1. How and where does your company encrypt data at rest and data in motion?

   We encrypt data both at rest and in transit. During transit, we utilize a 256-bit SSL encryption and while at rest we utilize a 256-bit Whole Disk encryption. The connection to e-Builder Enterprise is encrypted and authenticated using a strong protocol (TLS 1.1 or greater with a preference for TLS 1.2 or greater).

2. How does your company manage encryption keys including the frequency of key rotation?

   The encryption keys are managed by e-Builder and kept outside of the production Amazon Web Services (AWS) account to guarantee that access by AWS is not possible. We provide both physical and logical separation between the encryption keys and the encrypted data. Encryption keys are rotated on an annual basis.

3. How does your company vet employees who will have physical access to the network and computer infrastructure that hosts your application?

   Physical and environmental protection is provided with Amazon Web Services (AWS) security. The controls are validated on an ongoing basis for compliance. Amazon Web Services Cloud has many compliance controls in place to maintain security and data protection in the cloud. AWS compliance is built on traditional programs to help e-Builder and our clients establish and operate in a secured environment. The compliance programs AWS participates in that are applicable to protecting e-Builder's client data include: SOC 1/ ISAE 3402, SOC 2, SOC 3, ISO 9001:2008, ISO 27001:2013, ISO 27017:2015 and ISO 27018:2014.

   Aspects of the physical hosting facility and the mechanisms in place include the following:

   - **Access Controls**
     - 24-hour manned security, including foot patrols and perimeter inspections
     - Biometric scanning for access
     - Dedicated concrete-walled Data Center rooms
     - Computing equipment in access-controlled steel cages
     - Video surveillance throughout facility and perimeter
     - Building engineered for local seismic, storm and flood risks
     - Tracking of asset removal
   - **Environmental Controls**
     - Humidity and temperature control
     - Redundant (N+1) cooling system
   - **Power Supply**
     - Underground utility power feed
     - Redundant (N+1) CPS/UPS systems
     - Redundant power distribution units (PDUs)
     - Redundant (N+1) diesel generators with on-site diesel fuel storage
   - **Fire Detection & Suppression**
     - Dual-alarmed, dual-interlock, multi-zone, pre-action dry pipe water-based fire suppression

4. Do your company undergo 3rd party audits to validate their controls?

   Operations at e-Builder are audited annually by an independent third party and maintain compliance with SSAE 16 SOC 1 Type 2 standards. Our most recent audit was performed by Auditwerx, a member of the American Institute of Certified Public Accountants (AICPA). We are able to provide a copy of our recent SSAE 16 SOC 1 Type 2 audit report upon request.

   We also contract with a third-party security firm, Whitehat Security. White Hat provides both vulnerability scanning and static code analysis. Whitehat provides detailed feedback reports on any potential security issues. Identified vulnerabilities are reviewed for severity then added to the backlog for the responsible team (development and/or operations) for resolution. Once the fix has been implemented/deployed, Whitehat restests to ensure the issue is truly resolved.

   In addition to e-Builder's SSAE 16 SOC 1 Type 2 compliance, the Amazon Web Services Cloud has many compliance controls in place to maintain security and data protection in the cloud. AWS compliance is built on traditional programs to help e-Builder and our clients establish and operate in a secured environment. The compliance programs AWS participates in that are applicable to protecting e-Builder's client data include: SOC 1/ ISAE 3402, SOC 2, SOC 3, ISO 9001:2008, ISO 27001:2013, ISO 27017:2015 and ISO 27018:2014. More information can be found at: https://aws.amazon.com/compliance/

5. What are your company's notification policies and procedures after a security event – and what constitutes security event?

   The Customer will be notified via email and/or phone within 72 hours of a confirmed data breach involving Customer's data. The e-Builder SaaS Operations Team has controls in place to maintain 24/7 monitoring and respond to security events, intrusion attempts, and/or issues on the infrastructure that host all of our client data. The team monitors notifications from various sources and alerts from internal systems to identify and manage physical and environmental threats.

6. Are backups of my data moved offsite and are they encrypted?

   Backup of our client's data in the AWS Cloud is encrypted, continuous and virtual. The data is copied between at least 3 different datacenters within the respective AWS Region.

7. To what geographic locations is it possible for my data to move?

   Data for US Customers will remain in the AWS US Regions (will not leave the country).

   The AWS Cloud infrastructure supporting our client's data and the e-Builder Enterprise application is built around Regions and Availability Zones. Instances of our client's data and the e-Builder Enterprise software are layered across Availability Zones located throughout our largest production environment in the *AWS US Eastern Region 1*. New customers are setup in our newer environment in the AWS US West 2 region (Oregon). A Region is a geographical

location that has multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking and connectivity, housed in separate facilities that are at least 75 miles apart. These Availability Zones provide e-Builder and our clients with the ability to operate production applications and databases which offer more availability, fault tolerance and scalability than would be possible from a single data center. Availability Zones are connected to each other with fast, private fiber-optic networking, allowing our client's data and the e-Builder Enterprise application to automatically fail-over between Availability Zones without interruption providing real-time redundancy.

8. How does your company securely delete or destroy my data when requested?

   As e-Builder Enterprise is hosted with AWS, we rely on AWS physical security controls & data sanitation to securely dispose of storage hardware. As an added precaution, we do securely wipe drives before deleting them from our servers/environment.

9. How do I get my data if your company goes out of business or I terminate the contract?

   Optional services for data export are available. e-Builder can export data in standard MS SQL format and can contract to provide that service on a periodic basis or at the end of contract.

10. How does your company ensure my data is not lost or destroyed?

    Customer data and backups files are copied to a minimum of 3 datacenters within the AWS region.

11. What happens to my data if your company is purchased by another company?

    Customer data belongs to the customer.

12. In what situations can a third-party seize my data? Will I receive advance notification?
    e-Builder is required to comply with any court of competent jurisdiction regarding lawful orders. Depending on the nature of the seizure/warrant, e-Builder will give notice as soon as practicable, while adhering to the terms of the respective warrant/order.
13. Who pays the penalties for a data breach and any costs of breach notification?
    See the Indemnity and Limitation of Liability provisions of the Piggyback agreement between the parties contemplated hereunder.
14. What insurance do your company have to cover a data breach?

    e-Builder maintains cyber (errors and omissions) liability insurance. Our limit is $2M.

15. Do you have the following authentication policies for your passwords?

    - Do you have a minimum length for the password? Yes
    - Can you make your password expire after 30 days? Yes
    - Do you have password complexity like numbers, upper/lower case letters and special characters? Our highest level of password complexity includes at least one letter, one number, and one special character.

- Would the account lock out after three invalid attempts to log on? Yes
- Can a user re-set their own password after locking it out and how is this done? The assigned City's e-Builder Administrator must first unlock the user. User can then re-set their own password.
- Does your cloud solution log off the account after a certain time of inactivity? Yes

16. Do you store any personal identifiable information on the hard drive of the user that accesses your cloud solution, even if it is a temporary file?

    No personal identifiable information is stored on the hard drive of the user that accesses e-Builder Enterprise. Users can optionally include personal home address and phone information on their user profile.

17. Please provide the most recent copy of your SOC II report.

    e-Builder can provide a SOC I Type II report.

18. Please provide Attestation of Compliance Report

    The e-Builder SOC 1 Type II report can be shared with an appropriate Non-Disclosure Agreement (NDA) in place.