

AuditBoard, Inc.
Security Terms

AuditBoard shall implement and maintain documented policies and procedures ("Security Policy") that includes appropriate administrative, physical, technical and organizational measures designed to: (i) protect the security, confidentiality, availability and integrity of Customer Data; (ii) protect against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of Customer Data; (iii) protect against threats or hazards to the security, confidentiality, availability and integrity of Customer Data; and (iv) comply with Applicable Data Protection Laws. AuditBoard shall regularly monitor, evaluate and assess the effectiveness of the administrative, physical, technical and organizational measures implemented.

AuditBoard's administrative, physical, organizational and technical measures shall include, at a minimum, the following:

1. Access to Customer Data. Access controls to manage access to Customer Data and system functionality, unique IDs and passwords, strong (i.e., two-factor) authentication for remote access systems, and promptly revoking or changing access in response to terminations or changes in job functions. AuditBoard shall prevent disclosure or dissemination of Customer Data to any person not having a need to know of or access to such information. Access to Customer Data must therefore respect the "need to know" and "least privilege" principles: access can only be granted to persons whose function justifies it, for a specific purpose and their privileges are restricted to the strict minimum necessary to perform their duties.

AuditBoard shall implement and maintain controls to ensure the proper segregation of systems and data and make sure Customer Data and/or systems are properly isolated. Further, the Services must not involve any manual interaction from AuditBoard for the day-to-day management of resources provided by AuditBoard to Customer as part of the Services.
2. Access Control to Systems; Password Management. Unauthorized access to information technology systems must be prevented, including through the use of technical and administrative measures for user identification and authentication. AuditBoard shall ensure appropriate password hardening standards are in place that align with accepted industry security frameworks to ensure sufficient controls, including use of passwords with sufficient length and complexity.
3. Physical Security. AuditBoard shall provide technical and organizational measures to control access to premise and facilities and prevent unauthorized access. Controls are in place to protect AuditBoard's information technology infrastructure from environmental hazards, to manage and monitor employees into and out of AuditBoard's facilities where Customer Data is processed, and to otherwise prevent unauthorized individuals from gaining physical access to premises, buildings or rooms where systems that process Customer Data.
4. Network Security. Network security controls shall include the use of firewalls, layered DMZs, and updated Intrusion Detection and/or Prevention Systems to help protect systems from intrusion or limit the scope or success of any attack or attempt of unauthorized access.
5. Vulnerability and Patch Management. Vulnerability management procedures and technologies shall be used to identify and mitigate against security vulnerabilities. AuditBoard shall ensure that application system and network device vulnerabilities are evaluated and security patches are applied in a timely manner. AuditBoard shall also conduct periodic penetration testing of Internet facing applications and shall use a risk based approach to determine the timing for remediation of the vulnerabilities. AuditBoard shall remediate or mitigate critical or high risk vulnerabilities discovered under this Section promptly.
6. Policy Review. AuditBoard shall review its Security Policy at least annually and provide change management procedures to ensure all modifications to AuditBoard's technology and information assets are tested, approved, recorded and monitored as needed.
7. Administrative/Organizational Management. Organizational management shall ensure the proper development and maintenance of information security and technology policies, procedures and standards, including the Security Policy.
8. Input (Data Integrity); Auditing, Logging. AuditBoard shall retain information system log records to the extent needed to enable monitoring and reporting of unauthorized information system activity, including account logon events, account management, security events, policy change, privileged functions and administrator account creation/deletion. AuditBoard shall conduct regular reviews for indications of inappropriate or unusual activity, and AuditBoard shall protect log records from unauthorized access, unauthorized release, loss, modification, falsification, and deletion. This includes making sure it is possible to examine and establish whether, and by whom, Customer Data have been entered, modified or removed from its information technology assets and infrastructure.
9. Data Incidents. AuditBoard shall promptly notify Customer in writing of any loss, unauthorized disclosure or misuse of Customer Data or of AuditBoard's Security Policy upon AuditBoard becoming aware of such incident (each a "Data Incident"). A comprehensive written notice should be provided to Customer. The notice shall summarize in reasonable detail the nature and scope of the Data Incident and the corrective action taken or to be taken by AuditBoard. The notice shall include supplements in the detail reasonably requested by Customer to the extent this is available, including, but not limited to, relevant forensic reports. AuditBoard shall use all industry standard efforts to remedy any Data Incident immediately but no later than within thirty (30) days of discovery of a Data Incident.

10. Audits and Compliance. AuditBoard shall keep full and accurate records and make these available for inspection by Customer and its agents and independent auditors no less than once per year upon reasonable written notice during the term of Agreement and for a reasonable period thereafter or as otherwise required by law. For clarity, the documentation that may be requested as part of Customer's ongoing due diligence and compliance requirements include by way of example audit information provided under SSAE 18 SOC2 reports, information security policies, incident response policies, physical security plans, privacy policies, and procedures related various relevant regulatory requirements as requested and may be amended from time to time.
11. Contingency planning. AuditBoard maintains policies and procedures for responding to a disaster or business continuity issue, that damages or makes unavailable Customer Data or systems that contain Customer Data, including a data backup plan and a disaster recovery plan.
12. Job Control. Processing of Customer Data occurs only as permitted by Agreement. This includes implementing appropriate security and integrity procedures, such as (i) requiring AuditBoard employees, representatives and other personnel to sign terms and conditions requiring confidentiality and information security responsibilities, including requirements to protect Customer Data and compliance with the Agreement and with applicable laws (including Applicable Data Protection Laws), and (ii) providing appropriate privacy and information security training to such AuditBoard's personnel.
13. Secure Destruction and Disposal. Developing, implementing and maintaining appropriate measures designed to destroy or otherwise properly destroy and sanitize Customer Data prior to disposal, including release of technology infrastructure and assets used to process Customer Data out of organizational control, or release of such systems for reuse. Proper destruction or sanitization methods include compliance with NIST-developed guidelines for media sanitization, to ensure that third parties cannot obtain Customer Data in hardcopy form and Customer Data in digital form is not recoverable by any known forensic means.
14. Disclosure (Transmission) Control; Encryption. AuditBoard shall encrypt all Customer Data in transit and at rest using industry standard encryption protocols.
15. Availability Control; Business Continuity; Transition of Services; Data Portability. Customer Data is protected against accidental destruction or loss (including requirements specified in this Agreement). Comprehensive data assurance mechanisms are employed including backups, data redundancy, environmental controls (e.g., fire and smoke detectors, fire suppression and secure facilities) and the implementation, maintenance and regular testing of disaster recovery plans.