Built.io shall comply with the following to the extent that Built.io hosts or otherwise has access to Sensitive Information.

1. **Objectives and Exceptions**.
   Built.io shall have implemented a Security Policy that is designed to:
   (a) Take reasonable steps to protect the confidentiality, integrity, and availability of all Sensitive Information; and
   (b) Take reasonable steps to protect against accidental, unauthorized, or unlawful access, copying, use, processing, disclosure, alteration, transfer, loss or destruction of the Sensitive Information.

   Built.io's Security Policy pertains only to those components and areas over which Built.io has control. This policy does not apply to any changes, modifications, configurations or other actions taken by Customer or its client's with respect to other aspects of Customer solution.

2. **Security Measures**. Built.io shall develop (or modify, as appropriate), implement and maintain reasonable appropriate security measures and procedures to manage and control identified security risks, commensurate with Built.io's obligations pursuant to the Agreement. Such security measures and procedures shall include reasonable physical, technical, and organizational safeguards that are (a) appropriate in consideration of: (1) the sensitivity of the Sensitive Information involved, and (2) the significance of the processing to the protection of privacy, and (b) no less rigorous than (1) those maintained by Built.io for its own systems and information of a similar nature and (2) no less rigorous than accepted industry standards for ensuring the confidentiality, integrity, and availability of confidential information.

   Built.io shall also be responsible for performing the following non-exhaustive obligations:

   (a) Physical Security Measures

   (a) **Physical Security and Access Control** – Ensuring that all systems hosting Sensitive Information of which Built.io is aware of are maintained in a reasonably physically secure environment that ensures barrier(s) to unauthorized access, and that access restrictions at physical locations containing Sensitive Information, such as buildings, computer facilities, and records storage facilities, are designed and implemented to permit access only to authorized individuals, and to reasonably detect any unauthorized access that may occur, including without limitation 24 x 7 security personnel at all relevant locations. These locations will have provisions or redundancy to protect against fire and natural disasters. Locations will provide redundant power, network and cooling systems.

   (b) Physical Security for Media – Implementing and maintaining reasonable and appropriate security measures and procedures that are designed to protect and prevent the unauthorized viewing, copying, alteration or removal of any media containing Sensitive Information.

   (c) Media Destruction – Implementing and maintaining appropriate security measures and procedures that are designed to destroy removable media containing Sensitive Information that is no longer used, or alternatively to render Sensitive Information on such removable media unintelligible and not capable of reconstruction by any technical means before re-use of such removable media is allowed.

   (b) Technical Security Measures

(a) Access Controls on Information Systems – Implementing and maintaining reasonable and appropriate security measures and procedures that are intended to allow access to all systems hosting Sensitive Information and/or being used to provide services to Customer shall be protected through the use of access control systems that uniquely identify each individual requiring access, grant access only to authorized individuals and based on the principle of least privileges, prevent unauthorized persons from gaining access to Sensitive Information, appropriately limit and control the scope of access granted to any authorized person, and log all relevant access events. These security measures and procedures may include, but shall not be limited to, Built.io implementing and maintaining:

(i) Access Rights Policies – appropriate policies and procedures regarding the granting of access rights to Sensitive Information, designed to ensure that only authorized and trained individuals have access. Built.io shall maintain an accurate and up to date list of all staff who have access to the Sensitive Information and shall have the facility to promptly disable access by any individual staff upon termination of employment.

(ii) **Authorization Procedures for Persons Entitled to Access –** reasonable and appropriate security measures and procedures to establish and configure authorization profiles in order to ensure that personnel will only have access to the Sensitive Information and resources they need to know to perform their duties, and that they are only able to access the Sensitive Information within the scope and to the extent covered by their respective access permission. The access will be allocated on basis of segregation of duties, least privilege and on role basis.

(iii) Authentication Credentials and Procedures – appropriate security measures and procedures for authentication of authorized staff, including, but not limited to, the following:

- Systems transmitting and storing Sensitive Information that are designed to prevent access by unauthorized users;
- When privileged access (e.g. root or superuser level access) is granted to systems which handle Sensitive Information and/or are used to provide Services, such access shall be logged; and
- Laptop encryption for all staff who access the Sensitive Information.

(iv) Access Control from outside the Secured Area – reasonable and appropriate security measures and procedures designed to prevent the Built.io's information systems or Sensitive Information from being accessed by unauthorized persons from outside the secure area.

(v) Access Monitoring – reasonable and appropriate security measures and procedures for monitoring access to the Built.io's information systems and Sensitive Information and for maintaining records of system or applicable access attempts, both successful and failed.

(vi) **Intrusion Detection** – reasonably appropriate security measures and procedures designed (i) to ensure that Sensitive Information, assets and /or systems being used to provide Services are protected against the risk of intrusion by our intrusion detection system (IDS), and (ii) to monitor each and every instance of access to Built.io's assets and information systems and to Sensitive Information to detect the same, and to promptly respond to the same. Additional security is available via Built.io's anti-virus plugin which can be acquired for an additional fee.

(vii) **Network Security** – Built.io will establish and maintain infrastructure to ensure that the network is reasonably protected from external as well as internal threats using tools and infrastructure such as firewalls, ACLs, IDS/IPS and other controls as reasonably

necessary. The network will be scanned for vulnerabilities. Penetration testing will be performed at least once a year. Event logging will be in place to ensure that intrusion attempts are logged.

(viii) **Mobile Technology Security** - Built.io shall ensure that any mobile or portal system and/or storage device that processes or stores Sensitive Information will have software which will encrypt the Sensitive Information when the device is outside of the designated data processing facility and/or during transport. The encryption software used will meet the requirements of generally available, commercial software designed to provide disc/media encryption.

(b) Data Management Controls

(i) **Data Monitoring Tools.** The Application will include technical functionality that permits Customer to determine access rights. Customer is responsible for review and monitoring of the Sensitive Information to en sure compliance with applicable laws and the Agreement.
(ii) **Data Destruction –** Implementing and maintaining appropriate security measures and procedures to destroy Sensitive Information when appropriate and in accordance with the Agreement.
(iii) **Data Availability Control** – Implementing and maintaining appropriate security measures and procedures in order to ensure data availability, including procedures to ensure that Sensitive Information is protected from accidental destruction or loss, and against loss of data caused by a power shortage or interruptions in the power supply.
(iv) **Software Patching** – Implementing and maintaining appropriate security measures and procedures in order to ensure the reasonably regular update and patching of all computer software and network device software to eliminate vulnerabilities and remove flaws that could otherwise facilitate security breaches.
(v) **Infrastructure Management -** Built.io will demonstrate reasonable infrastructure management with change control process.
(vi) **Backup, Retention, and Recovery** – Implementing and maintaining appropriate backup and recovery security measures and procedures in order to ensure data availability in the event of loss of data or information systems from any cause. All Sensitive Information will be encrypted when stored and backed-up.
(vii) **Hardening**: All the server, network devices and systems need to be hardened to ensure that default accounts are disabled and unused services are stopped.
(viii) **Application Security**: Built.io will ensure that the application is reviewed on regular basis. Access to the applications may be accomplished through 128 bit SSL channel. Source code audits will occur at least once per year.

(c) <u>Organizational Security Measures</u>

(a) Responsibility – Built.io will assign responsibility for information security management to appropriate skilled and senior staff. As permitted by applicable law, background checks are carried out for all employees who have access to Sensitive Information.
(b) Qualification of Employees – Built.io will ensure the implementation and maintenance of appropriate security measures and procedures to ensure the reliability, technical expertise, and personal integrity of all employees, agents, and contractors who have access to Built.io's information system or Sensitive Information.
(c) Obligations of Employees – Built.io shall be responsible for implementing and maintaining appropriate security measures and procedures in order to verify that any employee, agent or contractor accessing the Sensitive Information knows his obligations and the consequences of any security breach.

3. **Training and Education.** Built.io shall institute training and education program to ensure that staff are trained in and are adequately aware of their responsibilities under the Security Policy.

4. **Audits.** Upon reasonable advance notice, and more than once per calendar year, Customer shall have the right to audit and inspect the systems, network, facilities, applications and books and records of Built.io and its permitted subcontractors to ensure compliance with this Security Schedule.

5. **Incident Management/Escalation.** Built.io shall develop and implement (and require its sub-contractors to develop and implement) an incident response plan for dealing with any security incidents, including, without limitation, escalation paths to senior management based on the incident classification or severity, incident contact lists, initial responses, investigation log, system recovery, issue and eradication, reporting and review and follow up procedures, including appropriate reports to regulatory and law enforcement agencies. Built.io shall notify Customer as soon as is reasonably practical in the event that Built.io has confirmed any actual instances of unauthorized access to the Sensitive Information.

6. **Certifications/Model Clauses**. With respect to data from European Union Nationals, Built.io agrees to to comply with the Standard Contractual Clauses for Data Processors located at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF as may be updated from time to time.