platforming, moving from on-premise to cloud hosting, or moving from one cloud host to another.
3. If requested, Supplier will (or cause its subcontractors to) certify its compliance with the requirements of the ISSAS and provide written responses to any reasonable questions submitted to Supplier by an Allstate-designated representative, or a request to provide an independent audit report.
4. Allstate will require a security assessment, audit, and/or certification of the ISSAS on an annual basis, in the event of a Security Incident, and in the event of a material change to an Environment that hosts ISSAS Data. Allstate may perform security assessments or audits (including audits related to Supplier's confidentiality obligations) at Allstate's expense, to confirm compliance with the ISSAS and industry best practices. Supplier cannot charge Allstate for any such audit (*i.e.*, for Supplier time spent on audit). Supplier must provide documents or artifacts as required by Allstate to conduct such audit(s) or assessment(s) at no additional costs to Allstate. The Supplier must keep all ISO or SOC2 Type II certifications current and in good standing and upon request of Allstate, provide copies thereof.
5. Within a mutually agreed upon timeframe, Supplier will correct security issues identified in a security assessment or audit performed by Allstate, or a third party working on behalf of Allstate.

B. Geographical Restrictions

Supplier will not allow ISSAS Information to be stored, processed, transmitted, or accessed outside of the country of origin without Allstate's prior written approval or as detailed in an Agreement between the Parties.

C. Supplier Access to Allstate-Managed Environments

When applicable, this section sets forth the terms that apply to the Supplier's access to and use of Allstate's Network, Environment, and information technology resources.

1. Supplier may only use Allstate Networks, Assets, Computers, and Facilities for the sole purpose of providing the Services.
2. Allstate reserves the right to: (i) monitor all Supplier activity while connected to the Allstate Network or Allstate Environment, and (ii) revoke the Supplier access privileges at any time when necessary to (a) perform maintenance across Allstate-Managed Environments or (b) protect the confidentiality, availability, or integrity of Allstate-Managed Environments or ISSAS Information.
3. Unless stated within the terms of the Agreement, upon termination, Supplier will return Allstate Assets promptly, but not exceeding 60 calendar days.