EXHIBIT B
DATA SECURITY STANDARDS

INTRODUCTION & DEFINITIONS

These Data Security Standards ("**Data Security Standards**") reflect the reasonable controls that the parties maintain as part of its information security policies and procedures. The term "should" in these Data Security Standards means that the party will use commercially reasonable efforts to accomplish the stated Data Security Standards. Any required policies, procedures, or processes mentioned in these Data Security Standards must be documented, reviewed, and approved, with management oversight, on a periodic basis. Terms defined in these Data Security Standards shall apply solely to these Data Security Standards. Capitalized terms used but not defined herein shall have the meanings assigned to such terms in the Agreement. In the event of a conflict or inconsistency between these Data Security Standards and the agreement to which these Data Security Standards are attached (the "**Agreement**"), the Agreement shall prevail.

I. SITUSAMC DATA SECURITY STANDARDS

SitusAMC shall take the following technical and organizational measures to ensure the security of the Confidential Information and Company Personal Data. Not all the stated Data Security Standards will apply to all Services or other Deliverables, but SitusAMC must be able to reasonably show how the Data Security Standards do not apply.

A. TECHNOLOGY GOVERNANCE, RISK ASSESSMENT, AND COMPLIANCE

1. Controls are validated through a documented risk assessment program conducted at least on an annual basis to aid in determining their compliance with industry standards and to the extent necessary managed remediation efforts and to to verify the effectiveness of the controls that aid in protecting business operations, Confidential Information and Company Personal Data.
.
2. SitusAMC's security policies and procedures provide requirements for the administration of the receipt, transmission, processing, storage, control, distribution, retrieval, and access of confidential and protected information, assets, and associated services.
3. SitusAMC will maintain, and Company may request, a copy of SitusAMC's most recent SOC 2 report.

B. PHYSICAL AND ENVIRONMENTAL SECURITY

1. Physical and environmental security processes and procedures are in place for facilities with access or storage of Confidential Information and Company Personal Data.
2. Applications are hosted in ISO 27001 certified data centers. Physical access to these data centers is highly restricted.
3. SitusAMC will take reasonable measures to prevent unauthorized personnel from gaining access to Company Personal Data. Personnel are granted access to areas of the facility based on the principle of least privilege.
4. Physical access to facilities is restricted, with all access recertified at least on an annual basis.
5. Detective monitoring controls (e.g., CCTV) are in place with a defined retention period.
6. Addition or removal of assets from the facility are documented and tracked.
7. Information Technology must obtain approval from InfoSec prior to allowing assets with SitusAMC Confidential Information to be removed from a facility.
8. Facilities maintain environmental controls, including fire detection and suppression, climate control and monitoring, power and back-up power solutions, and water damage detection.
9. Environmental control components are monitored and tested at least on an annual basis.

C. PROTECTION OF DATA

1. Confidential information and Company Personal Data must be protected and encrypted in transit and at rest (including in backup) as well as when shared with SitusAMC's subcontractors, using

strong cryptographic algorithms with the latest supported TLS or equivalent protocols.

2. Authentication credentials are encrypted in transit and at rest and must be supported through multi-factor authentication.
3. SitusAMC Information Security Policy includes data classifications, encryption use, key and certificate lifecycle management, permitted cryptographic algorithms and associated key lengths, message authentication, hash functions, digital signatures, random number generation and is reviewed against industry standards on at least an annual basis.

D. IDENTITY AND ACCESS MANAGEMENT

1. Documented logical access practices supports role-based, and "need-to-know" access based, on the principle of least privilege and segregates duties during the approval and provisioning process.
2. Logical access requirements cover remote access, access request approval prior to access provisioning and periodic recertification of access.
3. Each account provisioned is uniquely identified.
4. Management of privileged user accounts, including service accounts, follows a documented process and are restricted.
5. SitusAMC will take reasonable measures to prevent unauthorized persons from gaining electronic access to Company Personal Data. Such measures include the following:
    a) Access to the data processing system is limited to authorized individuals and requires identification and successful authentication by username and password using state-of-the-art security measures.
    b) Authentication media and access codes to access data processing systems on 3rd and 2nd Level are linked to personal credentials (password and user ID). No reusable IDs (e. g. trainee1, etc.) are assigned.
    c) A process for requesting, approving, issuing, and withdrawing authentication media and access authorizations has been set up and documented.
    d) If the workstation is inactive for more than five minutes, a password-protected screen saver is automatically activated using the built-in mechanisms of the operating system.
    e) Workstations are protected against unauthorized use when leaving the workstation temporarily (by manually activating the password-protected screen saver or by locking the system).
    f) Elevated account passwords are managed by password managers and are generated with a minimum complexity of at least 12 characters as well as a character mix of numbers, special characters and upper-and-lower case letters.
    g) Access to the workstations and password manager is password protected. The password must be at least 10 characters long as well as a character mix of numbers, special characters, and upper-and- lower case letters
6. Authentication and authorization practices cover SitusAMC systems and networks and include password provisioning requirements, password complexity requirements, password resets, thresholds for lockout attempts, thresholds for inactivity, and prohibition against use of shared accounts.
7. The access rights of SitusAMC employees and external party users to Confidential Information and Company Personal Data and facilities shall be removed upon termination, but in no less more than 24- hours after termination of their employment, contract or agreement, or adjusted upon change of role.
8. Multi-factor authentication is implemented for:
    a) The initiation of any privileged access session and/or retrieval of credentials with privileged access;
    b) External connectivity to the SitusAMC network;
    c) SaaS providers and toolsets used by SitusAMC employees or contractors;
    d) Access to SitusAMC networks or systems;
    e) Applications containing sensitive or Company Personal Data; and

f) Applications directly accessible from the internet.

E. SECURITY CONFIGURATION

1. SitusAMC maintains controls over its communication network to aid in safeguarding data, including but not limited to electronic mail and instant messaging systems.
2. A network diagram, to include devices, as well as a data flow diagram are kept current.
3. Network devices have internal clocks synchronized to reliable time sources.
4. Standard security configurations utilizes the principles of least functionality/privileges and security hardening demonstrated.
5. Information systems must be deployed with recognized industry standard security configurations and reviewed on at least an annual basis.
6. Drift or deviation from hardened builds/security configuration baselines are identified, reported, and remediated.
7. The production network is isolated from the development and test environments.
8. Malware protection mechanisms exist to aid in detecting and/or preventing against malware and other threats.
9. Malware protection mechanisms are configured to perform real-time or scheduled scans of systems, and provide alerts when malware is discovered.
10. All devices and malware protection mechanisms must be kept up-to-date with latest anti-virus software and definitions.
11. Network and host-based intrusion detection and intrusion prevention systems (IDS and IPS) are deployed with generated events fed into centralized systems for analysis.
12. Cookie activity is compliant with the laws applicable to SitusAMC.
13. Access to non-corporate/personal email and instant messaging solutions are restricted.
14. Preventive controls block malicious messages and attachments as well as prevent auto- forwarding of emails.
15. SitusAMC ensures testing and staging systems are separated logically from production systems.

F. SECURITY OPERATIONS

1. SitusAMC personnel are trained (on an ongoing basis – no less regularly than annually) to identify, and report suspected security weaknesses and events/incidents.
2. Data Loss Prevention (DLP) technology, processes, and/or solutions are deployed to aid in protecting against the exfiltration of Confidential Information and Company Personal Data.
3. SitusAMC maintains a security event and incident management response policy and procedure.
4. Retention schedule for various logs is defined and followed.
5. Security event logs from information systems are collected, centrally managed, analyzed, and correlated for the purpose of aiding in the detection of anomalous behavior that may indicate malicious events/incidents.
6. Utilizes industry standard fraud and threat detection processes to aid SitusAMC for monitoring and reporting actual and suspected instances of fraud, and establish protocols for specific notification and communication, internally.
7. SitusAMC maintains a process to conduct digital forensics including data collection, data/evidence preservation for future analysis, analysis, reporting of findings, and closure.
8. At least on an annual basis, SitusAMC conducts attack simulations on a segregated environment including social engineering exercises (e.g., phishing), red teaming, and tabletop exercises with reporting, remediation/acceptance, and tracking of such findings.

G. VULNERABILITY MANAGEMENT

1. Vulnerability scans and penetration tests are performed against internal and external networks and applications at least once on an annual basis and prior to system provisioning for systems that process, store, or transmit Confidential Information and Company Personal Data.
2. Any critical vulnerabilities identified during vulnerability scans or penetration testing are

prioritized and resolved.

H. TECHNOLOGY DEVELOPMENT

System Development Life Cycle (SDLC)

1. For Software development, SitusAMC adheres to its system development life cycle (SDLC) process.
2. The SDLC contains the control requirements for SitusAMC's software development.
3. The SDLC includes a secure design review, that includes controls to aid SitusAMC in identifying vulnerabilities and design flaws.
4. SitusAMC utilizes a risk-based approach to remediate or resolve identified vulnerabilities and design flaws prior to production or making such Software generally available to its clients.

Third-Party Software: To the extent third party and/or open source code or software is used, it will be evaluated, approved, licensed, inventoried, and supported as applicable.

1.

I. TECHNOLOGY OPERATIONS

1. Documented operational procedures are designed to aid SitusAMC in providing for the secure operation of SitusAMC's assets.
2. Operational procedures include monitoring of capacity, performance, service levels, and key performance indicators.
3. SitusAMC utilizes reasonable, industry standard measures to aid it in protecting media in storage including offsite storage.
4. SitusAMC maintains a data retention and destruction policy that includes practices for the destruction of Confidential Information and Company Personal Data, which also includes disposal or reuse of equipment used for logical and physical storage.
5. Retention procedures for records shall be handled in accordance with SitusAMC's data retention and destruction policy.
6. The ability to write to portable electronic media is limited to documented exceptions.
7. Changes to the system, network, applications, data files structures, other system components and physical/environmental changes are monitored and controlled through SitusAMC's change control process and environment.
8. Changes must be reviewed, approved, and monitored during pre- and post-implementation to test the accuracy of the expected changes and their desired result.
9. SitusAMC also maintains an emergency change management procedure in the event factors exist that require an emergency change outside of the standard change management procedures.
10. Any changes materially affecting SitusAMC's services must be communicated prior to implementation.

J. RECORDS MANAGEMENT

1. Records created, received, stored and/or retained follows a defined, regularly reviewed procedure that manages the record throughout its lifecycle.
2. For any information that is held according to SitusAMC retention obligations, it will be disposed of or destroyed in accordance the DRDP.

K. PSEUDONYMIZATION & ENCRYPTION

1. Encryption. All communication of our systems over public networks is encrypted according to the state of the art. SitusAMC encrypts user passwords by using best-practice one-way hash functions and the core databases are encrypted at rest using industry best practices disk

encryption schemes.

2. Pseudonymization. SitusAMC uses pseudonyms for storing user related interactions whenever possible.
3. Data Transfer Control. Company Personal Data is transferred exclusively using the encrypted HTTPS protocol.
4. Data Entry Control. Company's activities related to the creation and update of user data records are logged.

L. TECHNOLOGY ASSET MANAGEMENT

1. SitusAMC maintains technology asset registration policy and procedures including unique identifiers for assets, classifications, asset ownership, asset location.
2. SitusAMC maintains a technology asset inventory governance structure to include recorded changes to asset records, back up of asset registers, annual compliance validation of the asset registers, asset ownership recertification, asset register updates when asset records are altered, regular license audits of assets, and remediation of unauthorized assets.
3. SitusAMC maintains its technology asset lifecycle management program and includes lifecycle status of assets, identification of assets not in compliance with SitusAMC's lifecycle management policy, and notification to asset owners of non-compliant assets.
4. SitusAMC maintains its asset provisioning and disposal program, which includes disposing of/removing/deleting all technology assets in a secure manner when they reach end of life.

M. INCIDENT AND EVENT MANAGEMENT

1. Documented incident, event, or problem management procedures include systematic tracking of problems from discovery to resolution.
2. SitusAMC's event management policy and procedures include monitoring for the detection of anomalous events that indicate deviation from the norm beyond a defined threshold.
3. SitusAMC also processes and analyzes events to determine if action is required, and to the extent Company Data is directly involved, and engages Company via the Incident Management process.
4. The incident management policy and procedures include the responsibilities of SitusAMC personnel and identification of parties to be notified in case of an information security event/incident.
5. The SitusAMC's incident management policy and procedures also cover prioritization, roles and responsibilities, internal escalation, notification to Company, tracking and reporting, containment and remediation, and preservation of data to maintain forensic integrity in accordance with industry standards.

N. BUSINESS AND TECHNOLOGY RESILIENCY

1. SitusAMC maintains a formal, business resiliency plan to enable orderly, and sustainable recovery objectives, support processes, operations and technology components within the anticipated time frame given the nature of the disruption.
2. SitusAMC's disaster recovery approach includes the following:
    a) Service Providers. Using state-of-the-art service providers to help deliver services.
    b) Backups. Backups are taken and tested regularly on all relevant systems.
    c) SLAs. SitusAMC uses commercially reasonable efforts to make products and services for our clients available with a monthly uptime percentage, as may be defined in the Agreement.
    d) Global Offices. SitusAMC operates across five countries, and in the event of regional issues in one of SitusAMC's offices, SitusAMC's teams in other locations can support to help recover smoothly.

e) Business Continuity Planning. SitusAMC's business continuity program focuses on natural and man-made disasters for operation of SitusAMC's various global sites and includes plans for different scenarios as well as regular training for the business continuity team. The team is therefore able to recover operations in the event of emergency.

f) Disaster Recovery Planning. SitusAMC's disaster recovery program focuses on technical disasters for operation of the SitusAMC's platform and includes plans for different scenarios as well as regular training for the recovery team. The team is therefore able to regain data in cases of emergency.

3. SitusAMC tests its resiliency and disaster recovery plans at least on an annual basis, notes deficiencies/failures and addresses them accordingly for compliance purposes.

O. ORGANIZATIONAL SECURITY

1. SitusAMC personnel are notified and provided access (a downloadable copy is available) to the SitusAMC Code of Conduct.
2. All SitusAMC personnel will receive Privacy and Security Policy training and are required to read and sign (either physically or electronically) a computers user's agreement (CUA). Signed documents are returned to the Human Resources department where they are kept on file.
3. SitusAMC conducts a tracked performance and/or appraisal review process of its employees.
4. SitusAMC maintains current organizational charts representing key management responsibilities for the Services provided to Company.
5. SitusAMC performs background checks on its personnel.
6. SitusAMC's personnel enter into agreements with SitusAMC that contain non-disclosure or confidentiality obligations.

II. COMPANY DATA SECURITY STANDARDS

Company shall take the following technical and organizational measures to ensure the security of Confidential Information and Company Personal Data:

A. Security Measures.

1. Company will maintain the security measures described in this Exhibit and may implement additional or alternative security measures while making sure the security level of the defined measures is not reduced.

B. Physical Access Control Measures. Company will take reasonable measures to prevent unauthorized persons from gaining physical access to Company Personal Data. Such measures include one or more of the following:

1. Physical access to office buildings and facilities, including rooms hosting data servers, where Company Personal Data is processed is restricted to authorized personnel.
2. Mechanisms in place to restrict physical access to rooms hosting servers storing Company Personal Data to authorized personnel, including identification mechanisms.
3. Servers and other media hosting Company Personal Data are not taken off-site without authorization.
4. Visitors to premises or the rooms hosting servers storing Company Personal Data are identified, escorted by an authorized individual, and their entrance and exit are timely logged.
5. Workstations used by the Exporter's personnel are not taken off-site without authorization and are deployed with proper safeguards to minimize the potential for data leakage, including hard-drive encryption and system lockouts.

C. Logical Access Control. Company will take reasonable measures to prevent unauthorized persons from processing or using Personal Data. Such measures include one or more of the following:

1. Access is strongly authenticated (e.g., by using unique and non-shared personal credentials and strong password policies according to accepted best practices, including multifactor authentication)

and utilizes multi-factor authentication.

2. Access rights to Company Personal Data are granted following a documented request and approval flow.
3. Access to Company Personal Data is restricted with the principle of least privilege.
4. Company Personal Data Administrative access privileges are limited to those persons who actually need it (e.g., have a role that requires admin access).
5. Access rights to Company Personal Data are periodically checked (at least quarterly).
6. Access attempts (both successful and failed) are logged and monitored.
7. Leaves, team changes, and inactive users (e.g., parental leave, sabbatical) are timely addressed (user accounts removed/disabled/adjusted).
8. Multi-factor authentication must be implemented for:
    a) The initiation of any privileged access session and/or retrieval of credentials with privileged access;
    b) External connectivity to the SitusAMC network;
    c) Access to SitusAMC networks or systems;
    d) Applications containing sensitive or Company Personal Data; and
    e) Applications directly accessible from the internet.

D. Pseudonymization Measures. Measures are applied to avoid the association of the Company Personal Data to a specific person whenever possible, e.g., by replacing personal identifiers or names by random data.

E. Encryption Measures. Measures include one or more of the following:

1. The IT systems processing Company Personal Data allow only secure channels or protocols for inbound network connections.
2. The IT systems ensure that proper cryptographic methods are employed for Company Personal Data in-transit and at-rest using strong cryptographic algorithms with the latest supported TLS or equivalent protocols.
3. Certificates and cryptographic keys are securely managed in regard to creating, storing, sharing, deploying, rotating, and/or revoking keys.

F. Measures to ensure integrity, availability, and resilience. Measures include the following:

1. Data integrity, including:
    a) The IT systems processing Company Personal Data produce error and event logs, which are reviewed regularly to identify potential issues of data integrity.
    b) Up-to-date antivirus and antimalware utilities are deployed on all IT systems used in the processing of Company Personal Data.
    c) Company Personal Data is transferred exclusively using the encrypted HTTPS protocol.

2. Transmission control, one or more of the following:
    a) Certificates and cryptographic keys are securely managed in regard to creating, storing, sharing, deploying, rotating, and/or revoking keys.
    b) Secrets (passwords, OAuth 2 Clients, Tokens) used for authentication towards remote services are securely managed in regard to creating, storing, sharing, deploying, rotating, and/or revoking keys.

3. Transport control including one or more of the following:
    a) The IT systems processing Company Personal Data allow only secure channels or protocols for inbound network connections.
    b) Certificates and cryptographic keys are securely managed in regard to creating, storing, sharing, deploying, rotating, and/or revoking keys.
    c) Secrets (passwords, OAuth 2 Clients, Tokens) used for authentication towards remote services are securely managed in regard to creating, storing, sharing, deploying, rotating, and./or revoking keys.

4. Input and data modification controls, such as:
    a) Events related to access to the system are logged.
    b) Minimum attributes to be logged:
    c) Timestamp
    d) Source Identity
    e) Successful and Failed Authentication
    f) Successful and Failed Authorization
    g) Authorization Details (what was authorized)
    h) A process is in place to review and react upon the tracked events.
    i) Logs are protected against unauthorized access and tampering.