Information Security Addendum

Section 1 - Purpose

1.1 This ISA sets forth TriTech's commitments for the protection of Client data. TriTech will use commercially reasonable technical and organizational measures designed to protect against unlawful or unauthorized access, use, alteration, or disclosure of Client data that comes into possession of TriTech via TriTech's Stratus platform or any other TriTech hosted environment.

Section 2 - General Provisions

2.1 TriTech will implement and maintain a written information security program that maintains administrative, technical, and physical safeguards, designed to:

- ensure the security and confidentiality of all Client Confidential Information that is processed, stored, or controlled by TriTech;
- protect against anticipated threats or hazards to the security or integrity of such Confidential Information;
- prevent unauthorized access to or loss, acquisition, disclosure, or use of such Confidential Information; and
- ensure the secure disposal of such Confidential Information in compliance with applicable National Institute of Standards and Technology (NIST) standards.

2.2 TriTech will use reasonable efforts to ensure its written information security program and administrative, technical, and physical safeguards align with accepted industry practices, and comply with applicable data protection and privacy laws, as well as the terms and conditions of the Agreement, including those contained in this Information Security Addendum.

Section 3 - Definitions

3.1 **Client Data** means all information and data entered, stored, generated, or processed in or through TriTech Systems by or on behalf of the client in connection with the services under the Agreement.

3.2 **Confidential information** includes a company's nonpublic information, but excludes a company's publicly available information.

3.3 **Confidentiality** refers to the protection from unauthorized disclosure.

3.4 **Least Privilege** is the practice of limiting access to the minimal level that will allow employees and contractors to still perform their assigned responsibilities.

Section 4 - Data Management & Protection

4.1 **Data Classification.** TriTech shall maintain an appropriate data governance program to classify and retain information.

4.2 **Encryption.** All Client Data is encrypted in transit and at rest, with access restricted based on the principle of least privilege.

4.3 **Segregation.** Client Data will be logically segregated from the data of other TriTech clients.

4.4 **Removeable media.** TriTech will not allow its employees or contractors to store Client Data on any portable removable media (such as USB mass storage, external hard drives, and CD/DVDs);

4.5 **Data Archival and Backup.** TriTech leverages data replication across geographically dispersed data centers as well as a local backups.

4.6 **Media Sanitization.** When sanitization is required, TriTech will comply with industry standard practices employing reasonable secure methods that render client information unreadable and unrecoverable.

Section 5 - Human Resources

5.1 **Screening. Background Checks and Training.** TriTech conducts reasonable and appropriate background investigations on all its employees and contractors prior to commencement of employment. TriTech shall not allow any employee or contractor to perform services for client or access Client Data if such background checks reveal such individual was convicted of a felony involving theft, dishonesty, or breach of trust.

5.2 **Training.** TriTech will provide annual security awareness training on policies and procedures regarding the security, integrity and confidentiality of Client Data to all new and existing employees and contractors.

5.3 **Revocation.** TriTech will revoke physical and logical access for each TriTech employee or contractor within 24 hours of such individual's termination of employment.

Section 6 - Authentication and Access Management

6.1 TriTech shall assign a unique identifier (User ID) to all users accessing its information processing systems.

6.2 TriTech maintains password controls in accordance with then-current industry standards. For example; including minimum length, lockouts, expirations, stored encrypted, and password reuse. Password controls shall be included in all TriTech information systems that contain Confidential Information.

6.3 TriTech will follow the principle of "least privilege" when granting access to TriTech systems.

Section 7 - Application Performance and Security

7.1 TriTech will utilize a software development life cycle that follows best practices defined by NIST and the OWASP Software Assurance Maturity Model (SAMM), excluding some encryption standards for TriTech's non-Stratus hosted environments.

7.2 TriTech will ensure the security of its applications and environment by leveraging a "security by design" approach. TriTech will perform both static and dynamic automated web application security code analysis on all code prior to deployment in a production environment and correct security flaws discovered by source code analyses prior to deployment.

7.3 TriTech will, in accordance with generally accepted industry standards, monitor the Services and TriTech networks, servers, and applications for potential security vulnerabilities. TriTech will promptly respond to any identified vulnerabilities and assess criticality to resolve, or implement compensating controls for, such identified vulnerabilities within a reasonable amount of time, taking into account the risks posed by each such vulnerability.

7.4 TriTech QA and test networks and environments will be physically or logically separated from production networks and environments.

7.5 TriTech will enforce a formal change management process which will include tracking and approving all product changes. Any such changes will be internally reviewed and tested within a staging environment before such changes are finalized and deployed.

7.6 TriTech will not use Client Data for testing purposes.

Section 8 - Business Resiliency and Incident Response

8.1 **Incident Response.** TriTech information security program will include written incident response policies and procedures to define roles and responsibilities in the event that there is any actual, or reasonably suspected, unauthorized access to TriTech facilities or systems.

8.2 **Security Breach.** Upon becoming aware of any actual or reasonably suspected unauthorized third-party access to, or disclosure of, Client Data, TriTech will: (i) immediately investigate, and take reasonable measures to remediate, the cause of such Client Data Incident, and (ii) promptly, but no later than forty-eight (48) hours after discovery, notify Client of such Client Data Incident. The notification will include, to the extent known, details of the incident, including the time, date, and nature of the incident and contact information for a member of TriTech's information security team who can answer additional questions.

8.3 **Business Continuity/Disaster Recovery.** TriTech will maintain a Business Continuity and Disaster Recovery Plan for the Services and implement the Plan in the event of a disaster, as defined in the BCP. The BCP will include disaster avoidance procedures which are designed to safeguard Client Data and TriTech's data processing capabilities in the event of a disaster as defined in the BCP. TriTech will test the BCP on at least an annual basis.

Section 9 - Threat Management

9.1 Security relevant updates such as patches and configuration fixes shall be applied in a timely manner based upon the classification of information by a system and/or the criticality of the update.

9.2 Endpoint protection is deployed to all applicable devices on TriTech's network to safeguard data and workflows.

9.3 TriTech will deploy vulnerability scanning mechanisms in its information systems and on hosted applications and will configure such mechanisms to conduct regular scans on TriTech operating systems and infrastructure, web applications, and databases. TriTech will analyze and assess all scan reports.

9.4 TriTech will undergo annual penetration testing and will conduct quarterly security audits to identify potential vulnerabilities in the infrastructure used to provide the Services.

Section 10 - Physical Security

10.1 **Facilities Access.** TriTech will employ physical security procedures to ensure that only authorized individuals and guests have access to corporate facilities. Such procedures will include the use of CCTV, cardkey access, processes to log and monitor visitors, and use of receptionists.

10.2 **Data Center Access.** TriTech will employ physical security procedures and controls to ensure that only authorized individuals have access to TriTech data centers.

10.3 **Physical Security.** TriTech will employ data center security measures that align with the AICPA trust principles for physical security and will, at a minimum, secure TriTech data centers using: floor-to-ceiling walls, multi-factor authentication for data center access, 24/7 security monitoring, alarmed exits, and onsite security personnel.

10.4 **Data Center Locations.** TriTech primary and disaster recovery data centers will be located in geographically diverse locations to enhance security, availability, and resiliency.

Section 11 - Annual Security Reviews

11.1 TriTech will undergo an annual independent third-party SOC 2 Type II (or its equivalent or successor) assessment of its information security program and its administrative, technical, and physical safeguards for all facilities used to deliver the Services. TriTech will provide the results report upon request.