AAIS Membership
Data Security Policy

Definitions

"***Data Assets***" means facilities, information applications, systems, and networks associated with accessing, processing, storing, or transmitting Protected Data.

"***Protected Data***" means all data and information, whether in written or electronic form, that is (a) submitted to AAIS by a Member or any of its Affiliates; (b) obtained, developed or produced by AAIS in connection with the Services; or (c) derived from or produced as a result of using any data or information in (a) or (b).

"***Security Breach***" means any incident where (a) there is any unauthorized access to, disruption or misuse of, any Data Asset or Protected Data; (b) there is any loss of, unauthorized access to or acquisition of, or blocked access or use of, Protected Data; (c) Protected Data has been transmitted, disclosed, stored, or disposed of in an unencrypted or unsecured format in violation of the this Agreement; or (d) notice to individuals, regulators or others may be required under Applicable Law.

"***Security Program***" means AAIS's comprehensive information security program and controls.

"***AAIS Personnel***" includes all Contractors (including AAIS's employees) and any of AAIS's other agents, vendors, consultants, service providers or subcontractors that have access to Protected Data or Data Assets.

Information Security Safeguards

1.0 Security Program

1.1. General. AAIS at its own cost and expense, establish, adhere to, and maintain a Security Program based upon the NIST Cybersecurity Framework to (a) protect the integrity, availability, security and confidentiality of Protected Data; (b) assess and mitigate information security risk; and (c) provide for the secure disposal of Protected Data. The Security Program must comply with all Applicable Law and shall include widely accepted industry standard methodologies for (a) restricting and controlling access to Protected Data (including for authorizing and removing access permissions for AAIS Personnel); (b) providing annual information security training to all AAIS Personnel; (c) data segregation, governance, and classification of Protected Data; (d) multi-factor authentication/password administration (including required multi-factor authentication for all AAIS Personnel when Protected Data is accessed); (e) secure remote access; (f) encryption (including encryption of Protected Data in transit); (g) network and application security (including network intrusion detection, firewalls, anti-virus protections, security software patching), including as described in 2.2; (h) data destruction; (j) physical security and environmental controls; (k) Security Breach prevention, detection and response; (l) third party risk assessment and management; (m) penetration testing and vulnerability assessment; and (n) secure software development and scanning.

Upon Member request, AAIS shall provide the most recent SOC2 or relevant from an independent source certifying the Security Program's compliance with such standards. AAIS shall document its Security Program and keep it current in light of changes in Applicable Law and insurance industry standards. AAIS shall not materially weaken any of the foregoing components of the Security Program without Member communication and consent through the

Board of Directors.

1.2 Network and Host Security. AAIS shall use and maintain network intrusion detection, firewalls and anti-virus protection. AAIS shall implement widely-accepted industry best practices with respect to system hardening on systems hosting Protected Data, including disabling all unnecessary and insecure services and protocols. AAIS shall install all security vulnerability patches for its systems software and applications in accordance with documented AAIS patch management procedures that prioritize the remediation of vulnerabilities based on risk. Patches classified as critical or high shall be deployed as soon as practicable under the circumstances but by not less than 30 days from the time when it is made available by the manufacturer. For AAIS services that may be accessed via the web, the AAIS shall also provide options for reducing risk through secure technologies and techniques including IP filtering, application gateway or network packet filtering firewalls and browser-type restrictions.

2.0 Security, Risk, Compliance and Vulnerability Assessments.

2.1 Security Assessments. On at least an annual basis, AAIS shall communicate and make available all third party audit reports and a statement of standard security protocols that inform and support Member IT organizations' internal audits. If any medium or high risk control gaps are identified (including by a third party security rating provider), AAIS shall remediate such gaps as through transparent and accountable review and implementation in communication with the Board and member stakeholders. AAIS shall not materially weaken its security practices as described in periodic communications without the consent of Members through the Board of Directors. Notwithstanding the limitations above, following the occurrence of a Security Breach, AAIS shall conduct an independent onsite or virtual security assessment, the results of which shall be disclosed to the Members. Further, prior to making a major change to its Data Assets or Security Program, AAIS shall first notify the membership with a minimum of 5 business days unless of a critical nature.

2.2 Risk Assessments. AAIS shall conduct annual security risk assessments with respect to all Data Assets and, at Members' request, provide any Member with report of the findings and recommendations. AAIS shall timely remediate any items identified in such assessment.

2.3 Compliance Assessments. AAIS shall conduct annual self-audits with respect to the Security
Program and, at Member request, provide a report of the findings and recommendations. AAIS must promptly cure any non-compliance identified by such audits.

2.4 Vulnerability Assessments. AAIS shall conduct semi-annual vulnerability assessments of all Data Assets to identify, quantify, rank and mitigate weaknesses in the Security Program. AAIS shall conduct an annual perimeter network penetration test using a qualified independent party. AAIS shall timely remediate all critical and high risk findings identified in such assessments.

3.0 Permissability Access/Storage, Audit Logs, Integrity and Destruction of Data.

3.1 Access Limitations. AAIS shall not allow access to Protected Data except for (a) AAIS Personnel who have a need to access Protected Data pursuant to this Agreement and whose authorization has been approved in accordance with the Security Program; and (b) the Member or its designated representatives.

3.2 Use of Third Party Service Providers. If AAIS uses a third party service provider to access, process, or store Protected Data, then AAIS shall include in its Security Program a comprehensive third party information security assessment process that is (a) based on best practices and industry standards; (b) assesses information security control design and implementation; (c) identifies security control deficiencies and risks of proposed or existing third party service providers, and remediate those risks. AAIS shall not allow a third party service provider to access, process, or store Protected Data unless AAIS requires that the third party service provider adhere to all of the requirements of this Policy as though it were the AAIS. AAIS shall be jointly and severally liable for a third party service provider's failure to comply with this Policy. Upon request by Member, AAIS shall promptly provide a list of all of its third party service providers that have accessed, processed, or stored Protected Data, as well as information regarding AAIS's third party information security assessment process, and the results of AAIS's assessments.

3.3 Access and Storage Facilities. AAIS shall not access or store Protected Data from any facility in or outside the United States unless the facility has been approved in advance by Member for such access or storage in writing as set forth in a Statement of Work. AAIS shall prevent the movement or copying of Protected Data to any facility that is only approved for accessing Protected Data.

3.4 Data Integrity. Except as otherwise set forth in the Agreement, AAIS shall not modify, delete or destroy any Protected Data or media on which Protected Data resides. At Member's request, AAIS shall identify, in writing, Protected Data or media that has been modified or destroyed. If any of Protected Data is modified, lost or destroyed due to any act or omission of AAIS or any AAIS Personnel, or due to their breach of this Exhibit, AAIS shall promptly regenerate or replace Protected Data to the best of AAIS's capability and ability. AAIS shall prioritize this effort to comply with reasonable deadlines to be established by Member, so that the loss of Protected Data will not have an adverse effect upon Member's business or the Services. If AAIS fails to correct or regenerate the lost or destroyed Protected Data within the time reasonably set by Member, Member may obtain data reconstruction services from a third party, at AAIS's approval and expense, and AAIS shall cooperate with such third party as requested by Member.

3.5 Audit Logs. AAIS shall generate audit logs for actual or attempted unauthorized use, access, disclosure, theft, manipulation, reproduction or possible compromise of any Data Assets. AAIS shall review the audit logs on a regular basis and maintain adequate evidence of its review for the purposes of an audit. AAIS shall maintain the audit logs for no less than twelve (12) months and provide them upon Member's request. In addition, AAIS must maintain any audit logs that reveal evidence relating to a Security Breach for no less than three (3) years, or as otherwise directed by Member.

3.6 Return and Destruction of Data. Within five business days following (a) any request from Member; or (b) the termination or expiration of the Agreement, AAIS shall return to Member or its designee all Protected Data under AAIS's control in any form reasonably requested by Member. Once Member confirms that such Protected Data has been successfully returned, AAIS shall destroy any of Protected Data that remains under its control. Whenever AAIS is required to destroy any of Protected Data, AAIS shall do so in accordance with NIST SP 800-88 Rev 1, or the relevant successor standard, and provide attestation in a form substantially similar to Appendix G thereof, including sanitization and media destruction details. AAIS shall maintain a report of all Protected Data so destroyed and provide such report to Member upon request.

4.0 Security Breach Management

4.1 Notification to Member. AAIS shall notify Member of any Security Breach within twenty four hours following discovery of such Security Breach via e-mail. Such notice shall (a) describe the nature of the Security Breach; (b) provide AAIS's estimate of the impact on Protected Data; (c) identify a senior level person responsible for communicating with Member regarding the Security Breach; and (d) describe investigative and remediation actions taken and planned.

4.2 Investigation and Remediation. AAIS shall provide regular updates on all investigative and corrective action taken. AAIS agrees to reasonably cooperate with Member in its investigation of and response to any Security Breach. Upon completion of the investigation, AAIS shall provide Membership with a written report that describes (a) the cause and extent of the Security Breach; (b) Protected Data impacted; and (c) all remedial action taken, including to prevent any recurrence of the Security Breach.

4.3 Notices and Costs. If Member determines that notice is required by Applicable Law or Member's contractual obligations, AAIS shall promptly provide all necessary information for Members to notify any affected individuals, consumer reporting, regulatory or law enforcement agencies or other identified entities.

5.0 Access, Use and Disclosure of Protected Data

5.1 AAIS shall not collect, use or disclose Protected Data except as necessary to perform the Services and process transactions requested by Member. Without limiting the generality of the foregoing, AAIS shall not use Protected Data, including in an aggregated or anonymized form, for purposes including but not limited to data analytics, marketing materials, or product development, unless expressly permitted by Member in writing. AAIS shall limit access to Protected Data to only: (a) AAIS Personnel with a need to access Member Data pursuant to this Policy; and (b) Member or its designated representatives. If AAIS receives any request, warranty, subpoena or other legal or governmental request with respect to Protected Data, AAIS shall immediately notify Member and shall not make any disclosure thereof without prior written consent of Member, unless AAIS's attorneys determine that such disclosure is required to prevent penalties. AAIS shall not modify, delete or destroy any Member Data without prior authorization from Member except to perform the services under the Agreement or comply with the requirements of this Policy.