Information Security Program Summary Exhibit

1. **Scope.** Built is committed to maintaining the security and availability of its products and services consistent with prevailing industry standards. The Information Security Program Summary ("IS Summary") describes the administrative, physical and technical safeguards Built maintains to protect data defined as Confidential Data, Participant Data, and Client Data in the Agreement ("Protected Data") from unauthorized access, use or disclosure that would violate the Agreement.

2. **Information Security Program.** Built maintains and complies with its InfoSec Program that requires commercially reasonable policies to remain aligned with an industry recognized security framework (e.g., CIS Top 20, ISO27001, NIST, etc.). The InfoSec Program includes and addresses administrative, technical, and physical safeguards, including at a minimum:

    1. proper disposal of data after it is no longer needed;
    2. access controls on electronic systems used to maintain, store, access, or transmit Protected Data;
    3. access restrictions at physical locations containing Protected Data;
    4. strong encryption (i.e., secure protocols and algorithms) protecting electronic Protected Data in motion and at rest;
    5. business continuity, disaster recovery and incident management;
    6. testing and monitoring of electronic systems;
    7. procedures to detect actual and attempted attacks on, or intrusions into networks where Protected Data traverses and systems containing or accessing Protected Data;
    8. compliance with applicable laws and regulations related to information security;
    9. application security and risk assessment; and
    10. annual data privacy and security refresher training for all employees, contractors, and agents.

    Built reviews its InfoSec Program and all other Protected Data security precautions no less than annually, and updates and maintains the same as necessary to comply with applicable laws, regulations, technology changes, industry best practices, and to support Built's data privacy program and policy.

3. **Security Protocols.** Pursuant to the InfoSec Program, Built maintains the following specific security protocols:

    a. **Encryption.** Built employs strict encryption processes for all data in transit and at rest. For example, data is required to be transmitted only via secure means (HTTP over TLS, or "HTTPS"). If transmission of files between a Client and Built is applicable as part of a Client's chosen service offering, Built requires that the file(s) be transmitted via secure means (e.g., SFTP). All databases and backups containing Client Data are encrypted via AES 256-bit encryption.

    b. **Physical Security.** Built utilizes Amazon Web Services ("AWS") as its Infrastructure-as-a-Service provider. The production environment where Client Data is securely stored at-rest is cloud-hosted in AWS and Built additionally maintains a backup disaster recovery/failover site within a separate AWS region. AWS is renowned for rigorous physical security measure and those can be referenced at the following site: https://aws.amazon.com/compliance/data-center/data-centers/. Built may updates it Infrastructure-as-a-Service provider with prior notice to Client.

    c. **Management, Control, and Protection of Networks.** Built maintains and employs identity access management ("IAM") policies and procedures that are founded on the principles of least privilege to ensure access to systems containing Client Data is restricted to authorized personnel only including the following controls:
        i. Access to firewalls are restricted to a limited number of authorized personnel;
        ii. All connections to the external network terminate at a firewall;
        iii. Network devices deny all access by default;
        iv. Security patches are regularly reviewed and applied to network devices;
        v. Critical network segments are isolated;
        vi. Insecure protocols are prohibited from being used to access network devices;
        vii. Access to diagnostic/maintenance ports on network devices are restricted; and
        viii. Network intrusion prevention and detection methods are utilized.

d. **Secure Development Practices.** Built's development environments are separated into Local, Test, Quality Assurance ("QA"), and Production. Each environment is on a different AWS account and cannot communicate with each other and cannot access any data or secure content in another environment. Built's software development life cycle process includes a formalized request and approval process for changes, multi-peer code review, static code analysis, and separation of concerns for promoting changes to production. All environment promotion processes are controlled by non-development personnel.

e. **Employee Access**. Built will not give any of its employees access to Protected Data without a written nondisclosure agreement between the employee and Built protecting Protected Data. Prior to allowing any Built employee to perform Services for Client, Built will conduct a background check on employee consistent with the following:

- SSN validation confirms the SSN is valid and identifies both the state and the year of issuance. The search also covers the national death index.
- Search of sex offender registries in all 50 states and the District of Columbia.
- Search of various US and international government watch lists, such as the Office of Foreign Asset Control, Interpol and Specially Designated Nationals.
- National criminal search is a multi-jurisdictional search that encompasses numerous sources. It includes national security sources, numerous federal databases, and arrest and criminal data from various local, county and state agencies.
- County criminal checks for all counties returned for that applicant over the last 7-year period. This includes any legally reportable felony and misdemeanor convictions, pending cases and dismissed records.

No employee will be assigned to provide Services to Client if that employee's background check includes a felony conviction of any criminal offense involving dishonesty, breach of trust, or money laundering, or who has entered into a pretrial diversion or similar program in connection with such an offense, within the five years prior to the start date of the proposed assignment.

f. **Significant Subcontractor Access.** Built requires all Significant Subcontractors who will access Protected Data to enter into written agreements including substantially similar confidentiality and data security terms as those described in this IS Summary.

4. **Data Backup.** Built's databases containing Protected Data are backed up daily and stored within encrypted secure backup storage. Built conducts daily differential backups and weekly full backups. Additionally, there is live, near-real-time database synchronization happening across our primary and failover data centers within AWS. These secondary copies are also backed up in the same manner.

5. **Data Breaches.** In the event of exposure of Protected Data due to an intrusion by an untrusted third party ("Data Breach"), Built will (i) notify Client within two business days of Built's confirmation of the Data Breach; and (ii) cooperate with Client and law enforcement and/or regulatory agencies, where applicable, to investigate and resolve the Data Breach, including without limitation by providing reasonable assistance to Client in notifying third parties impacted or injured by the same. Built will give Client prompt access to such records related to a Data Breach as Client may reasonably request; provided such records shall be treated as Built's confidential information pursuant to the confidentiality and non-disclosure terms of the Agreement and Built shall not be required to provide Client with records belonging to, or compromising the security of, its other customers.